

Erhvervsøkonomi og Erhvervsjura
Copenhagen Business School 2019
Kandidatafhandling – CAND.MERC.JUR

Relationen mellem Hvidvaskdirektivet og Databeskyttelsesforordningen

En juridisk, økonomisk og integreret analyse

The relation between The Fourth Anti Money Laundering Directive and
The General Data Protection Regulation

A legal, economic and integrated analysis



Forfattere: Angela Hao Yun Lo (115896) og Isabella Foshammer Andersen (108112)

Vejledere: Camilla Kampmann og Kalle Johannes Rose

Afleveringsdato: 15. maj 2019

Antal anslag: 236.967

Abstract

This thesis examines the effect data minimisation has on the efficiency of applying the enhanced customer due diligence measures, which is required in connection to the banks work on combating money laundering. Even though the bank lawfully can process personal data, it does not deprive the bank from complying with the general principles and the regulatory authorities.

By analysing the two provisions the banks are imposed on, by the European Union, we are able to demonstrate that data minimisation has a restricting effect on the performance of the enhanced due diligence. One of the restricting core elements is that these provisions counteracts each other by both having the elements of subjective evaluation of whether the customer is high or low; which determines the processing, amount and kind of personal data obtained by the bank. It is shown that assessment customers can require obtaining a large amount of personal data, while The General Data Protection Regulation finds it necessary to minimize the large amount. Verdicts from the supervisory authority data have shown that minimisation shall be followed at all cost.

Furthermore, our analysis has shown that when banks have to perform an enhanced customer due diligence, an asymmetric information in personal information exist between the bank and the customer favouring the customer. The combination of Principal Agent solutions and signalling and screening theories have shown in our analysis to be the optimal solution for this asymmetric balance. This solution entails customers signs a contract which imposes the customers the burden of proof and sanctions if violation of the contract. In addition, the solution includes customers signals the bank in the case of establishing a business relationship and the bank monitors the customers. We hypothesise that this solution will result in a reduction of the deadweight loss the society suffers from money laundering.

However, our final analysis demonstrates that the principles of data minimization limits the effects of our hypothesised solution for asymmetric information by restricting the processing of personal data to an inadequate level, in relation to its purpose. As a result of this, the element of signalling and partly monitoring will be restricted. In conclusion, our hypothesis cannot completely hinder an asymmetric balance of personal information resulting in an unsatisfying reduction of deadweight loss for the society.

Indholdsfortegnelse:

Abstract	1
Kapitel 1	5
1.1 Indledning	5
1.2 Problemstilling	6
1.2.1 Problemformulering.....	8
1.2.2 Juridisk problemstilling.....	8
1.2.3 Økonomiske problemstilling	8
1.3 Synsvinkel og afgrænsning	8
1.4 Metode	10
1.4.1 Juridisk metode	10
1.4.1.1 Retsdogmatisk metode	10
1.4.1.2 EU-retlig fortolkning	11
1.4.1.3 Primær og sekundær regulering.....	11
1.4.1.4 Fortolkningsregler	12
1.4.1.5 Juridisk litteratur	12
1.4.1.6. Soft-law	12
1.4.2 Økonomisk metode.....	13
1.4.2.1 Neoklassisk teori	13
1.4.2.2 Spilteori	13
1.4.2.3 Principal-agent teorien	15
1.4.3 Integreret metode	15
1.5 Kildekritik	16
1.6 Struktur	17
Kapitel 2	19
2.1 Definition af hvidvask af penge	19
2.2 Definition af den risikobaserede tilgang.....	20
2.3 Definition af kundernes risikogrupper i bankerne.....	20
2.4 Definition af kundekendskabsprocedurerne	21
2.5 Definition af dataminimering	23
Kapitel 3	24
3.1 Formålsfortolkning af 4AMLD og GDPR.....	24
3.2 Den skærpede kundekendskabsprocedure	27

3.2.1 Personoplysninger ifølge hvidvaskdirektivet og hvidvaskloven	31
3.3 Dataminimeringen i GDPR's artikel 5, stk. 1, litra c.....	33
3.3.1 Ordlydsfortolkning af dataminimeringens principper	34
3.3.2 Fortolkning af dataminimerings principper	36
3.4 GDPR's påvirkninger for 4AMLD.....	37
3.4.1 Etablering af forretningsforbindelse	38
3.4.2 Igangværende forretningsforbindelse	40
3.4.2.1 Den vedvarende overvågning.....	40
3.4.2.2 Den vedvarende overvågning i forhold til dataminimeringen	41
3.4.2.2.1 Ajourføring af informationer:	44
3.4.2.2.2 Konsekvensanalyse	46
3.4.2.2.3 Artikel 30-fortegnelse:.....	48
3.4.2.2.3 Den risikobaserede tilgang vs. subjektiv vurdering	50
3.5 Delkonklusion	55
Kapitel 4	57
4.1 Bayesian spil.....	58
4.1.1 Signaling teori.....	60
4.1.2 Screening teori	67
4.1.3 Principal-agent problemet.....	72
4.1.3.1 Den asymmetriske information mellem bankerne og kunderne.....	72
4.1.3.2 Adverse Selection og Moral Hazard	74
4.1.3.2.1 Tredjepartsvurdering	76
4.1.3.2.2 Overvågning.....	78
4.1.3.2.3 Indgåelse af kontrakt	80
4.1.3.2.4 Bevisbyrde	81
4.2 Delkonklusion.....	82
Kapitel 5	85
5.1 Løsninger sammenholdt med gældende ret	87
5.1.1 Signaling.....	87
5.1.2 Screening	89
5.1.3 Uafhængig vurdering af tredjepart	91
5.1.4 Overvågning	94
5.1.5 Indgåelse af en kontrakt	95
5.3 Kampen mellem 4AMLD og GDPR	97

5.2.1 Mulighederne for fravigelse af GDPR	99
5.3.1 Omkostninger i forbindelse med bekæmpelse af hvidvask af penge	100
5.3.1.1 Omkostninger ved at overholde dataminimeringen	100
5.3.1.2 De bødeforlæg ved overtrædelse af GDPR og 4AMLD	102
5.3.1.3 Konsekvensanalyse	104
5.3 Delkonklusion	106
Konklusion	108
Perspektivering	111
Litteraturliste	113

Kapitel 1

1.1 Indledning

Når der sker hvidvask af penge, er dette ekstremt skadeligt for samfundet.¹ Undersøgelser fra FN viser, at der på verdensplan årligt hvidvaskes penge for mellem to og fem procent af det globale bruttonationalprodukt (omtales herefter BNP).² Anskues problemet på nationalt plan, fremgår det af den nationale risikovurdering fra 2015, at potentialet for hvidvask af penge i Danmark er estimeret til cirka 20,6 mia. DKK.³

Hvidvask af penge finder blandt andet sted gennem pengeinstitutter.⁴ Der er set eksempel på, at hvidvask af penge er sket gennem Danske Bank⁵, hvoraf dette udløste massiv mediedækning. Gennem denne massive mediedækning af denne hvidvask-sag er samfundets borgere blevet mere oplyste, når det kommer til hvidvask af penge gennem bankerne, samt hvordan dette påvirker samfundet.

I et forsøg på at intensivere kampen mod hvidvask af penge og derved beskytte samfundet; herunder den finansielle sektor, udkom der i 2015 et nyt Hvidvaskdirektiv⁶ (omtales herefter 4AMLD) fra Den Europæiske Union (omtales herefter EU).⁷ Et andet beskyttende udspil fra EU, Databeskyttelsesforordningen⁸ (omtales herefter GDPR), udkom i 2016. Denne forordnings formål er at beskytte medlemsstaternes borgeres personoplysninger.⁹

Det ses ved disse to regelsæt, at de hver især søger at beskytte individuelle samfundsmæssige hensyn. Ved 4AMLD betragtes en politisk holdning til, at bankerne skal overvåge deres kunder i kampen mod

¹ Statsadvokaten, "Hvidvask i Danmark, Den nationale risikovurdering 2018", side 3.

² United Nations Office on Drugs and Crime "Money-Laundering and Globalization".

³ Statsadvokaten, "Den nationale risikovurdering 2015" side 1.

⁴ Statsadvokaten, "Hvidvask i Danmark, Den nationale risikovurdering 2018", side 7.

⁵ Bruun & Hjejle, "Rapport om non-resident porteføljen i Danske Banks estitiske filial", 19. september 2018.

⁶ Europa-Parlamentets og Rådets direktiv (EU) 2015/849 af 20. maj 2015.

⁷ Statsadvokaten, "Hvidvask i Danmark, Den nationale risikovurdering 2015", side 8.

⁸ Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016.

⁹ jf. GDPR, artikel 1, stk. 1.

hvidvask af penge¹⁰, mens GDPR har sit fokus på, at borgernes privatliv skal beskyttes; blandt andet fra denne slags overvågning.¹¹

Hvordan kan de danske banker i deres kamp mod hvidvask af penge, samtidig sikre beskyttelse af deres kunders personoplysninger?

1.2 Problemstilling

Problemstillingen i denne afhandling tager sit afsæt i ovenstående indledning. Afhandlingens formål er at analysere forholdet mellem de danske banker og deres fysiske kunder, hvor bankerne er efter 4AMLD blevet pålagt at skulle foretage aktive tiltag for at bekæmpe hvidvask af penge.¹² Disse tiltag består efter 4AMLD artikel 18, stk. 1, blandt andet i udførelse af skærpede kundekendskabsprocedurer, som kræver indsamling og behandling af bankens kunders personoplysninger. Ydermere består disse tiltag i, at bankerne skal overvåge deres kunders bankaktiviteter, jf. 4AMLD artikel 18, stk. 2.

Foruden disse tiltag, som bankerne skal foretage efter 4AMLD, er bankerne pålagt at skulle yde beskyttelse af deres kunders personoplysninger, jf. GDPR artikel 3, stk. 1. Bankerne har efter GDPR artikel 6, stk. 1, litra c og e hjemmel til at behandle deres kunders personoplysninger ved de tiltag, som er blevet pålagt dem at udføre efter 4AMLD. Omend bankerne har behørig behandlingshjemmel, fritages de ikke for ansvaret om at skulle sikre sig, at de ved indsamlingen og behandlingen af deres kunders personoplysninger, ikke overtræder GDPR's principper for dataminimering. Dataminimeringen består af en række principper som bankerne ved behandling af kundernes personoplysninger skal sikre at overholde uagtet, at der foreligger behørig behandlingshjemmel.¹³ Dataminimeringens principper har til formål at sikre, at al indsamling og behandling skal være relevant, tilstrækkeligt og begrænset til, hvad der må anses for nødvendigt set i forhold til formålet, jf. GDPR artikel 5, stk. 1, litra c.

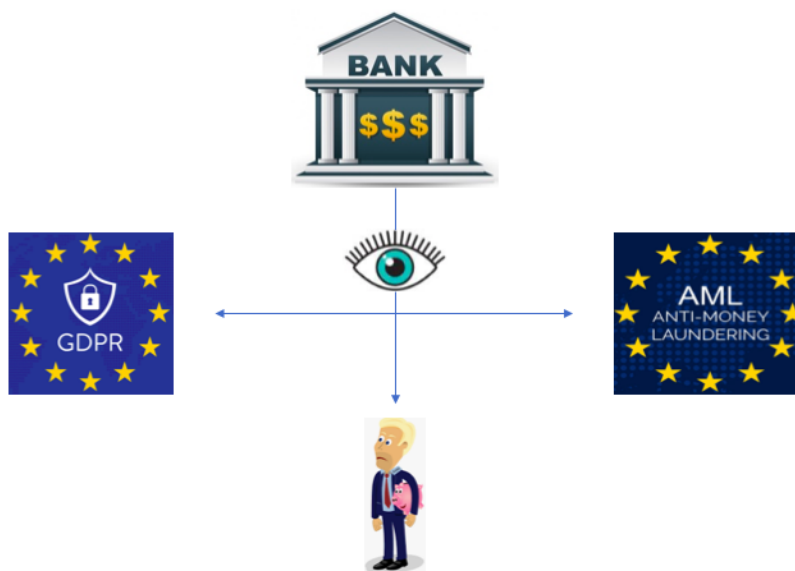
¹⁰ Jf. 4AMLD artikel 18, stk. 2.

¹¹ Justitsministeriet, betænkning nr. 1565, "Betænkning om databeskyttelsesforordningen (2016/679) - og de retlige rammer for dansk lovgivning", Del 1, bind 1, side 9.

¹² Jf. 4AMLD artikel 2, stk. 1, nr. 2.

¹³ Datatilsynet, "Hvad er dine forpligtelser".

Afhandlingen tager sit udgangspunkt i ovenstående to hensyn. Det ønskes undersøgt, om disse to hensyn, som illustreret ved figur 1, trækker bankerne i hver sin retning. Herved om dataminimeringen i GDPR påvirker bankernes udførelse af de tiltag, som de skal foretage i kampen mod hvidvask af penge.



Figur 1. Egen tilvirkning.¹⁴

For at skabe afklaring omkring dette, foretages der en juridisk analyse, hvor gældende ret analyseres, og hensynene bag 4AMLD og GDPR opstilles og sammenholdes. Efter den juridiske analyse vil det blive analyseret, hvad der er den mest økonomisk effektive løsning i bankernes kamp mod hvidvask af penge, samt hvorledes de kan tilrettelægge overvågningen af deres kunder. Afsluttende vil samspillet mellem den juridiske analyse og den økonomiske analyse opstilles. Her vil resultatet af den økonomiske analyse blive holdt op mod beskyttelsesprincipperne i dataminimeringen i GDPR. Dette sker med henblik på at kunne udlede, om dataminimeringen påvirker bankernes bekæmpelse af hvidvask af penge, og hvis dette er tilfældet, om det er muligt at finde frem til løsningsforslag, der er effektive.

¹⁴ Jf. litteraturliste

1.2.1 Problemformulering

I denne afhandling ønskes følgende hovedproblemformulering, som også udgør den integrerede problemformulering, besvaret:

I hvilken grad påvirker beskyttelsen i dataminimeringen efficiensen af den skærpede kundekendskabsprocedure, som bankerne skal foretage ved bekæmpelse af hvidvask af penge?

For at kunne besvare hovedproblemformuleringen, opstilles en juridisk og en økonomisk problemstilling.

1.2.2 Juridisk problemstilling

I hvilken grad påvirker dataminimeringen i Databeskyttelsesforordningen udførelsen af den skærpede kundekendskabsprocedure?

1.2.3 Økonomiske problemstilling

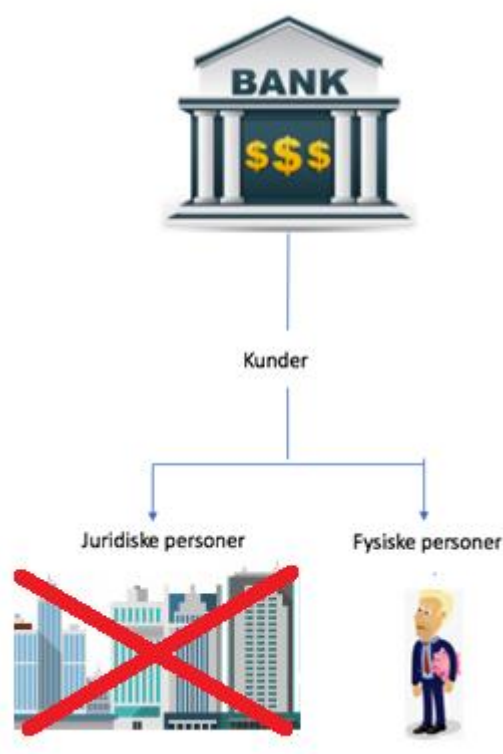
Hvorvidt er det muligt, på efficient vis, at påvirke den asymmetriske information, der foreligger mellem bankerne og kunderne ved bankernes bekæmpelse af hvidvask af penge?

1.3 Synsvinkel og afgrænsning

Denne afhandling vil blive belyst og behandlet ud fra de danske bankers synsvinkel og der afgrænses hermed for behandling af andre finansielle institutter. Bankernes synsvinkel er valgt, da afhandlingens problemstilling betragter bankernes behandling. Kommissionens eller kundernes perspektiv kunne også have været interessant at behandle, men afhandlingen afgrænses til udelukkende at være ud fra bankernes synsvinkel.

Som belyst ved figur 1, har afhandlingen udelukkende fokus på fysiske kunder, som handler på egne vegne og i eget regi. Derfor afgrænser afhandlingen sig fra at omfatte juridiske erhvervskunder; eksempelvis virksomheder.

4AMLD omfatter både hvidvask af penge og finansiering af terror, hvorfor det primære fokus for afhandlingen vil bestå i hvidvask af penge. Finansiering af terror kan forekomme som statuering af eksempler i afhandlingen, men vil ikke blive behandlet yderligere. Derudover afgrænses der fra GDPR og 4AMLD's regler angående opbevaring og sletning af personoplysninger.



Figur 2. Egen tilvirkning.¹⁵

I denne afhandling er fokus den skærpede kundekendskabsprocedure, som bankerne pålægges at udføre efter 4AMLD, afdeling 3. Der vil herved blive afgrænset fra andre former for kundekendskabsprocedurer, samt andre tiltag som bankerne er blevet pålagt efter 4AMLD ved bekæmpelsen af hvidvask af penge. Disse vil dog blive inddraget ved relevans.

GDPR artikel 5, stk. 1 litra c, som behandler principperne for dataminimering, er den primære artikel, som afhandlingen behandler i GDPR. Af denne grund vil andre lovregler i forordningen ikke blive behandlet. Disse kan dog blive henvist til ved relevans.

¹⁵ Jf. litteraturliste.

Ved anvendelse af afgørelser fra Datatilsynet, vil der i afhandlingen afgrænses fra anvendelse af historiske afgørelser. Der vil udelukkende blive inddraget afgørelser, som er afsagt efter GDPR's indtræden.

Inddragelsen af spilteori vil blive afgrænset til, at der kun anvendes modeller, som omhandler non-verifiable information samt Signaling og Screening spil. Herved afgrænses der fra behandling af andre spilteoretiske modeller.

1.4 Metode

Afhandlingen vil tage sit afsæt i følgende juridiske, økonomiske og integrerede metoder.

1.4.1 Juridisk metode

Den bagvedliggende grund for metodevalget er, at ved benyttelse af disse metoder, vil der være mulighed for at analysere lovteksterne og de bagvedliggende tekster med formålet om at udvinde den konkrete betydning. Den juridiske metode anvendes med henblik på at kunne tage stilling til afhandlingens retlige problemstilling, samt hvilken påvirkning problemstillingen har i det praktiske retsliv.¹⁶

1.4.1.1 Retsdogmatisk metode

Ved benyttelse af den retsdogmatiske metode vil den gældende ret og regulering henholdsvis systematiseres, beskrives og analyseres.¹⁷

Ved anvendelse af den retsdogmatiske metode, er domstolene og andre juridiske personer underlagt at følge en bestemt systematik for løsningen af juridiske problemstillinger. For at en retsdogmatisk analyse kan anses som værende korrekt og gyldig, skal den juridiske metode følges. Årsagen til dette er, at hvis alle juridiske problemer løses efter samme metode, vil alle afgørelser nå til samme resultat,

¹⁶ Tvarnø, Christina D. og Nielsen Ruth, "Retskilder & Retsteorier", 4. udgave, 2014, side 56.

¹⁷ Ibid. side 30.

fordi alle således har den samme forståelse og fortolkningsstil.¹⁸ Den retsdogmatiske systematik udspiller sig i et hierarki, som følger dette hierarki; 1) Lovregulering, 2) Retspraksis, 3) Retssædvaner og sidst i hierarkiet 4) Forholdets natur.¹⁹

1.4.1.2 EU-retlig fortolkning

Fortolkning af EU-regulering sker blandt andet ved benyttelse af subjektiv fortolkning, formålsfortolkning (teleologisk fortolkning) og fortolkning med omtanke for helheden af retssystemet.²⁰ Disse fortolkningsmetoder vil anvendes i denne afhandling for at kunne undersøge formålet med bestemmelserne, hvoraf dette bliver foretaget ud fra selve lovteksten og forarbejderne til de relevante bestemmelser.

Det skal ydermere have i mente, at EU-retlige reguleringer findes på mange sprog, og med hjemmel i CILFIT-sagen²¹ er alle sproglige udgaver af det originale affattede sprog lige autentiske.²² Der kan dog forekomme vanskeligheder ved sammenligning af den danske version af GDPR og 4AMLD med andre sproglige udgaver, da kan foreligge forskellige forståelsesnuancer.²³ Af denne grund vil der i afhandlingen kun blive sammenlignet med den engelske udgave.

1.4.1.3 Primær og sekundær regulering

Ved hvidvask af penge er det kapitalens frie bevægelighed,²⁴ der er den primære regulering i denne afhandling. Det skal derfor sikres, at den sekundære regulering, 4AMLD, ikke hindrer kapitalens frie bevægelighed, hvis og når der sker en grænseoverskridende pengeoverførsel på tværs af medlemslandene.

¹⁸ Ibid. side 34.

¹⁹ Tvarnø, Christina D. og Nielsen Ruth, "Retskilder & Retsteorier", 4. udgave, 2014, side 34.

²⁰ Ibid. side 223.

²¹ Sag 283/81, Srl CILFIT og Lanificio di Gavardo SpA mod Ministry of Health.

²² Sag 283/81, Srl CILFIT og Lanificio di Gavardo SpA mod Ministry of Health. Præmis 18.

²³ Tvarnø, Christina D. og Nielsen Ruth, "Retskilder & Retsteorier", 4. udgave, 2014, side 235.

²⁴ jf. TEUF artikel 63.

Udover EU's traktater omfatter den primære regulering rettigheder og almindelige bindende principper²⁵, såsom blandt andet proportionalitetsprincippet.²⁶

De bindende sekundære reguleringer omfatter forordninger, direktiver og afgørelser.²⁷ Denne afhandling vil have fokus på GDPR og 4AMLD, hvilket er den sekundære regulering.

1.4.1.4 Fortolkningsregler

Ved fortolkning af lovteksterne i afhandlingens juridiske analyse, vil der blive anvendt ordlydsfortolkning og formålsfortolkning.

Ordlydsfortolkning anvendes for at udlede lovens sproglige mening og dermed klarlægge, hvad indholdet er i lovteksten.²⁸ Formålsfortolkning benyttes i sammenhæng med ordlydsfortolkningen. Begrundelsen for anvendelsen er at kunne nå frem til lovreglens formål og dermed udlede, hvordan den skal overholdes.

1.4.1.5 Juridisk litteratur

Juridisk litteratur og teori anses ikke for at være retskilder, og der kan derfor ikke støttes ret på disse. Litteraturen og teorien er relevant at anvende i analysen i denne afhandling, da dette er relevant for den juridiske informationssøgning, samt for at kunne fortolke og analysere retskilder i forbindelse med afhandlingens problemformulering.

1.4.1.6. Soft-law

Soft-law kan blandt andet bestå i udtalelser og vejledninger og anses ikke for at være bindende retsakter.²⁹ Det er dog set før, at EU-domstolen har henvist til ikke-bindende retsakter til støtte for sin afgørelse.³⁰ I afhandlingen vil vejledninger og andre former for soft-law blive refereret til og

²⁵ Tvarnø, Christina D. og Nielsen Ruth, "Retskilder & Retsteorier", 4. udgave, 2014, side 119.

²⁶ Ibid. side 139-140.

²⁷ Tvarnø, Christina D. og Nielsen Ruth, "Retskilder & Retsteorier", 4. udgave, 2014, side 141.

²⁸ Blume, Peter "Retssystemet og juridisk metode" 3. udg. 2016, side 299.

²⁹ Tvarnø, Christina D. og Nielsen Ruth, "Retskilder & Retsteorier", 4. udgave, 2014, side 119.

³⁰ Ibid side 144.

analyseret, da dette har relevans for fortolkningen af reguleringen. Årsagen til anvendelsen af vejledninger i denne afhandling er ønsket om at kunne belyse bankernes synspunkt. Vejledningerne er det pågældende tilsyns³¹ guidelines til, hvordan bankerne på behørig vis kan søge at overholde de respektive regelsæt.

1.4.2 Økonomisk metode

1.4.2.1 Neoklassisk teori

Neoklassisk teori anvendes som et introducerende redskab i denne afhandling, hvor formålet er at belyse afhandlingens økonomiske problemstilling. Den Neoklassiske teori anvendes til at belyse, hvordan den økonomiske situation burde se ud under de opstillede forudsætninger. Den neoklassiske teori bygger på, at der på markedet er perfekt information, perfekte markeder og at produktet og parterne på markedet er homogene.³² Derudover forudsættes det, at der ikke findes ind- og udgangsbarrierer.³³

Neoklassisk teori bygger på en deduktiv tilgang. Ved et deduktivt ræsonnement tages der udgangspunkt i bestemte udsagn, hvor logikken tilbyder en række slutningsregler, hvis de opstillede udsagn er sande.³⁴

1.4.2.2 Spilteori

For at vurdere kundernes risiko for hvidvask af penge gennem bankerne, opstilles et Bayesian spil. Dette er et spil, som opstilles med antagelsen om, at bankerne har inkomplet information om kunderne, hvormed der herefter anvendes Bayes' regel, når kunderne forsøger at overføre informationer. Bayes' regel har den formodning, at rationelle personer antages at opdatere deres holdninger og tro på baggrund af den nye information.³⁵

³¹ Der er her tale om Finanstilsynet for 4AMLD, og Datatilsynet for GDPR.

³² Knudsen, Christian "Økonomisk Metodologi Bind 2 - Virksomhedsteori og Industriøkonomi" 2. Udg. 1997, side 56.

³³ Ibid.

³⁴ Knudsen, Christian "Økonomisk Metodologi Bind 1 - Videnskabsteori & Forklaringstyper" 2. Udg. 2017, side 58.

³⁵ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 83.

Der vil, baseret på Bayesian spillet, opstilles ingen, en eller flere pooling og separate ligevægte. Disse har til formål at udlede teser, som forventes at kunne oplyse om, hvorvidt kunderne skal anlægges en mistanke om hvidvask af penge eller ikke. Spillet operer med to kundetyper, kriminelle kunder og ikke-kriminelle kunder. Den eller de pooling ligevægte, der søges at finde, skal belyse de situationer, hvor begge kundetyper vælger samme strategi i en given situation. Det forhold, at begge kundetyper vil benytte samme strategi i en given situation bevirker, at bankerne ikke kan udlede noget om disse kunders type. De separate ligevægte, der søges at finde, skal belyse de situationer, hvor kundetyperne benytter sig af forskellige strategier i en given situation.³⁶ Det vil her være muligt for bankerne at udlede noget om, hvilken type kunderne er, baseret på deres strategi i den givne situation.

Baseret på de eventuelt opstillede pooling og separate ligevægte, kan det udledes, hvorvidt der er tale om, at spillet har en perfekt Bayesian ligevægt eller ej. Ordet perfekt illustrerer idéen om, at overbevisninger og handlinger er i overensstemmelse med hinanden.³⁷ Med udgangspunkt i dette antages det, at begge kundetyper handler rationelt og ikke har incitament til at afvige fra de udledte pooling og separate ligevægte. Findes det, at en af kundetyperne har incitament til at afvige fra de udledte pooling og separate ligevægte, vil der dermed ikke være tale om, at det opstillede spil, har en perfekt Bayesian ligevægt.

Ovenstående spilteori anvendes kortfattet i afhandlingens økonomiske analyse i en mere introducerende form. Formålet er, på baggrund af det opstillede spil, at åbne op for den økonomiske analyse til anvendelse som et udgangspunkt til den senere belysning af den retsøkonomiske tilgang i den integrerede analyse.

Ved den økonomiske analyse vil der blive benyttet Signaling og Screening modeller. Ved at benytte Signaling og Screening modeller, opstilles der et spil, hvor den ene part besidder privat information, som ikke kan verificeres af hverken den anden part eller af en tredjemand.³⁸ Det er relevant at opstille dette spil for at besvare den konkrete problemstilling. Spillet opstilles med formålet om at kunne udlede, om der forefindes en mulighed, hvorpå bankerne kan kende forskel på de kriminelle kunder og de ikke-kriminelle kunder.

³⁶ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 83.

³⁷ Ibid. side 84.

³⁸ Ibid. 122.

Ved et Signaling og Screening spil kan det ikke vides med sikkerhed, om parten har incitament til at fortælle sandheden, eller ikke har incitament til dette. Ved et Signaling spil kan parten, som besidder informationen, søge at overbringe informationer til den anden part ved at signalere, hvilken type parten er.³⁹ I forlængelse af at parten vil signalere informationer om, hvilken type parten er, skal den anden part derfor søge at screene parten med henblik på at udlede informationer, som den anden parts handlinger afslører.⁴⁰ Som nævnt kan det dog ikke vides, om de informationer der forsøges overbragt, er sande eller ikke er sande, samt om disse bliver opfanget korrekt af den part som screener. Her er der tale om, at bankerne skal foretage en korrekt screening af kunderne for at kunne vurdere, om disse udgør en risiko for hvidvask af penge.

1.4.2.3 Principal-agent teorien

Til at besvare den økonomiske problemstilling, benyttes Principal-Agent teorien (omtales herefter P/A teorien). Ved anvendelse af denne teori vil fokus være på forholdet mellem bankerne og deres kunder, og den asymmetriske information, der foreligger imellem dem.⁴¹ Det antages, at både bankerne og kunderne handler ud fra et subjektivt, men rationelt grundlag.

Ved P/A teorien inddrages de teoretiske begreber Adverse Selection og Moral Hazard. Adverse Selection vil blive benyttet til at søge at løse den asymmetriske information, der knytter sig til ex ante tidspunktet, hvor Moral Hazard søger at løse den asymmetriske information ved ex post tidspunktet.⁴²

1.4.3 Integreret metode

Tilblivelsen af den integrerede analyse udarbejdes efter en retsøkonomisk tilgang. Denne tilgang benyttes til at udlede, hvilken økonomisk efficiens de gældende retsregler har i et samfundsmæssigt perspektiv, dette gennem en analyse af de gældende retsregler i en økonomisk kontekst.⁴³ Begrebet efficiens er kernebegrebet inden for den retsøkonomiske metode, hvilket hermed tager sit afsæt i, at

³⁹ Ibid. 123.

⁴⁰ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 123.

⁴¹ Knudsen, Christian "Økonomisk metodologi bind 2 - virksomhedsteori og industriøkonomi" 2. Udg. 1997, side 164.

⁴² Ibid. side 167.

⁴³ Tvarnø, Christina D. og Nielsen Ruth, "Retskilder & Retsteorier", 4. udgave, 2014, side 484.

det forudsættes, at samfundets ressourcer allokeres ud til de områder, hvor de findes mest efficiente.⁴⁴ Ved anvendelse af den retsøkonomiske metode, vægter det samlede positive resultat, som tiltagene tilsammen måtte give, mere end de enkelte enheder, der måtte tabe på det udførte tiltag.⁴⁵

Den integrerede analyse tager sit udgangspunkt i den økonomiske analyse, hvor spilteori er anvendt til opstilling af et Screening og Signaling spil. Dette er med formålet om at besvare afhandlingens overordnede problemformulering, hvorfor de økonomiske betragtninger sættes i relation til den juridiske analyse, sammenholdt med det samfundsmæssige hensyn. Screening og Signaling spillets resultat opstilles med formålet om at udlede en retsøkonomisk forståelse af forskellen mellem den juridiske og økonomiske analyse.

Det endelige mål for den integrerede analyse er at besvare afhandlingens overordnede problemformulering.

1.5 Kildekritik

Til at søge teori er fagbøger, hjemmesider, artikler og generel internetsøgning blevet anvendt.

Ved valg af inddragede artikler og hjemmesider har vi forholdt os kritiske til både afsender udgivelsesår, involverede parter, synsvinkel og formålet for materialet. Endvidere har vi forholdt os kritiske til det forhold, at artikler kan være skrevet som partsindlæg.

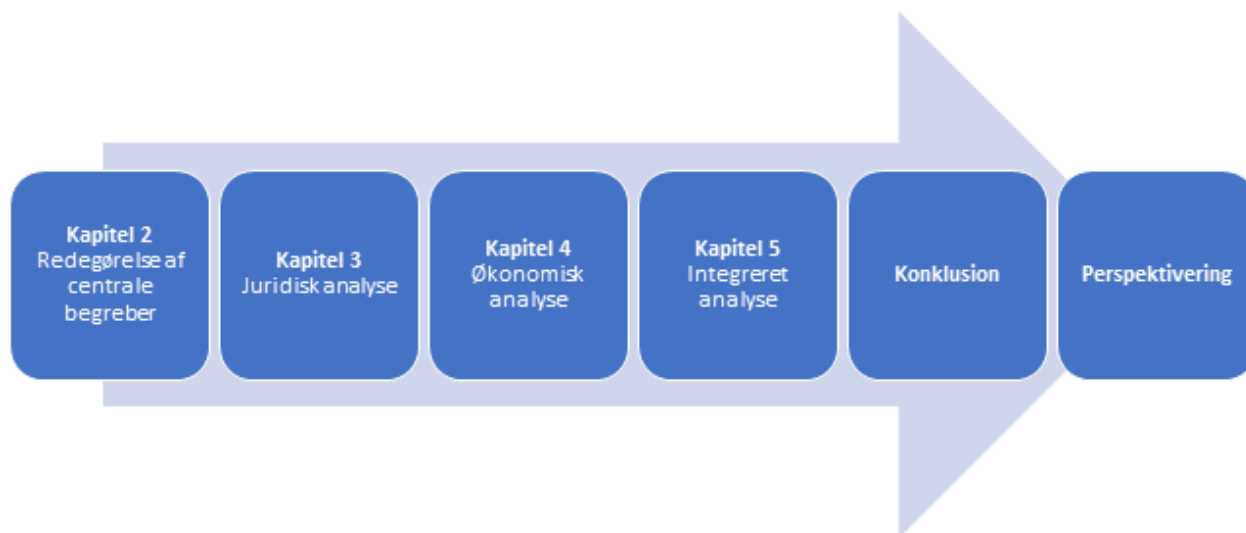
De anvendte fagbøger er skrevet af anerkendte forfattere inden for fagområdet. Ved udvælgelsen af de juridiske fagbøger, har udgivelsesåret været en væsentlig faktor. De regelsæt, som er afhandlingens primære fokus, er fra henholdsvis 2015 og 2016, hvilket stiller krav til, at de fagbøger som anvendes i afhandlingens juridiske del, også skal være af nyere dato. Dette skyldes, at de således har fokus på nuværende gældende ret og heraf ikke en forældet ret.

⁴⁴ Skovbo, Eva A. ”Advokaten 1 – Bør advokater forstå sig på retsøkonomi?” Advokat Samfundet, 2004.

⁴⁵ Ibid.

1.6 Struktur

Afhandlingen er struktureret ud fra kapitler som vist i figur 3, hvor hvert kapitel indledes med en kort indledning, og afsluttes med en delkonklusion.



Figur 3. Egen tilvirkning

Kapitel 2 redegør for de centrale begreber, som vil blive benyttet i afhandlingen. De centrale begreber omfatter: *hvidvask af penge, den risikobaserede tilgang, kundernes risikogrupper i bankerne, kundekendskabsprocesserne samt dataminimeringen.*

Kapitel 3 omfatter den juridiske analyse, hvilken har til formål at besvare den juridiske problemformulering. I dette kapitel analyseres gældende ret inden for 4AMLD og GDPR; herunder belyses den skærpede kundekendskabsprocedure og dataminimeringen, hvorefter de holdes op mod hinanden.

Kapitel 4 opstiller den økonomiske analyse omhandlende, hvorvidt det er muligt at påvirke den informationsasymmetri, der foreligger mellem bankerne og kunderne. I analysen opstilles et Bayesian spil, hvor det søges om informationsasymmetrien, kan løses ved et Signaling og Screening spil samt ved benyttelse af P/A teori.

Kapitel 5 indbefatter den integrerede analyse, hvilken tager udgangspunkt i den juridiske og økonomiske analyse, som er foretaget i kapitel 3 og 4. På baggrund af dette søges det at udlede en løsning, som er efficient for samfundet, men samtidig er forenelig med GDPR. Løsningen har til

formål at analysere den retsøkonomiske forståelse, og hvad der betragtes som efficient med henblik på at besvare problemformuleringen.

Kapitel 2

Formålet med dette kapitel er at redegøre for de mest centrale begreber, som anvendes i afhandlingen. Dette gøres med formålet om at give læseren en dybere forståelse af de begreber der benyttes.

2.1 Definition af hvidvask af penge

Den juridiske definition af hvidvask af penge fordrer, at et forhold kan kategoriseres som hvidvask af penge, jf. 4AMLD artikel 1, stk. 3, når:

- der konverteres eller overføres formuegoder, såfremt man har viden om, at disse er erhvervet ved en strafbar lovovertrædelse
- det forties eller tilsløres, hvorfra formuegodet har sin oprindelse, karakter, lokalisering, disposition, ejendomsret eller bevægelse. Dette med viden om, at formuegodet er erhvervet ved en strafbar lovovertrædelse
- der erhverves eller besiddes formuegoder, hvor det er kendt ved modtagelsen af disse, at de er erhvervet ved en strafbar lovovertrædelse
- der er tale om medvirken til anskaffelsen af disse goder.

Hvidvask af penge sker hyppigst gennem en proces bestående af tre aktiviteter: 1) Placement, 2) Layering og 3) Legitimation. Ved første aktivitet sker placeringen af formuegodet. Dette kan eksempelvis ske ved placering af finansielle midler på en bankkonto. Herefter sker der layering, hvilket forbindes med processen, hvor formuegodet flyttes rundt i det finansielle system, hvortil formuegodet i sidste ende forbindes til en legitim organisation. Formålet med layering er at maskere formuegodet, så det ikke er muligt at spore det tilbage til den fysiske person. Ved sidste og tredje aktivitet sker der en legitimation, hvor formuegodet kan benyttes uden, at dette kan spores tilbage en strafbar lovovertrædelse.⁴⁶ Det har ikke relevans, hvor der geografisk set er sket hvidvask af penge, jf. 4AMLD artikel 1, stk. 4.

Ved hvidvask af penge kan det økonomisk anskues som, at der sker en udvanding af samfundets BNP. Det anses således fordi samfundsøkonomien svindles for manglende finansielle midler i form af manglende indbetaling af skat, når der sker hvidvask af penge.

⁴⁶ Chapman, Rose “Anti-Money Laundering A Practical Guide To Reducing Organizational Risk” 1. udgave, 2018, side 2

2.2 Definition af den risikobaserede tilgang

I denne afhandling vil begrebet og metoden, den risikobaserede tilgang, anvendes hyppigt. Den risikobaserede tilgang vil blive tillagt dette store fokus, da 4AMLD og hvidvaskloven lægger stor vægt på denne tilgang, ved udførelsen af foranstaltningerne til bekæmpelse af hvidvask af penge. Dette belyses blandt andet i 4AMLD artikel 8 og hvidvasklovens § 7.

Ved anvendelse af en risikobaseret metode, fremmes lovgivernes mulighed for at allokere ressourcerne ud til de områder og problemstillinger, hvor risikoen for hvidvask af penge anses for at være størst. Disse risikoområder anskues også som de områder, hvor hvidvask af penge udgør den største negative effekt på samfundet.⁴⁷

2.3 Definition af kundernes risikogrupper i bankerne

Ved forretningsforbindelser i bankerne, skal bankerne ud fra en risikovurdering, allokere deres kunder i risikogrupper. Denne allokering skal ske baseret på, hvor stor en risiko bankerne anser, at der måtte være for, at de pågældende kunder hvidvasker penge gennem bankerne.⁴⁸ Bankerne grupperer kunderne i følgende risikogrupperinger: 1) Begrænset risiko, 2) Almindelig risiko og 3) Øget risiko.⁴⁹ De kunder som grupperes i den begrænsede risikogruppe, er de kunder, hvor bankerne ser mindst mulig risiko for mulig hvidvask af penge. Ved den almindelige risikogruppe, allokeres de kunder, som bankerne ser en almindelig risiko for mulig hvidvask af penge. Og ved den øgede risikogruppe, allokeres de kunder, som bankerne ser som værende den størst mulige risiko for mulig hvidvask af penge. Når kunder allokeres til en bestemt risikogruppe, er der ikke tale om en permanent gruppering. Det kan forekomme under forretningsforbindelsens levetid, at kunderne allokeres til en anden risikogruppe.⁵⁰

⁴⁷ Bounds, Gregory M. og Malyshev, Nikolai, "OECD Reviews of Regulatory Reform Risk and Regulatory Policy: Improving the Governance of Risk" 2010, side 186

⁴⁸ Finanstilsynet "Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven), oktober 2018, side 76

⁴⁹ Ibid. side 77

⁵⁰ Ibid. side 76

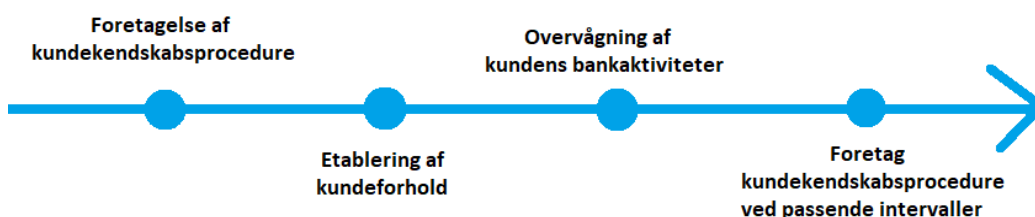
2.4 Definition af kundekendskabsprocedurerne

Fokus i denne afhandling er på den skærpede kundekendskabsprocedure. Denne findes i 4AMLD, afdeling 3. Den skærpede kundekendskabsprocedure anvendes af bankerne med formålet om, at den skal fungere som et redskab i kampen mod hvidvask af penge, hvor den skal kontrollere og begrænse de pågældende risici, der foreligger, jf. 4AMLD artikel 18, stk. 1. I afhandlingens juridiske analyse anvendes den skærpede kundekendskabsprocedure som et vurderingsredskab til at allokere kundernes risiko for mulig hvidvask af penge. I den økonomiske analyse benyttes den skærpede kundekendskabsprocedure som et redskab for bankerne til at skelne mellem deres kundetyper. Den skærpede kundekendskabsprocedure anvendes nærmere i den økonomiske analyse ved spilteori i et Signaling og Screening spil.

Der eksisterer tre forskellige kundekendskabsprocedurer: 1) Den almindelige kundekendskabsprocedure, 2) Den skærpede kundekendskabsprocedure og 3) Den lempelige kundekendskabsprocedure. Først vil den almindelige kundekendskabsprocedure blive defineret, hvorefter den skærpede kundekendskabsprocedure og den lempelige kundekendskabsprocedure vil blive defineret med afsæt i den almindelige kundekendskabsprocedure.

Bankerne skal foretage en almindelig kundekendskabsprocedure af deres kunder ved følgende forhold: 1) Ved etablering af en ny forretningsforbindelse, 2) Hvis en kundes relevante oplysninger ændrer sig, og 3) Ved andre passende tidspunkter i forretningsforbindelsen levetid. Derudover skal den almindelige kundekendskabsprocedure foretages ved en række yderligere tilfælde; ved enkelte stående transaktioner (over et vist beløb), ved mistanke om mulig hvidvask af penge eller hvis der opstår tvivl om hvorvidt de indhentede personoplysninger om en kunde er korrekte, jf. 4AMLD artikel 11, sammenholdt med hvidvasklovens § 10.

En kundekendskabsprocedure skal følge denne proces gennem forretningsforbindelsens levetid, jf. 4AMLD artikel 11:



Figur 4. Egen tilvirkning

Der findes ikke en lovbestemt metode, hvorved kundekendskabsproceduren ved passende intervaller skal foretages, og det er derfor bankerne, der internt skal udarbejde interne politikker angående dette, hvilke skal være tiltænkt ud fra en risikobaseret tilgang.⁵¹ Når kundekendskabsproceduren foretages, kan det være relevant for bankerne, som supplement til den almindelige kundekendskabsprocedure, at foretage skærpede kundekendskabsprocedurer af den deres kunder. Dette kan eksempelvis være relevant, hvis denne kunde, på baggrund af den almindelige kundekendskabsprocedure, udviser øget risiko for hvidvask af penge. I dette tilfælde er det påkrævet, at den pågældende bank skal foretage en skærpet kundekendskabsprocedure af denne kunde.⁵²

Udover den almindelige kundekendskabsprocedure og den skærpede kundekendskabsprocedure, er der den lempelige kundekendskabsprocedure. Bankerne kan foretage lempelige kundekendskabsprocedurer af deres kunder, hvis de ud fra en konkrete vurdering, har identificeret kunderne til kun at udgøre en begrænset risiko for hvidvask af penge, jf. 4AMLD artikel 15 sammenholdt med hvidvasklovens § 21. Modsat påkravet, som bankerne er underlagt i forhold til at foretage skærpede kundekendskabsprocedurer ved øgede risikokunder, er bankerne ikke pålagt at skulle foretage lempede kundekendskabsprocedurer af deres kunder, når disse alene udviser en begrænset risiko for hvidvask af penge, jf. 4AMLD artikel 18 sammenholdt med hvidvasklovens § 21.

De skærpede kundekendskabsprocedurer anvendes for, at bankerne kan vurdere, om deres kunder kunne udgøre eller fortsat udgør en øget risiko med henblik på at hvidvaske penge.⁵³ I 4AMLD artikel 18, er det nærmere bestemt, hvornår bankerne skal foretage skærpede kundekendskabsprocedurer af deres kunder. De skal foretage skærpede kundekendskabsprocedurer af deres fysiske kunder ved blandt andet to på forhånd fastlagte forhold; hvis en kunde er etableret i et af de tredjelande, som Kommissionen har identificeret som et højrisikotredjeland⁵⁴ eller hvis en kunde har status som en politisk eksponeret person⁵⁵ (omtales herefter PEP), jf. 4AMLD artikel 18, stk.1. Udover disse to forhold, skal bankerne foretage skærpede kundekendskabsprocedurer ved højrisikotilfælde, som de

⁵¹ Finanstilsynet "Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven), oktober 2018, side 50

⁵² Ibid. side 78

⁵³ Ibid.

⁵⁴ Kommissionens delegerede forordning (EU) 2016/1675, bilag, højrisikotredjelande.

⁵⁵ Definitionen på en PEP i 4AMLD artikel 3, stk. 9.

identificerer, jf. 4AMLD artikel 18, stk. 1. Når bankerne skal vurdere, om de finder, at der foreligger høj risiko for hvidvask af penge hos deres kunder, skal de som minimum kigge på de minimumsfaktorer, der er oplistet i 4AMLD bilag III, jf. 4AMLD artikel 18, stk. 3.

Såfremt det er muligt og er inden for rimeligheden af bankernes råderum, er bankerne pålagt at skulle undersøge baggrund og formål med alle komplekse og usædvanlige store transaktioner hos deres kunder. Dette gælder ligeledes for transaktionsmønstre, som bankerne anser for at være usædvanlige, og som ikke har et klart påviseligt økonomisk eller lovligt formål, jf. 4AMLD artikel 18, stk. 2. For at kunne afgøre, om der er tale om en af de nævnte situationer, er den bagvedliggende intention, at bankerne skal foretage overvågning af deres kunders forretningsforbindelser.⁵⁶

2.5 Definition af dataminimering

GDPR omfatter som hovedregel de dataansvarlige myndigheder og virksomheder, som har oprindelsesland i blandt andet Danmark; herunder de danske banker. De danske banker omfattes af GDPR's regler, når de er etableret i Danmark og behandlingen af deres kunders personoplysninger foretages i et af medlemslandene i EU. Endvidere finder GDPR's regler anvendelse for bankerne, når behandlingen består i overvågning af deres kunders færden og adfærd i Danmark.⁵⁷

Dataminimering findes i GDPR artikel 5, stk. 1, litra c, og er et af de grundlæggende principper i forordningen, som bankerne skal overholdes ved behandling af deres kunders personoplysninger.⁵⁸ De tre principper, der tilsammen danner begrebet dataminimering er, at behandling af personoplysninger skal være tilstrækkelige, relevante og begrænsede til, hvad der er nødvendigt for at tjene det formål, som personoplysningerne skal anvendes til.⁵⁹

GDPR artikel 5, stk. 1, litra c:

1. Personoplysninger skal:

c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (>dataminimering«)

⁵⁶ COM(2013) 45 Final, side 35.

⁵⁷ Erhvervsstyrelsen, Justitsministeriet, Digitaliseringsstyrelsen og Datatilsynet, "Vejledning til databeskyttelsesforordningen" Oktober 2017. Side 5.

⁵⁸ Ibid. side 10.

⁵⁹ jf. GDPR artikel 5, stk. 1, litra c.

Kapitel 3

Det ses, at der har været sager, hvor banker ikke har formået at overholde 4AMLD's regler i en sådan grad, der kunne anses for tilstrækkelig. Eksempelvis udpensles det i Bruun & Hjejles rapport,⁶⁰ vedrørende en sag om Danske Bank, at der foreligger en problemstilling i forhold til, at bankerne kan stå i en situation, hvor at det kan være problematisk at efterleve 4AMLD's regler vedrørende kundekendskabsprocedurerne.

Formålet med dette kapitel er, ved hjælp af den juridiske analyse, at belyse i hvilken grad dataminimeringen i GDPR påvirker bankernes udførelse af den skærpede kundekendskabsprocedure. Denne analyse vil bestå i fortolkning af formålsbetragtningerne for de to regelsæt, 4AMDL og GDPR, for derefter at stille dem op mod hinanden. Endvidere vil det blive analyseret, hvad gældende ret er, og i hvilken grad det er muligt for bankerne at foretage den skærpede kundekendskabsprocedure efter, at der er sket etablering af en forretningsforbindelse. For at klarlægge bankernes mulighed for at udføre disse procedurer, analyseres der, med henvisning til afsnit 2.4, hvad der ved den skærpede kundekendskabsprocedure kræves af organisering og omfang.

Efter analyse af den almindelige kundekendskabsprocedure, herunder den skærpede kundekendskabsprocedure, vil dataminimeringens principper i GDPR blive analyseret. Dette er med formålet om at kunne vurdere, hvilken grad dataminimeringen påvirker udførelsen af den skærpede kundekendskabsprocedure.

Afsluttende i dette kapitel vil det blive vurderet, om det er muligt ud fra Datatilsynets relevante afgørelser at udlede noget, der kan bidrage til besvarelse af den juridiske problemformulering.

3.1 Formålsfortolkning af 4AMLD og GDPR

Kapitlet tager sit udgangspunkt i formålsfortolkningen af 4AMLD og GDPR. Formålet for regelsæt skal findes i de respektive præambelbetragtninger.

⁶⁰ Bruun & Hjejle, "Rapport om non-resident porteføljen i Danske Banks estiske filial" 19. September 2018.

Det overordnede formål med 4AMLD findes i præambelbetragtning nr. 1. Ved en formålsfortolkning kan det udledes, at 4AMLD har til hensigt at forhindre, at ikke-lovligt tjente finansielle midler skal skade den finansielle sektors integritet, stabilitet og omdømme. Ydermere søger 4AMLD at forhindre, at hvidvask af penge skal udgøre en trussel mod det indre marked og hindre fremgangen i den internationale udvikling. Disse formål vil direktivet søge opnået ved, at 4AMLD skal fungere som et redskab, der skal medvirke til at forhindre, at hvidvask af penge sker på EU-plan.⁶¹

For at forhindre, at hvidvask af penge skal udgøre en trussel mod det indre marked, har 4AMLD til hensigt, at komplicerede forhold forenkles på tværs af landegrænserne i medlemsstaterne.⁶² Bestemmelserne i 4AMLD består af vid fleksibilitet i henhold til medlemslandenes nationale regler, således at det er muligt for medlemslandet at tilpasse de risici og trusler, der måtte forekomme for hvidvask af penge.⁶³

Det ses både i præambelbetragtningerne samt i forarbejderne til 4AMLD, at 4AMLD følger de anbefalinger, som er fastlagt af Financial Action Task Force (omtales herefter FATF). Anbefalingerne er fulgt med formålet om at kunne bekæmpe hvidvask af penge på den mest effektive måde, både på EU og internationalt plan.⁶⁴ ⁶⁵ Den skærpede kundekendskabsprocedure er blandt andet skabt ud fra anbefalingerne fra FATF.⁶⁶ Årsagen til at 4AMLD følger FATF's anbefalinger på området, er begrundet i, at hvidvask af penge og finansiering af terrorisme foregår internationalt, og derfor bør EU også følge FATF's anbefalinger, da disse anses som det førende internationale organ for bekæmpelse af hvidvask og finansiering af terrorisme.⁶⁷

4AMLD tager hensyn til de internationale foranstaltninger for bekæmpelse af økonomisk kriminalitet, hvilket er med henblik på, at bekæmpelsen sker effektivt.

⁶¹ Jf. 4AMLD, præambelbetragtning nr. 1.

⁶² COM(2013) 45 Final, side 2.

⁶³ Ibid.

⁶⁴ Jf. 4AMLD, præambelbetragtning nr. 3 og 4.

⁶⁵ COM(2013) 45 Final, side 3.

⁶⁶ Ibid. side 14.

⁶⁷ Ibid.

GDPR har til formål at beskytte fysiske personer i forbindelse med behandling af disses personoplysninger.⁶⁸ Dette formål består ud fra den betragtning, at beskyttelse af fysiske personers personoplysninger er en grundlæggende rettighed.⁶⁹ GDPR's formål er at kunne bidrage til at skabe en union med frihed, sikkerhed og retfærdighed, men også en økonomisk union, hvor der skal ske konvergens mellem økonomien på det indre marked og for fysiske personers velfærd.⁷⁰ Dette har, med afsæt i den hastige teknologiske udvikling, skabt et behov for skærpet databeskyttelse ved behandling af personoplysninger.⁷¹ GDPR har til hensigt at skabe en mere ensartet beskyttelsesramme i alle EU's medlemslande. Dette er medvirkende til, at kunderne, i forbindelse med den hastige teknologiske udvikling, vil kunne finde tryghed i, at deres personoplysninger er beskyttede mod unødvendig behandling.⁷²

Retten til beskyttelse af fysiske personers personoplysninger består i, at de har ret til, at deres personoplysninger ikke behandles til unødvendige formål.⁷³ Det forhold, at beskyttelsen består i en grundlæggende rettighed bevirker, at der ikke er tale om en absolut, men i stedet, at denne ret skal ses i sammenhæng med den funktion, som beskyttelsen har i samfundet. Ydermere skal retten afvejes i forhold til andre grundlæggende rettigheder, der oplistet i chartret⁷⁴ samt i forhold til proportionalitetsprincippet.⁷⁵

Sammenlignes formålene med de to regelsæt, kan det klarlægges, at de har til formål at beskytte to forskellige hensyn i samfundet. 4AMLD har til formål at beskytte det indre marked mod hvidvask af penge,⁷⁶ mens GDPR har til formål at beskytte fysiske personers rettigheder ved behandling af disses personoplysninger.⁷⁷ Det kan klarlægges, at der i henhold til GDPR's formål er råderum til, at forordningen skal kunne beskytte det indre markedes økonomi, idet at den tilsigter at skabe en konvergens mellem økonomien og beskyttelsen af personoplysninger.⁷⁸

⁶⁸ Jf. GDPR præambelbetragtning nr. 2.

⁶⁹ Jf. Den Europæiske Unions charter om grundlæggende rettigheder (2012/C 326/02), artikel 8, stk. 1.

⁷⁰ Jf. GDPR præambelbetragtning nr. 2.

⁷¹ Betænkning nr. 1565 del I, bind 1. Justitsministeriet, Rosendahl's a/s. Side 9

⁷² Ibid.

⁷³ Den Europæiske Unions charter om grundlæggende rettigheder, (2012/C 326/02), artikel 8, stk. 1 og 2.

⁷⁴ Den Europæiske Unions charter om grundlæggende rettigheder, (2012/C 326/02)

⁷⁵ Jf. GDPR præambelbetragtning nr. 4.

⁷⁶ Jf. 4AMLD præambelbetragtning nr. 2.

⁷⁷ Jf. GDPR præambelbetragtning nr. 1.

⁷⁸ Jf. GDPR præambelbetragtning nr. 2.

3.2 Den skærpede kundekendskabsprocedure

Bankerne pålægges efter 4AMLD at skulle foretage kundekendskabsprocedurer ved flere tidspunkter i forretningsforbindelsens levetid, jf. 4AMLD artikel 11, stk. 1, litra a-f. Kundekendskabsproceduren skal bankerne foretage ved etablering af en forretningsforbindelse, ved relevante ændringer samt på andre passende tidspunkter i forretningsforbindelsens levetid. Der vil altid være tale om etablering af en forretningsforbindelse, når en kunde opretter en konto hos en bank, eller på anden vis bliver oprettet som kunde i en bank, jf. hvidvasklovens § 3, nr. 3.⁷⁹

En relevant ændring kunne eksempelvis bestå i, at den pågældende kunde får status som en PEP, eller hvis pågældende kunde til- eller fraflytter Danmark.⁸⁰ Ved en relevant ændring, skal bankerne tage stilling til disse ændringer ud fra en risikovurdering. Her skal bankerne vurdere, om det er nødvendigt, at de indsamler nye oplysninger om den pågældende kunde.⁸¹ Formålet med kundekendskabsproceduren ved disse relevante ændringer er, at bankerne skal sikre, at de oplysninger, som besidder om den pågældende kunde, til stadighed er tilstrækkelige og korrekte, jf. GDPR artikel 11, stk. 1, litra f.

Når bankerne skal foretage kundekendskabsprocedurerne ved passende tidspunkter angår dette, at de skal foretages med passende intervaller i forretningsforbindelsens levetid.⁸² Passende interval er intervaller, som bankerne selv fastsætter ud fra en subjektiv vurdering, jf. 4AMLD artikel 11 sammenholdt med hvidvasklovens § 10.⁸³

Bankerne skal skærpe deres fokus på kunder, som udgør en øget risiko for hvidvask af penge.⁸⁴ For at bankerne kan vurdere, om kunderne muligvis udgør en øget risiko for hvidvask af penge, skal de internt have foretaget en risikobaseret analyse af deres egen forretningsplan med formålet om at kunne vurdere sin risikoprofil. Baseret på den risikobaserede analyse, skal bankerne udarbejde interne

⁷⁹ Finanstilsynet, "Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven)", 2018, side 49.

⁸⁰ Ibid. side 50.

⁸¹ Ibid. side 49-50.

⁸² Ibid. side 50.

⁸³ Ibid.

⁸⁴ Ibid.

politikker og procedurer. Disse politikker og procedurer skal omhandle bankernes tilgang til etablering af nye forretningsforbindelser.⁸⁵

I 4AMLD artikel 18, stk. 1, er der på forhånd fastsat to forhold, som bevirker, at kunderne skal allokeres som øgede risikokunder. Ved disse kunder, skal bankerne udføre skærpede kundekendskabsprocedurer som supplement til de før omtalte, normalt udførte kundekendskabsprocedurer. Disse to forhold består i kunder fra på forhånd fastslåede højrisikotredjelande og PEP-kunder. Disse højrisikotredjelande, er lande, som består på baggrund af FAFT's anbefalinger og Kommissionens egen identifikation. FAFT har identificeret en række tredjelande til at udgøre en høj risiko for hvidvask af penge. Identifikationen består på baggrund af en metodisk tilgang, hvorpå det er vurderet på landenes strategiske mangler i forhold til bekæmpelse af hvidvask. Disse mangler kan eksempelvis være relateret til landets lovgivning, hvortil dette udgør en øget trussel for den finansielle infrastruktur i EU.⁸⁶ Kommissionen har ved deres identifikation valgt at følge samme metodiske tilgang som FAFT.⁸⁷ Baggrunden for denne liste af højrisikotredjelande er at beskytte det finansielle system for risikoen for hvidvask af penge, som forekommer fra disse bestemte tredjelande.⁸⁸ På nuværende tidspunkt består listen af 11 tredjelande, som er identificeret som højrisikotredjelande.⁸⁹

Det andet på forhånd fastsatte forhold vedrører kunder, der har status som en PEP, jf. 4AMLD artikel 18, stk. 1. En PEP er defineret som en politisk eksponeret person, der har et særligt tillidshverv, hvoraf denne person anses som eventuelt mere disponibel over for korruption og bestikkelse.⁹⁰ Definitionen af en PEP er stort set enstemmig i hele EU, kun afbrudt af enkelte forskelle, da ikke alle medlemslande har indrettet sig på samme måde.⁹¹ En PEP vil i Danmark, blandt andet være den danske statsminister, ministre, parlamentsmedlemmer og højesteretsdommere.⁹² De personer som anses for at være PEP-

⁸⁵ The Wolfsberg Group "The Wolfsberg Group, ICC and BAFT Trade Finance Principles" 2017, side 16.

⁸⁶ SWD(2018) 362 Final, "Commission staff working document methodology for identifying high risk third countries under directive (EU)2015/849" side 10.

⁸⁷ Ibid.

⁸⁸ Jouroá, Vêra "Anti-Money Laundering: EU list of high-risk third countries" 2019, side 1.

⁸⁹ Kommissionens delegerede forordning (EU) 2016/1675, bilag, højrisikotredjelande.

⁹⁰ Finanstilsynet, "Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven)" side 80.

⁹¹ Ibid.

⁹² Ibid. side 87.

kunder, er oplistet i Finanstilsynets PEP-liste⁹³, og bankerne kan her finde frem til, hvem de skal kategorisere som værende PEP. Udover disse personer, som er oplistet i PEP-listen, er nærtstående familiemedlemmer og nære samarbejdspartnere til en PEP, også omfattet af reglerne for en PEP, jf. 4AMLD artikel 3, nr. 10 a-c og artikel 23.

Når bankerne skal foretage skærpede kundekendskabsprocedurer ved PEP-kunder, er dette af en forebyggende karakter og skal ikke sidestilles med, at PEP-kunderne er kriminelle. Det er således ikke i overensstemmelse med 4AMLD og FATF's anbefalingerne at afvise PEP-kunder, alene på baggrund, at de har status som en PEP.⁹⁴ Hvis bankerne etablerer en forretningsforbindelse med en PEP, skal der tages rimelige foranstaltninger. Bankerne skal foretage en udvidet risikovurdering af PEP-kunderne for at vurdere, om de kunne være disponible for at misbruge bankerne til hvidvask af penge eller blive bestukket hertil.⁹⁵ Efter risikovurderingen skal den bankerne indhente godkendelse hos sin hvidvaskansvarlige⁹⁶. Den hvidvaskansvarlige i den pågældende bank, skal give sin godkendelse til, at der kan ske etablering forretningsforbindelsen eller eventuelt fortsætte forretningsforbindelsen med denne PEP, antaget at en kunde skifter fra at være en almindelig kunde til at være en PEP-kunde.⁹⁷ Efter der er sket etablering af PEP-kunder eller fortsættelsen af deres forretningsforbindelse, skal bankerne træffe specifikke foranstaltninger. Disse foranstaltninger består i, at bankerne skal holde øje med PEP-kundernes formues oprindelse samt opretholde vedvarende skærpede overvågning med PEP-kundernes bankaktiviteter. Dette med formålet om at vurdere, om der kunne være tale om usædvanlige transaktioner. En usædvanlig transaktion kan eksempelvis bestå af en transaktion af en vis størrelse eller hvis der er noget usædvanligt knyttet til afsender eller modtager.

Den risikovurdering som bankerne som nævnt skal foretage af PEP-kunderne skal indebære en vurdering af, om der er risiko for, at PEP-kundernes nærtstående eller nære samarbejdspartnere kunne være disponible for at misbruge bankerne til hvidvask af penge.⁹⁸

⁹³ Finanstilsynet "PEP-liste" oprettet 29. dec. 2017, opdateret 10. maj. 2019.

⁹⁴ jf. 4AMLD præambelbetragtning nr. 33.

⁹⁵ Finanstilsynet, "Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven)", side 83.

⁹⁶ Hvidvasklovens § 7, stk. 2.

⁹⁷ Finanstilsynet, "Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven)", side 86.

⁹⁸ Ibid. side 87.

Den vedvarende skærpede overvågning, som bankerne skal foretage af PEP-kunderne bevirker, at bankerne skal udføre kundekendskabsprocedurer ved PEP-kunder oftere end, hvad normen er ved almindelige risikokunder. Der foreligger her mere skærpede vilkår for, hvornår en transaktion skal undersøges nærmere, og bankerne vil oftere finde det nødvendigt at indhente dokumentation for PEP-kunders transaktioner. Den skærpede overvågning af PEP-kunderne kan ske via samme system, som bankerne anvender ved andre forretningsforbindelser i den øgede risikogruppe. Overvågningen skal dog være proportional set i forhold til den risikovurdering, som bankerne har foretaget af PEP-kunderne. Dette vil sige, at jo højere risiko bankerne vurderer at de pågældende PEP-kunder udgør, desto mere skal overvågningen af de pågældende skærpes.⁹⁹ Hvis en PEP fratræder stillingen, som bevirker statussen som PEP, skal den pågældende kunde ikke længere skal have status som en PEP i bankerne. Ved en sådan situation, skal bankerne i de efterfølgende 12 måneder fortsat vurdere, hvilken risiko denne pågældende kunde indebærer,¹⁰⁰ samt om der fortsat foreligger en øget risiko for hvidvask af penge forbundet med denne kunde, jf. 4AMLD artikel 22.

Udover de to på forhånd fastlagte krav for udførelse af skærpede kundekendskabsprocedurer; forretningsforbindelser med PEP-kunder og forretningsforbindelser fra bestemte højrisikotredjelande, findes der ikke en udtømmende liste over hvilke situationer der medfører, at der skal udføres skærpede kundekendskabsprocedurer. Det er derfor op til bankerne individuelt at vurdere, ud fra en risikobaseret tilgang, i hvilke tilfælde de skal sikre, at de i deres forretningsforbindelse ikke misbruges til hvidvask af penge.¹⁰¹ Derudover skal det bemærkes, at der findes utallige af forskellige risici, hvor enkelte risici kan stå alene eller flere risici, tilsammen kan øge eller mindske den samlede risiko.¹⁰² Det er i dette tilfælde, at bankernes interne risikovurderinger af egen forretningsplan er relevante. Disse er relevante, da bankerne her har vurderet, hvor deres risici for at blive udnyttet til hvidvask af penge ligger. Ved udførelsen af disse risikovurderinger vil dette give bankerne en dybere forståelse af hvilke situationer, der medfører, at en skærpede kundekendskabsprocedurer skal udføres, samt hvornår det kan vurderes, at kunderne udgør en øget risiko for hvidvask af penge.

⁹⁹ ”Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven)”, side 90.

¹⁰⁰ COM(2013) 45 final, side 37.

¹⁰¹ COM(2013) 45 final, side 78.

¹⁰² jf. 4AMLD præambelbetragtning nr. 30.

Når bankerne skal vurdere, om deres kunder skal allokeres som øgede risikokunder, skal de som minimum forholde sig til de oplistede faktorer i 4AMLD bilag III, jf. 4AMLD artikel 18, stk. 3. I bilag III er der oplistet en række minimumsfaktorer, som kan være medvirkende til at identificere, om kunderne udgør øgede risici for hvidvask af penge. Idet at der er tale om minimumsfaktorer, er der lagt op til, at bankerne selv skal foretage en vurdering af yderligere forhold, som kunne være medvirkende til at identificere, om kunderne kunne udgøre en øget risiko. Minimumsfaktorerne er kategoriseret i; 1) Kunderisikofaktorer, 2) Risikofaktorer i forbindelse med produkter, tjenesteydelser, transaktioner eller leveringskanaler og 3) Geografiske risikofaktorer. Disse kategoriseringer kan give bankerne en indikation om hvilke informationer, som de skal forholde sig til for at vurdere kundernes risiko på behørig vis.

3.2.1 Personoplysninger ifølge hvidvaskdirektivet og hvidvaskloven

Bankerne skal vurdere på om deres kunders risici er forandrede efter etableringen af forretningsforbindelsen er sket. Dette skal ske ved at foretage vedvarende overvågning og indsamling af deres kunders personoplysninger i forbindelse med den skærpede kundekendskabsprocedure.

Ved indsamling af kundernes personoplysninger, skal dette ske i overensstemmelse med reglerne efter 4AMLD artikel 41, stk. 1-4 sammenholdt med hvidvasklovens § 16, stk.1 og 2. Det understreges her, at behandling af personoplysninger efter direktivet, omfatter al behandling af personoplysninger efter hvidvaskdirektivet, underlagt direktivet 95/46/EF¹⁰³. Dette har den betydning, at al indsamling og behandling af personoplysninger som hovedregel skal være i overensstemmelse med de regler, som GDPR fastsætter.¹⁰⁴ Derudover er det klarlagt i 4AMLD artikel 41, stk. 2, at der kun må indsamles og behandles personoplysninger på baggrund af dette direktiv, hvis det er med henblik på forebyggelse af hvidvask af penge og finansiering af terror. Med henvisning til denne artikel, er det vigtigt for bankerne, at det ikke er enhver form for personoplysninger, som må indsamles. Årsagen til dette er, at hvis der er tale om personoplysninger, som ikke er begrænsede til kun at opfylde

¹⁰³ Databeskyttelsesdirektivet fra 1995, som nu er blevet erstattet med databeskyttelsesforordningen (GDPR)

¹⁰⁴ ”Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven)”, side 97.

formålet om at forebygge hvidvask af penge, vil der være risiko for, at behandlingen anses som en ulovlig indsamling af personoplysninger. Det er derfor væsentligt for bankerne, at de kan klarlægge, hvilke oplysninger, der er vigtige at indsamle og behandle for at opfylde formålet.

Når bankerne skal udføre kundekendskabsprocedurer, skal de informere kunderne om, hvorfor der indsamles personoplysninger om den pågældende.¹⁰⁵ Denne forpligtelse kan have betydning for bekæmpelsen af hvidvask af penge, idet at bankerne her informerer kunderne om formålet for indsamlingen. Dette kan have den konsekvens, at kunderne kan afgive falske oplysninger, hvis der eksempelvis er tale om en kunde, som foretager hvidvask af penge. Dette forhold, at bankerne skal oplyse deres kunder om formålet for indsamlingen, modarbejder dermed formålet ved kundekendskabsproceduren, herunder den skærpede kundekendskabsprocedure.

Ved foretagelse af kundekendskabsprocedurerne, hvortil bankerne skal indsamle personoplysninger til udførelsen af denne, er det som nævnt ovenfor vigtigt, at informationerne er begrænsede til kun at omfatte, hvad der er relevant for formålet. Bankerne skal ved indsamling og behandling tage hensyn til de grundlæggende rettigheder og principper, som er oplistet i charteret. Det er nævnt i 4AMLD, at selvom dette direktiv er udarbejdet efter FATF's anbefalinger, har kommissionen tilpasset direktivet, således at det er i overensstemmelse med EU-retten. Dette gælder især, når det vedrører GDPR og beskyttelsen af personers grundlæggende rettigheder. Det er dog vigtigt, at indsamling og behandling efter 4AMLD er tilladt, men det bør være med respekt for de grundlæggende rettigheder.¹⁰⁶ Betydningen af dette er, at ved indsamling af kunders personoplysninger, skal bankerne også respektere dataminimeringen, både fordi denne er behandlet i GDPR, men også fordi at dataminimeringen er bygget op omkring proportionalitetsprincippet.

Det nævnes eksplicit i 4AMLD præambelbetragtning nr. 65, at bankerne skal respektere personers privatliv og familieliv samt retten til beskyttelse af deres personoplysninger. På baggrund af dette skal bankerne derfor navnlig tage hensyn til disse rettigheder ved indsamling og behandling af deres kunders personoplysninger. Dette er især væsentligt, når bankerne skal vurdere kunders risiko på baggrund af en konkret vurdering. Her er skal bankerne sikre, at vurderingerne foretages på baggrund af personoplysninger, som de forinden har sikret, er relevante. Vurderingen er endvidere vigtig for

¹⁰⁵ ”Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven)”, side 98.

¹⁰⁶ 4AMLD præambelbetragtning nr. 43.

bankernes indsamling, idet bankerne her får fastlagt, hvor langt de kan strække sig ved indsamlingen og behandlingen set i forhold til formålet. Det kan derfor klarlægges, at det er lovligt, at bankerne indsamler og behandler personoplysninger, så længe det er i fuld overensstemmelse med ovennævnte rettigheder, samt at indsamlingen og behandlingen kun anvendes til de formål, som 4AMLD påkræver; herunder kundekendskabsproceduren.¹⁰⁷ I samme præambelbetragtning, belyses det, at behandling af personoplysninger skal begrænses til kun at omfatte det, som er nødvendigt for at opfylde formålet. Det er derfor også her påkrævet, at bankerne, med afsæt i en subjektiv vurdering, skal klarlægge, hvad de betragter som værende nødvendigt for at opfylde formålet. Finder bankerne, at mistanke om mulig hvidvask af penge hos kunderne kan bekræftes, skal bankerne indberette mistanken til Hvidvasksekretariatet, herunder til SØIK, hvorfra de undersøger mistanken nærmere.¹⁰⁸

Som nævnt i 4AMLD er bekæmpelse af hvidvask af penge i samfundets interesse og 4AMLD pålægger bankerne tiltag, som de skal udføre for at bekæmpe hvidvask af penge. På baggrund af dette har bankerne efter GDPR artikel 6, stk. 1, litra c og e lovhjemmel til behandling af deres kunders personoplysninger. At bankerne har hjemmel til behandling af personoplysningerne, fritager dem ikke fra at skulle sikre, at deres behandling sker med overholdelse af GDPR artikel 5, stk. 1, litra c, og i overensstemmelse med de grundlæggende rettigheder.

3.3 Dataminimeringen i GDPR's artikel 5, stk. 1, litra c

Principperne i GDPR artikel 5 omhandler overordnet set god databehandlingsskik.¹⁰⁹ Principperne i GDPR er højere rangeret i hierarkiet end de resterende artikler i forordningen. Hvis der forekommer tvivl hos bankerne, om hvorledes lovreglerne i GDPR skal fortolkes, falder man tilbage på principperne i artikel 5.¹¹⁰ Årsagen til dette er, at principperne er udarbejdet med afsæt i den primære EU-ret, hvortil artiklerne i forordningen er sekundær ret. Er bankerne yderligere i tvivl om fortolkning af artiklerne, kan de søge råd og vejledning hos Datatilsynet.¹¹¹

¹⁰⁷ 4AMLD præambelbetragt nr. 43.

¹⁰⁸ Finanstilsynet "Indberetninger til SØIK" oprettet 8. juli 2009, opdateret 7. november 2018.

¹⁰⁹ Justitsministeriet "Betænkning om databeskyttelsesforordningen (2016/679) - og de retlige rammer for dansk lovgivning" del 1, bind 1, side 81.

¹¹⁰ KHF Jura, "Persondataforordningen, en vejledning om de nye regler for ikke-jurister", www.persondatavejledning.dk side 24.

¹¹¹ Erhvervsstyrelsen, Justitsministeriet, Digitaliseringsstyrelsen og Datatilsynet, "Databeskyttelsesforordningen, en introduktion til de kommende, nye regler om beskyttelse af personoplysninger" Oktober 2017, side 10.

Som udledt ved formålsfortolkningen af GDPR, er forordningens formål at beskytte kundernes personoplysninger. Dette hensyn skal bankerne, ved behandling af kundernes personoplysninger, sikre at overholde.¹¹² Afhandlingens primære fokus i GDPR er dataminimeringen, som er reguleret i GDPR artikel 5, stk. 1, litra c. De principper som foreskrives efter dataminimeringen, pålægger bankerne, at den indsamling og behandling de foretager af kundernes personoplysninger, skal være tilstrækkelig, relevant og begrænset til, hvad der er nødvendigt for formålet.¹¹³

3.3.1 Ordlydsfortolkning af dataminimeringens principper

Ordet relevant i bestemmelsen anvendes i forhold til, at det kun er de relevante personoplysninger, som må behandles i forhold til at kunne realisere formålet for indsamlingen. Det vil sige, at bankerne ikke må indsamle personoplysninger med argumentation i, at det kan være dem nyttigt at besidde disse, men at det ikke fandtes nødvendigt til at efterkomme behandlingsformålet.¹¹⁴ At personoplysningerne irrelevante relaterer sig til, at de også skal være tilstrækkelige. Tilstrækkeligheden gælder også, selvom de ekstra oplysninger er relevante, så må personoplysningerne ikke indsamles, fordi formålet kunne opfyldes uden disse ekstra personoplysninger.¹¹⁵

Den danske version af GDPR artikel 5, stk. 1, litra c har følgende ordlyd (egne understregninger):

“c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (»dataminimering«)”

Efter den danske version af GDPR artikel 5, stk. 1, litra c, kan der forekomme tvivl om, hvorledes ordet “tilstrækkeligt” og “relevant” bør fortolkes. Ved ordet tilstrækkelig kan der være tale om, at

¹¹² Erhvervsstyrelsen, Justitsministeriet, Digitaliseringsstyrelsen og Datatilsynet, “Databeskyttelsesforordningen, en introduktion til de kommende, nye regler om beskyttelse af personoplysninger” Oktober 2017, side 10.

¹¹³ Blume, Peter, “Den nye persondataret” 1. Udg. 2016, Jurist- og Økonomforbundets forlag. Side 66.

¹¹⁴ Blume, Peter “Den nye persondataret forordning 2016/679 om databeskyttelse lov 502/2018 om databeskyttelse” 2018, side 91.

¹¹⁵ Ibid.

omfanget skal være tilstrækkeligt, hvilket henviser til mængden af indsamlet data. Derudover kan der være tale om en kvalitetsmæssig tilstrækkelighed. Det fremgår ikke tydeligt i den danske version, hvorledes begreberne skal fortolkes, af denne grund anvendes den engelske version som medvirke i fortolkningen. Ordlyden af de to versioner synes ikke at være af videre betydning. Den engelske version af GDPR artikel 5, stk.1, litra c, lyder som følgende (egne understregninger):

“(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);”

Som det ses, er den engelske version relativt identisk med den danske version. Ordet relevant oversættes direkte til samme ord på dansk; relevant. Det ord som muligt kan anses for at være forskellig i sin oversættelse, er ordet ”adequate”, som anvendes i den engelske udgave, hvor i den danske version bruges ordet tilstrækkelig. Ordet ”adequate” oversættes fra engelsk til dansk til at kunne betyde ”tilstrækkelig/passende”. ”Tilstrækkelig” kan som nævnt defineres med udgangspunkt i flere aspekter alt afhængig af konteksten. Ordet ”tilstrækkelig” kan sættes i sammenhæng med beskrivelsen en af mængde, hvorimod ordet ”passende” nærmere beskriver en kvalitet. Ordet kan også have en betydning af tilfredsstillende/dækkende, når det skal beskrive en definition.¹¹⁶ Det kan fastslås ved fortolkning af den engelske version at ordet ”tilstrækkelig” bruges med formålet om at beskrive en mængde; “... *limited to what is necessary*”¹¹⁷. Begrebet ”limited” anses for at sætte en begrænsning i mængden i forhold til, hvad der må anses som nødvendigt. Det kan udledes, at både den danske og den engelske version begge er uklare. Det kan ud fra en ordlydsfortolkning, at begrebet ”tilstrækkelig” anvendes i forhold til mængden af indsamlede personoplysninger, skal være begrænset til at være tilstrækkelige.

Ordlydsfortolkningen af dataminimeringens principper bidrager til at fastslå, at bankerne skal begrænse behandlingen af kunders personoplysninger. Behandlingen må kun omfatte, hvad der er nødvendigt for det specifikke formål, og at principperne således har til formål at begrænse behandlingen af personoplysninger mest muligt.¹¹⁸ Det skal hertil nævnes, at “behandling af

¹¹⁶ Axelsen, Jens “Engelsk-Dansk Ordbog”, 13 udg. Gyldendal, 2003.

¹¹⁷ GDPR, artikel 5, stk. 1, litra c.

¹¹⁸ Datatilsynet 2007-42-0049 “Vedrørende monitorering og logning af 1-1 kommunikation på www.arto.com”

personoplysninger” omfatter enhver form for håndtering af personoplysninger; herunder blandt andet indsamling, registrering og søgning.¹¹⁹

3.3.2 Fortolkning af dataminimerings principper

Baseret på en subjektiv vurdering hos bankerne, vurderer bankerne om behandling kan anses for at være lovlydig og dermed forenelig med forordningen. Bankerne skal hermed foretage den subjektive afvejning med formålet om at sikre, at de opfylder betingelserne for lovlig behandling efter GDPR artikel 5, stk. 1, litra c.¹²⁰ For at foretage en lovlig behandling af kundernes personoplysninger, skal der ske efterlevelse af dataminimeringen.¹²¹ Kunderne sikres herved, at behandling af deres personoplysninger ikke sker på et ufuldstændigt grundlag.

Behandlingen efter dataminimering er underlagt proportionalitetsprincippet. Bankerne skal anvende en proportionalitetsvurdering, for at sikre at indsamlingen af personoplysninger er proportional, set i forhold til mistanken om kundernes risiko for hvidvask af penge. Endvidere skal bankerne ved en proportionalitetsvurdering sikre sig, at samme resultat ikke ville kunne opnås ved at benytte mindre indgribende midler;¹²² herunder en mindre mængde personoplysninger eller af mindre følsom karakter. Kan det udledes af bankernes proportionalitetsvurdering, at bankerne ikke har overholdt proportionalitetsprincippet, er behandlingen ikke sket i overensstemmelse med forordningen, hvorfor den derfor ikke kan anses for at være udført på et lovligt grundlag. Hvis der bliver statueret tvivl om, hvorvidt bankerne har overholdt proportionalitetsprincippet eller ej, er det i dette tilfælde bankerne, som skal kunne påvise, at det er et krav, at der skulle ske behandling af pågældende kundes personoplysninger.¹²³ Kan bankerne ikke fremvise dokumentation for, at behandlingen er proportional i forhold til deres mistanke, og kunne behandlingen være sket på mere lempelig vis, findes behandlingen ikke i overensstemmelse med proportionalitetsprincippet. Det er ikke lovligt at bankerne tilsidesætter dataminimering og indsamler yderligere personoplysninger, på baggrund af en

¹¹⁹ Erhvervsstyrelsen, Justitsministeriet, Digitaliseringsstyrelsen og Datatilsynet, “Databeskyttelsesforordningen, en introduktion til de kommende, nye regler om beskyttelse af personoplysninger” Oktober 2017, side 9.

¹²⁰ Blume, Peter “Den nye persondataret”, 1. Udg. 2016, Side 66.

¹²¹ Erhvervsstyrelsen, Justitsministeriet, Digitaliseringsstyrelsen og Datatilsynet, “Databeskyttelsesforordningen, en introduktion til de kommende, nye regler om beskyttelse af personoplysninger” Oktober 2017, side 10.

¹²² Kromann Reumert “Den nye databeskyttelsesforordning start jeres compliance-tjek med disse 6 trin”.

¹²³ Blume, Peter “Den nye persondataret forordning 2016/679 om databeskyttelse lov 502/2018 om databeskyttelse” 2018, side 92.

formodning, at behandlingen vil være nemmere at udføre ved besiddelse af disse. Bankerne skal efter GDPR artikel 30, føre fortegnelser over deres behandlingsaktiviteter. Bankerne skal kunne dokumentere hensynet og formålet ved behandling af personoplysninger.

Ydermere skal behandling være nødvendig for formålet, dette for at skabe tryghed hos kunderne. Kunderne kan med afsæt i denne rettighed sikre sig at behandling af deres personoplysninger kun anvendes til opfyldelse af behandlingsformålet og ikke yderligere end det. På denne vis sikrer kunderne sig, at bankerne ikke besidder personoplysninger om dem, som eventuelt kunne være ugunstige for dem. Det kan udledes af GDPR's præambelbetragtning nr. 39, at hvis bankerne finder, at behandling kan udføres på et mere lempeligt grundlag, skal bankerne forfølge denne mere lempelige tilgang. Udfører bankerne ikke behandlingen med denne mere lempelige tilgang, anses behandlingen ikke for at være begrænset til, hvad der er nødvendigt for forfølgelsen af mistanken om hvidvask af penge hos kunderne.

Afhandlingen ønsker at undersøge, hvilke påvirkninger dataminimeringen pålægger udførelsen af de skærpede kundekendskabsprocedurer. Hertil er det situationen, hvor bankerne har en mistanke og skal undersøge denne nærmere.¹²⁴ Bankerne skal ved forfølgelsen af mistanken, sikre at behandlingen er i overensstemmelse med GDPR artikel 5, stk. 1, herunder særligt for vores afhandling, litra c. Bankerne skal, som nævnt ovenfor, vurdere den konkrete situation sammenholdt med mistanken og ud fra denne proportionalitetsvurdering vurdere, om behandlingen vil være i forenelig med GDPR artikel 5, stk. 1, litra c.¹²⁵

3.4 GDPR's påvirkninger for 4AMLD

Ved bankernes udførelse af kundekendskabsprocedurerne, skal bankerne ved hver procedure vurdere, hvilke personoplysninger der skal indsamles, behandles og om dette er proportionalt i henhold til formålet.¹²⁶

¹²⁴ Finanstilsynet, "Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven), oktober 2018, side 53.

¹²⁵ Kromann Reumert "Den nye databeskyttelsesforordning start jeres compliance-tjek med disse 6 trin", januar 2018.

¹²⁶ Ibid.

Det synes vanskeligt for bankerne at skulle leve op til begge lovregler. 4AMLD kræver, at der indsamles så mange personoplysninger som muligt, for at udarbejde en korrekt og fyldestgørende kundekendskabsprocedure, således at kundernes risikoprofil vurderes korrekt. GDPR begrænser omfanget af behandlingen af personoplysninger i forhold til behandlingsformålet.

Afsnittet søger at analysere, hvilke personoplysninger bankerne kan indsamle, og hvordan de skal organisere udførelsen af de skærpede kundekendskabsprocedurer set i forhold til dataminimeringsbegrænsninger. Ved udførelsen af de skærpede kundekendskabsprocedurer, som skal foretages ved passende intervaller i forretningsforbindelsens levetid,¹²⁷ kræver dette, at bankerne har mulighed for at indsamle personoplysninger om kunderne. Dette kan forekomme problematisk, da det kan være ressourcekrævende at vurdere indsamlingen af relevante oplysninger, men det findes også ressourcekrævende for bankerne at skulle vurdere, hvor grænsen går for deres behandling af oplysningerne.

Udover at anvende kundekendskabsproceduren til at fastslå kundernes risiko, kan denne procedure anvendes til at få indblik i kundernes omstændigheder og transaktioner.¹²⁸ Ved brug af denne viden gives bankerne en bedre mulighed for at kunne kategorisere kundernes risikoprofil korrekt.

Som analyseret ovenfor, er bankernes indsamling og behandling af kundernes personoplysninger lovlige, jævnfør GDPR art. 6, stk. 1, litra c og e, i det omfang bankerne er pålagt at skulle udføre behandlingen efter 4AMLD, og såfremt bankerne ved hver behandling sikrer, at behandlingen sker i overensstemmelse med GDPR artikel 5, stk.1, litra c.

3.4.1 Etablering af forretningsforbindelse

Ved etablering af forretningsforbindelser, er bankerne efter hvidvasklovens § 10 sammenholdt med 4AMLD artikel 11, pålagt at skulle udføre de almene kundekendskabsprocedurer. Disse kundekendskabsprocedurer indebærer indsamling af information og identifikation af den potentielle kunde. Der kan derudover forekomme situationer med potentielle kunder, hvor skærpede

¹²⁷ Finanstilsynet, "Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven)", oktober 2018, side 47.

¹²⁸ Cox, Dennis "Handbook of Anti Money Laundering", 2015, side 170.

kundekendskabsprocedurer ydermere kræves udført som supplement til de almene kundekendskabsprocedurer.¹²⁹

De danske banker benytter sig som udgangspunkt af digital oprettelse ved etablering af nye forretningsforbindelser frem for et personligt møde. Dette er endog kun udgangspunktet, hvis der er tale om en dansk statsborger. Er kunderne, der ønsker at etablere sig i bankerne, ikke danske statsborgere, men fra et andet medlemsland eller fra et tredjeland, vil et personligt fremmøde i bankerne før etableringen være påkrævet.¹³⁰ Der kan argumenteres for, at hvis de danske banker benyttede sig af et personligt fremmøde ved alle etableringer af nye forretningsforbindelser, ville dette være mere effektivt i forhold til bekæmpelse af hvidvask af penge.

Ifølge GDPR artikel 22, stk. 1, har kunderne som hovedregel, ret til ikke at være genstand for afgørelser, som alene er baseret på en automatisk behandling. Herunder er der tale om profilering, hvor dette vil medføre retsvirkning eller tilsvarende betydeligt vil påvirke kunderne. Der findes endog en række undtagelser for denne hovedregel. Undtagelsen som kunne have været relevant set i lyset af afhandlingens problemstilling, er GDPR artikel 22, stk. 2, litra b, hvor profilering er lovligt, såfremt det er hjemlet i EU-retten eller i medlemsstaternes nationale ret. Denne undtagelse finder dog ikke anvendelse i dette tilfælde, da den relevante lovgivning i denne afhandling er 4AMLD, hvorfor bankerne er pålagt ikke at skulle foretage behandling ud fra profilering, men hvor behandling i stedet skal ske ud fra en subjektiv vurdering. Der henvises herved tilbage til hovedreglen om, at profilering ikke er lovligt. Baggrunden for at profilering efter hovedreglen ikke anses som værende lovlig behandling af personoplysninger fra bankernes side er, at kunderne vil blive genstand for en afgørelse, hvorved bankerne grupperer kunderne, som er henholdsvis begrænset risiko kunder og øget risiko kunder. Det ses derfor, at bankerne ikke kan benytte sig af undtagelsen til hovedreglen, hvorfor det vil være ulovligt for de danske banker at anvende generaliserede spørgsmål, ved udførelsen af deres kundekendskabsprocedure.

Påstanden om at et personligt fremmøde ved etableringen af en forretningsforbindelse, findes effektiv er begrundet i at medarbejderne i bankerne, ved dette møde kan foretage en subjektiv vurdering af kunderne. Den subjektive vurdering ved mødet, vil resultere i effektiv udførelse af

¹²⁹ Finanstilsynet, "Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven)", oktober 2018, side 78.

¹³⁰ Viden indsamlet ved telefonsamtale med Nordea og Danske Bank.

kundekendskabsproceduren og efterlevelse af princippet om dataminimering. Vurderingen foretages på baggrund af kundernes adfærd og svar på medarbejdernes spørgsmål. På denne måde vil der ikke være tale om generaliserede spørgsmål, men derimod vil det bero på en subjektiv vurdering af kunderne, hvilken medarbejderen personligt foretager. Herved vil det under dette personlige møde være muligt for bankernes medarbejder at sikre overholdelse af principperne i dataminimeringen. Hvis det findes nødvendigt, kan medarbejderen straks udvide proceduren til en skærpet kundekendskabsprocedure.

3.4.2 Igangværende forretningsforbindelse

3.4.2.1 Den vedvarende overvågning

Ved en igangværende forretningsforbindelse er det et påkrav efter 4AMLD artikel 13, stk. 1, litra d sammenholdt med hvidvasklovens § 11, stk. 1, nr. 5, at bankerne skal foretage vedvarende overvågning af deres kunder. Denne overvågning skal omfatte overvågning af kundernes ud- og indgående transaktioner, kundernes adfærd, herunder hvilke aktiviteter, som kunderne foretager, der involverer bankerne og som er synlige for bankerne via for eksempel den almindelige kontakt som bankerne har med kunderne.¹³¹

Formålet med bankernes udførelse af overvågningen er, at 4AMLD pålægger bankerne at sikre, at der er overensstemmelse mellem kundernes bankaktiviteter og den risikogruppe, bankerne har vurderet, at kunderne tilhører, baseret på den tidligere foretagne risikovurdering.¹³² Dette med henblik på, at bankerne konstant er opmærksom på risikoen for mulig mistanke om hvidvask af penge.

Bankerne skal tilrettelægge overvågningen således, at den findes passende i forhold til den enkelte kundes forhold. Ændrer kundernes forhold sig, herunder kundernes historisk og bankernes allerede eksisterende kendskab til kunderne, skal bankerne justere på overvågningen, således at den konstant er overensstemmende med kundernes forhold.¹³³

¹³¹ Finanstilsynet, "Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven)", oktober 2018, side 68.

¹³² Ibid.

¹³³ Ibid.

Hvis bankerne kan anses for at have en mere simpel forretningsmodel, må bankerne gerne udføre overvågningen med den procedure inden for henholdsvis risikogrupper. Dog henviser hvidvaskvejledningen til, at finansielle institutter, som anses for at have en simpel forretningsmodel er “...f.eks. en pengeoverførselsvirksomhed, der har samme kundetyper og kun overfører penge til et geografisk område.”¹³⁴ De banker, som er genstand for denne afhandling, anses ikke for at have en simpel forretningsmodel, udelukkende med argumentation i den ovenstående definition på en simpel forretningsmodel. De overførsler, der finder sted i de banker, som afhandlingen omfatter, antages ikke kun at vedrøre en enkelt kundetype, eller udelukkende kun at involvere pengeoverførsler til et enkelt geografisk område. De omtalte banker anses derfor ikke, for at må udføre denne standard overvågning. Bankerne er, efter 4AMLD artikel 13, stk. 1, litra d, pålagt at skulle holde dokumenter, data og oplysninger om kunderne ajourført, og hvis det anses nødvendigt for det formål, har bankerne efter denne artikel hjemmel til at måtte undersøge midlernes oprindelse, jf. 4AMLD artikel 13, stk. 1, litra d.

Som nævnt i afsnit 3.2, skal bankerne efter hvidvasklovens § 11, stk. 3, gennemføre alle kravene i kundekendskabsproceduren, dog kan proceduren gennemføres med udgangspunkt i en risikovurdering, hvorved bankerne som minimum skal forholde sig til bilag II og III, hvilke henvender sig til forholdsvis kundegrupper med begrænset risikoprofil og kundegrupper med øget risikoprofil.

Bankerne skal efter hvidvasklovens § 11, stk. 4 sammenholdt med 4AMLD artikel 13, stk. 3, over for Datatilsynet, med afsæt i deres kundekendskabsprocedure, kunne påvise, at de har overholdt lovreglerne. Dette skal ske ved at bankerne aktivt har taget tilstrækkelig stilling til risikoen for, at enhver kunde kunne være omfattet af en mulig mistanke om hvidvask af penge.

3.4.2.2 Den vedvarende overvågning i forhold til dataminimeringen

Ved overvågningen af kunderne skal bankerne, som ved udførelsen af kundekendskabsproceduren ved etableringen af forretningsforbindelsen, være opmærksomme på at overholde principperne for

¹³⁴ Finanstilsynet, “Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven)”, oktober 2018, side 68.

dataminimeringen i GDPR.¹³⁵ Som tidligere beskrevet i afhandlingen, omfatter dataminimeringen i GDPR artikel 5, stk. 1, litra c, et princip om, at behandlingen af personoplysninger skal være tilstrækkelig, relevant og begrænset til, hvad der må anses for nødvendigt for at opfylde formålet. Bankerne skal kunne påvise tilstrækkelig dokumentation for overvågningen af deres kunder, jf. GDPR artikel 30, stk. 1, og at dette sker i overensstemmelse med princippet om dataminimering.¹³⁶

Vedvarende overvågning af kunderne skal foretages, uanfægtet allokering af kundernes risiko.¹³⁷ Dette betyder, at selvom der er tale om en kunde med begrænset risiko, skal bankerne foretage overvågning af denne kunde.¹³⁸ Det må forventes, at behandlingshjemmel for at foretage kundekendskab proceduren, er af samme karakter, som ved etablering af forretningsforbindelsen eller ved den tidligere foretagne kundekendskabsprocedure, såfremt risikovurderingen af på den pågældende kunde, ikke har ændret sig.

Der kan forekomme situationer, hvor en kunde, der hidtil har været allokeret som værende en begrænset risiko kunde, ændrer status til at blive en øget risiko kunde. I en situation som denne, skal bankerne tage stilling til, om principperne i dataminimeringen er overholdt, herved om bankerne udelukkende har indhentet, hvad der må kunne anses, for at være nødvendigt, for at af- eller bekræfte en mistanke om hvidvask af penge, eller om indsamlingen kunne være sket på mere lempelig vis.¹³⁹ Er sidstnævnte tilfældet, så vil bankernes indsamling ikke være i overensstemmelse med dataminimeringsprincipperne, jf. GDPR artikel 5, stk. 1, litra c. Ydermere, hvis kunderne har skiftet risikogruppe, skal overvågningen af den pågældende kunde justeres.¹⁴⁰ Dette vil henlede til, at såfremt bankerne reagerer på, at der for kunderne foreligger en mulig mistanke om hvidvask af penge, skal bankerne justere overvågning af den pågældende kunde til at omfatte en mere udvidet overvågning af kundebankaktiviteter, som er passende set i forhold til kundernes risikotype. Denne udvidede overvågningen skal ske med formålet, om at af- eller bekræfte den mulige mistanke om

¹³⁵ Datatilsynet ”Hvad er dine forpligtelser?”

¹³⁶ Datatilsynet ”Hvad er dine forpligtelser?”

¹³⁷ Erhvervsstyrelsen, Justitsministeriet, Digitaliseringsstyrelsen og Datatilsynet, ”Databeskyttelsesforordningen, en introduktion til de kommende, nye regler om beskyttelse af personoplysninger” Oktober 2017, side 68.

¹³⁸ Ibid. side 92.

¹³⁹ Jf. Proportionalitetsprincippet

¹⁴⁰ Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven)”, oktober 2018, side 69.

hvidvask af penge.¹⁴¹ Ud fra mistanken, skal bankerne foretage en risikovurdering med henblik på at vurdere, om den pågældende kunde bør skifte risikogruppe. Dette vil altid være tilfældet, hvis bankerne har indgivet en underretning vedrørende mistanken til Hvidvasksekretariatet, herunder SØIK.¹⁴² Den udvidede overvågning kan bestå i, at bankerne eksempelvis indsnævrer tærskelværdierne for den pågældende kunde for, hvornår bankernes system skal rapportere om, at der muligvis kunne foreligge en mistanke om mulig hvidvask af penge ved kundernes bankaktiviteter. Et andet forhold ved den udvidede overvågning kan bestå i, at bankerne i stedet for at benytte automatiske systemer, manuelt overvåger kundernes bankaktiviteter ved mistanke om mistænkelig bankaktivitet.¹⁴³ Dette vil bevirke, at overvågningen bliver mere specifik frem for, at overvågningen, er underlagt en generaliseret automatisk overvågning.

Det kan være svært for bankerne, udelukkende at skulle foretage en vurdering, om hvilke personoplysninger, der kan anses som nødvendige at indhente ved en mistanke om mulig hvidvask af penge. På baggrund af at mistanken udelukkende er baseret på de aktiviteter som bankerne kan overvåge igennem deres automatiske system.

Som nævnt ovenfor angående personlige møder mellem kunderne og medarbejderne i bankerne, vil disse kunne anvendes i et vedvarende forhold, og gavne bankerne i kampen mod hvidvask af penge. Dette vil gøre det lettere for bankerne at overholde principperne i dataminimeringen, men det vil på den anden side være omkostningsfuldt for bankerne at afholde personlige møder med alle deres kunder. Det ville være ressourcekrævende for bankerne i form af, at medarbejderne skulle bruge meget tid på at indkalde kunder og efterfølgende afholde personlige møder, frem for at et automatisk system reagerer på mistanken og vurderer, hvilke personoplysninger, der skal indhentes. Det ville kræve meget manuelt arbejde for bankerne, hvilket skal balanceres med den mulige mistanke om hvidvask af penge. Der kan tales for og imod, om det ville være i overensstemmelse med proportionalitetsprincippet at skulle afholde disse personlige møder ved enhver mulig mistanke om hvidvask af penge. Det der taler for de personlige møder er, at principperne i dataminimeringen ville være lettere for bankerne at overholde. Det der taler imod personlige møder, er omkostningerne forbundet hermed som bankerne skulle afholde samt det forhold, om det ville være proportionalt over

¹⁴¹ Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven)”, oktober 2018, side 112

¹⁴² Ibid.

¹⁴³ Ibid.

for kunderne, at bankerne indkaldte den pågældende kunde til et personligt møde ved enhver mistanke. Der kunne eventuelt her sættes en tærskelværdi, som skulle have formålet at fastslå, om et personligt møde med bankerne, burde være nødvendigt.

Anvendelse af direkte kundekontakt ved etablering af forretningsforbindelsen, og ved udførelsen af en kundekendskabsprocedure ved igangværende forretningsforbindelser, kræver mange ressourcer hos bankerne. Dette forekommer specielt hvis det omhandler fuldførelse af kundekendskabsprocedure ved igangværende forretningsforbindelser. Det vil af denne grund, antageligt ikke være denne metode, som anvendes ved kundekendskabsproceduren, som skal foretages med passende intervaller.

3.4.2.2.1 Ajourføring af informationer:

FAFT's anbefaling nummer 10 udtrykker, at bankerne burde være påkrævet at skulle sikre, at dokumenter, informationer og data, som blev indsamlet under kundekendskabsproceduren ved etableringen af forretningsforbindelsen samt efterfølgende kundekendskabsprocedurer, skal holdes ajour, og relevansen skal vurderes. FATF vurderer, at dette skal ske gennem vurderinger af allerede eksisterende registre. Dette mener FAFT især skal foretages, hvis det omhandler kunder med øget risiko.¹⁴⁴

De personoplysninger som bankerne indsamlede om kunderne ved etablering af forretningsforbindelsen, vil bankerne have mulighed for at opdatere, ved at udføre en skærpet kundekendskabsprocedure for den igangværende forhold. Det kan argumentere for, at hvis personoplysningerne fandtes relevante ved etableringen af forretningsforbindelsen, så vil disse personoplysninger fortsat være relevante ved det igangværende forhold. Hvis bankerne vil udføre en skærpet kundekendskabsprocedure af en af deres kunder, vil disse personoplysninger være et godt udgangspunkt til at kunne vurdere, hvornår der er tale om, at personoplysningerne, som indsamles, er relevante.

¹⁴⁴ The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, 2012, side 66.

Der kan stadig forekomme usikkerheder ved at opdatere allerede indhentede informationer, uanfægtet om bankerne allerede har indsamlet pågældende personoplysninger ved etableringen af forretningsforbindelsen. Årsagen til dette er, at hvis de personoplysninger, bankerne vil komme i besiddelse af, ikke længere findes relevante, vil dette skabe problemer for bankerne, idet at bankerne vil have indsamlet informationer, der ikke er relevante og dermed ikke har bankerne levet op til kravet om dataminimering, jf. GDPR artikel 5, stk. 1, litra c. På den anden side af denne usikkerhed, kan dette også give en god indikator for, hvad der er relevant, nødvendigt og tilstrækkeligt. Der kan argumenteres for, at hvis bankerne vælger at opdatere oplysningerne, som de allerede har indsamlet ved etableringen af forretningsforbindelsen, vil de kunne vurdere kundernes forhold på de resultater, der måtte kunne udledes af opdateringen. Hvis opdateringen af personoplysningerne ikke besidder bemærkelsesværdige ændringer, så vil det for bankerne ikke anses nødvendigt at indsamle yderligere personoplysninger om kunderne, hvilket vil resultere i, at bankerne kun har behandlet personoplysninger, som forefindes relevante, tilstrækkelige og begrænset til at opfylde formålet, jf. GDPR artikel 5, stk. 1, litra c.

Viser det sig til gengæld at der findes en bemærkelsesværdig ændring ved de opdaterede personoplysninger. Dette kan forekomme at der ved personoplysningerne kan udledes, at kunderne ikke udviser videre risiko for hvidvask af penge, kan bankerne allokere kundernes risiko på ny, til eventuelt at udgøre en begrænset risikokunde. Er dette tilfældet, vil det derfor heller ikke være nødvendigt for bankerne at indsamle flere personoplysninger om den pågældende kunde. Hvis derimod de personoplysninger om kunderne, fortsat viser, at kunderne udgør en væsentlig risiko for hvidvask af penge, kan bankerne argumentere for, hvorfor de finder det nødvendigt at indsamle flere personoplysninger om den pågældende kunde. Ved denne metode mindskes bankernes risiko for at handle i strid med dataminimeringen. Der kan forekomme vanskeligheder for bankerne ved benyttelse af denne metode i forhold til, hvornår der kan argumenteres for, at behandlingen af personoplysningerne har karakter af tilstrækkelighed. Det kan være problematisk for bankerne at vurdere, hvornår der ikke er behov for indsamling af flere personoplysninger samt hvornår, personoplysninger findes begrænset til at opfylde formålet.

3.4.2.2.2 Konsekvensanalyse

En dataansvarlig, herunder bankerne, der foretager behandling af kunders personoplysninger, er som hovedregel efter GDPR artikel 35, stk. 1, forpligtet til at forholde sig til, om de skal udarbejde en konsekvensanalyse forud for behandlingen. Denne stillingtagen skal bero på objektiv vurdering, udfærdiget af bankerne, hvor de skal vurdere, om der ved behandlingen vil være forbundet en høj risiko for fysisk, materiel eller immateriel overskridelse af personens rettigheder.¹⁴⁵ En undtagelse til hovedreglen om, at bankerne skal foretage en konsekvensanalyse ved behandlingen, findes i GDPR artikel 35, stk. 10, hvor det foreskrives, at hvis 1) bankerne har hjemmel til behandling efter GDPR artikel 6, stk. 1, litra c eller e, 2) at behandlingen er påkrævet ved et retsgrundlag i EU-retten eller national ret, og 3) hvis der allerede foreligger en konsekvensanalyse vedrørende databeskyttelsen, som led i en generel konsekvensanalyse i forbindelse med vedtagelsen af det rette retsgrundlag.¹⁴⁶ Bankerne har hjemmel til behandling af kundernes personoplysninger efter GDPR artikel 6, stk. 1, litra c og e, idet 4AMLD og hvidvaskloven pålægger bankerne at skulle foretage behandling af kundernes personoplysninger. Til opfyldelse af betingelsen vedrørende den forudgående foretagende konsekvensanalyse, har Erhvervs- og vækstministeriet i Danmark udarbejdet et grund- og nærhedsnotat til folketingets Europavalg 25. marts 2013, hvorved en konsekvensanalyse forud for vedtagelsen af 4AMLD, var en del af dette notat.¹⁴⁷

Endvidere foreskriver GDPR artikel 35, stk. 10, at hvis den pågældende medlemsstat, trods undtagelsen, finder det nødvendigt, skal bankerne foretage en konsekvensanalyse forinden deres behandling af kundernes personoplysninger ved tilfælde med høj risiko for overtrædelse af kundernes rettigheder. Antages det, at staten finder det relevant, skal bankerne forud for deres behandling, udarbejde en konsekvensanalyse for deres behandling.

Ved udførelsen kan bankerne med rette følge ISO/IEC DIS 29134 "Information technology – Security techniques – Privacy Impact Assessment – Guidelines" til udarbejdelsen. Denne vejledning er udarbejdet af den internationale standardiseringsorganisation, ISO, med formålet om at fungere som en vejledning til, hvorledes eksempelvis private virksomheder, såsom banker, kan udføre deres konsekvensanalyse. Det er ikke et påkrav, at bankerne skal følge vejledningen, men Datatilsynet og

¹⁴⁵ Datatilsynet og Justitsministeriet, "Konsekvensanalyse", marts 2018, side 7.

¹⁴⁶ Ibid. side 19.

¹⁴⁷ Erhvervs- og vækstministeriet, "Grund- og nærhedsnotat til folketingets Europavalg - Fjerde revision af direktiv om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge og finansiering af terrorisme", 25. Marts 2013, side 8.

Justitsministeriet udtaler i sin vejledning til konsekvensanalysen, at det vil øge bankernes sandsynlighed for at få alle relevante forhold for behandlingen med.¹⁴⁸ Foruden de fire minimumskrav i GDPR artikel 35, stk. 7, foreligger der ikke en præcisering efter GDPR for, hvorledes konsekvensanalysen skal foretages.¹⁴⁹

De fire minimumskrav en konsekvensanalyse er påkrævet at indeholde er følgende: 1) bankerne skal foretage en systematisk fortegnelse over, hvilke behandlingsprocesser som kundernes personoplysninger vil gennemgå ved behandlingen, eksempelvis indsamling, registrering og lagring. Herved skal det også oplyses, hvilken specifik type personoplysning som bankerne behandler samt deres formål for den enkelte behandlingsproces, og ydermere hvilken legitim interesse, de forbinder hermed.¹⁵⁰ Bankerne kan her med korrekthed notere, at de har hjemmel til behandlingen efter 4AMLD, med formålet om bekæmpelse af hvidvask. 2) Bankerne skal vurdere, om deres behandling af kundernes personoplysninger kan anses for nødvendige og rimelige i forhold til det fastlagte formål for behandlingen. Dette minimumskrav skal sikre, at bankerne ikke behandler personoplysninger om kunderne, som ikke er nødvendige for opfyldelsen af formålet.¹⁵¹ 3) Bankerne skal vurdere på kundernes risici for overtrædelse af dennes rettigheder, som måtte være forbundet med behandlingen af dennes personoplysninger. Risiciene skal opvejes med bankernes formål¹⁵² om at bekæmpe hvidvask af penge efter 4AMLD. 4) Det sidste minimumskriterie er, at bankerne er påkrævet at tage stilling til, hvilke foranstaltninger de kunne fastsætte, for at sikre kundernes personoplysninger ved denne højrisiko behandling.¹⁵³

Viser bankernes konsekvensanalyse, at der om muligt kunne foreligge en høj risiko forbundet med behandlingen af kundernes personoplysninger. Bankerne skal forinden de foretager behandlingen, anmode Datatilsynet om en høring, om hvorvidt deres behandling er i overensstemmelse med GDPR's lovregler, jf. GDPR artikel 36, stk. 1 og 2. Finder Datatilsynet, at den planlagte behandling ikke er i overensstemmelse med GDPR's regler, skal Datatilsynet forinden otte uger efter anmodningen fra bankerne vedrørende høring - dog med mulighed for forlængelse, afgive skriftlig

¹⁴⁸Datatilsynet og Justitsministeriet, "Konsekvensanalyse", marts 2018. Side 17.

¹⁴⁹Ibid. side 19.

¹⁵⁰Datatilsynet og Justitsministeriet, "Konsekvensanalyse", marts 2018. Side 17-18.

¹⁵¹Ibid. side 18.

¹⁵²Ibid.

¹⁵³Ibid.

rådgivning til bankerne, og om nødvendigt benytte sig andre af Datatilsynets beføjelser som nævnt i GDPR artikel 58.

Finder Datatilsynet omend, at der ikke er foreliggende en mulig overtrædelse fra bankernes side ved behandlingen, foreligger der ikke et krav om, at Datatilsynet skal yde skriftlig rådgivning til bankerne.¹⁵⁴ Ved det tiltag, at bankerne anmoder Datatilsynet om forudgående høring angående deres behandlingsaktiviteter, og herfor modtager høringssvar fra Datatilsynet, bevirker ikke, at bankerne nødvendigvis er sikret godkendelse fra Datatilsynet for, at deres fremtidige behandlingsaktiviteter. Det vil til enhver tid, være bankernes ansvar, som dataansvarlig for behandlingen, at vurdere, om deres behandling lever op til GDPR's lovregler.¹⁵⁵

3.4.2.2.3 Artikel 30-fortegnelse:

Formålet med denne fortegnelse er, at bankerne skal kunne blotlægge, hvad de gør med deres kunders personoplysninger i tilfælde af, at Datatilsynet anmoder herom.¹⁵⁶ Der er her tale om, at hensynet bag formålet er at skabe gennemsigtighed.¹⁵⁷

Bankerne skal kunne påvise tilstrækkelig dokumentation for den udførte behandling, som de foretager af kundernes personoplysninger, og herved at behandlingen stemmer overens med formålet for behandlingen. I kraft af dette dokumentationskrav, er det ikke behørigt, at bankerne har vurderet, at behandling er i overensstemmelse med dataminimeringens principper. De skal kunne fremføre dokumentation herfor. Når bankerne har allokeret kundernes risikoprofil som almindelig, lav eller øget risikokunder, så bærer bankerne bevisbyrden for at kunne begrunde deres tilgang og årsag hertil, hvilket de kan pålægges at skulle fremføre for Datatilsynet.¹⁵⁸ Ifølge 4AMLD artikel 41, er bankernes

¹⁵⁴ Datatilsynet og Justitsministeriet, "Konsekvensanalyse", marts 2018. Side 22.

¹⁵⁵ Ibid. side 21.

¹⁵⁶ Justitsministeriet "Betænkning om databeskyttelsesforordningen (2016/679) - og de retlige rammer for dansk lovgivning" del 1, bind 1, side 452

¹⁵⁷ GDPR, præambelbetragtning nr. 100.

¹⁵⁸ Simonova, Anna "The risk-based approach to anti-money laundering: problems and solutions" 2011, side 347.

tiltag for at bekæmpe hvidvask af penge, underlagt 95/46/EF,¹⁵⁹ men da dette er et historisk direktiv, antages det, at GDPR subsidierer og træder i kraft som den relevante lovhjemmel.

Den begrænsning som GDPR ydermere pålægger udførelsen af bankernes arbejde ved bekæmpelse af hvidvask af penge er, at bankerne skal føre detaljeret interne fortegnelser af deres behandlingsaktiviteter, jævnfør GDPR artikel 30. Disse fortegnelser kaldes en artikel 30-fortegnelse. De fortegnelser, som er omhandlet i artikel 30, stk. 1, skal bankerne foreligge skriftligt, jf. GDPR artikel 30, stk. 3. Ved udførelsen af en artikel 30-fortegnelse, er det specifikt beskrevet i artiklens stk. 1, hvilke oplysninger fortegnelsen skal være indeholdt. I fortegnelsen skal det være beskrevet, hvem i bankerne, der foretager behandlingen. Dette indebærer, at der altid vil være en medarbejder i bankerne, som skal stå til ansvar for den behandling, som er foretaget. Det skal i fortegnelsen også være beskrevet til hvilket formålet behandlingen blev foretaget. Herved har bankerne mulighed for at sikre, at formålet og behandlingen stemmer overens, og at der således ikke er foretaget en unødvendig behandling af kundernes personoplysninger. Derudover skal bankerne beskrive risikokategoriseringen af kunderne og dennes personoplysninger. Hvis der forekommer tilfælde, hvor at personoplysningerne videregives til et tredjeland, skal dette også være beskrevet i denne fortegnelse. Er det muligt for bankerne at oplyse den tidsfrist for, hvornår der forventes sletning af kundernes personoplysninger og de sikkerhedsforanstaltninger, som findes bankerne efter GDPR artikel 32, stk. 1, skal dette også være nedfældet i fortegnelsen, jf. GDPR artikel 30, stk. 1, litra a-g.

En artikel 30-fortegnelse skal således indebære en detaljeret beskrivelse af, hvordan bankerne har foretaget behandlingen af kundernes personoplysninger, men den skal også indeholde forhold om, hvem i bankerne, der har foretaget denne behandling. Ved at bankerne skal foretage en artikel 30-fortegnelse, har Datatilsynet en mulighed for at sikre, at den foretaget behandling lever op til principperne om dataminimering. En artikel 30-fortegnelse har dermed status af at være et dokumentationskrav for den udførte behandlingen,¹⁶⁰ men den kan også fungere som en sikring for bankerne og for kunderne, for at behandling er sket på korrekt vis.

Formålet med indførelsen af en artikel 30-fortegnelse, er for det første at erstatte den tidligere fremgangsmåde, hvorved bankerne skulle foretage en generel anmeldelse til Datatilsynet ved

¹⁵⁹ Databeskyttelsesdirektivet, som nu er en historisk lovtekst.

¹⁶⁰ COM(2012) 11 final, side 10

behandling af en kunders personoplysninger.¹⁶¹ Det er ved denne artikel 30-fortegnelse i GDPR, gjort mere enkelt for bankerne, da de med en artikel 30-fortegnelse kun internt skal opbevare dokumentationen samt fortegnelse over den behandling som de har foretaget. Ydermere er formålet ved denne fortegnelse, at den skal fungere som et bevis på, at bankerne har efterlevet GDPR's regler.¹⁶²

En artikel 30-fortegnelse skal kunne fremvises, hvis der kommer et påbud om dette fra Datatilsynet, i forbindelse med Datatilsynets udførelse af et tilsyn med bankernes behandlingsaktiviteter.¹⁶³ Selvom tilgangen til en artikel 30-fortegnelse, er bygget på en risikobaseret tilgang,¹⁶⁴ så er Datatilsynet også inddraget i vurderingen. Med en artikel 30-fortegnelsen, er fokus lagt på ansvarlighed ("accountability").¹⁶⁵ Bankerne er ved denne fortegnelse pålagt bevisbyrden for, at deres behandling af personoplysninger, er foretaget på et hjemlet grundlag, som lever op til principperne i GDPR artikel 5, stk. 1, jævnfør GDPR artikel 5, stk. 2.

3.4.2.2.3 Den risikobaserede tilgang vs. subjektiv vurdering

Det er tidligere nævnt, at 4AMLD er bygget op omkring den risikobaserede tilgang. Denne tilgang giver bankerne mulighed for at allokere deres ressourcer ud til de områder i bankerne, hvor risikoen for mulig hvidvask af penge, er størst.¹⁶⁶ Princippet om dataminimering er derudover udarbejdet efter en subjektiv vurdering. Baggrunden for denne påstand er, at for at kunne vurdere om dataminimering er overholdt, er der tale om en subjektiv vurdering. Bankerne skal konstant bedømme om behandlingen af personoplysninger, opfylder det formål eller overskrider formålet, som personoplysningerne behandles efter og dermed også overtræder princippet angående dataminimering.

¹⁶¹ GDPR præambelbetragtning nr. 89

¹⁶² GDPR præambelbetragtning nr. 82.

¹⁶³ GDPR præambelbetragtning nr. 82.

¹⁶⁴ Erhvervsstyrelsen, Justitsministeriet, Digitaliseringsstyrelsen og Datatilsynet, "Databeskyttelsesforordningen, en introduktion til de kommende, nye regler om beskyttelse af personoplysninger" Oktober 2017, side 16.

¹⁶⁵ Justitsministeriet "Betænkning om databeskyttelsesforordningen (2016/679) - og de retlige rammer for dansk lovgivning" del 1 bind 1, side 441.

¹⁶⁶ Se afsnit 2.2

Ved at begge lovregler er gennemført med en tilgang til at den forpligtede institution, skal foretage vurderinger, om behandlingen af personoplysninger overholder de respektive lovregler, kan der både være tale om en fordel og en begrænsning for bankerne. Der kan argumenteres for, at det er en fordel for bankerne, at der ikke er helt klare retningslinjer, og at de derfor vil kunne skræddersy deres processer i forhold til risikoen, som forefindes i bankernes forretningsplan og deres kundeportefølje. Med argumentation i dette, giver det bankerne mere fleksibilitet og flere tilpasningsmuligheder, hvis en usædvanlig kunde forekommer. En anden fordel, som findes er, at det giver bankerne mulighed for at bekæmpe hvidvask af penge mere effektivt. På baggrund af at bankernes kundekendskabsprocedure ikke er kendte for igangværende forretningsforbindelser og mulige nye forretningsforbindelser, hvorved kriminelle kunder kan forekomme, jf. GDPR artikel 8, stk. 4, litra a. Ved at der ikke er offentligt kendskab til bankernes procedurer, antages det, at kriminelle ikke kan forudse, hvilke specifikke tiltag bankerne benytter sig af, for at bekæmpe hvidvask af penge, og det vanskeliggøres dermed for kriminelle at forsøge at hvidvaske penge gennem bankerne.

På den anden side, er der for det første tale om, at der skal foretages to vurderinger, som varetager hvert sit hensyn, hvor formålet med den risikobaserede tilgang, er at give bankerne adgang til at foretage så vidtgående behandlinger og processer, som de anser for passende.¹⁶⁷ Hvor den subjektive vurdering, ved princippet om dataminimering, har til formål, at bankerne skal foretage en vurdering af behandlingen, og begrænse denne behandling mest muligt.¹⁶⁸ For det andet sætter denne fleksibilitet en begrænsning, da der ikke findes klare retningslinjer angående, hvorledes bankerne skal forholde sig til både vurderingen angående den skærpede kundekendskabsprocedure samt til, hvordan dataminimeringen skal sikres overholdt. Der kan argumenteres for, at det er en begrænsning, at lovreglerne ikke indebærer entydige retningslinjer. Årsagen til denne begrænsning er, at det som bankerne anser som overholdelse af den skærpede kundekendskabsprocedure og principperne for dataminimering, ikke nødvendigvis er det samme som Finanstilsynet og Datatilsynet anser for efterlevelse af retsreglerne. Dette kan ses i tre nyere afgørelser fra Datatilsynet omkring efterlevelse af principperne for dataminimering.

¹⁶⁷ Se afsnit 2.2

¹⁶⁸ Se afsnit 2.2

3.4.2.2.4. Afgørelser

Formålet med analyse af afgørelserne, er at klarlægge, hvordan Datatilsynet fortolker reglerne for dataminimering set i forhold til, hvorledes virksomhederne fortolker disse. Endvidere om den subjektive vurdering udviser en påvirkning på udfaldet af afgørelserne. Da GDPR er nyligt vedtaget, er omfanget af Datatilsynets afgørelser vedrørende dataminimeringen meget begrænsede. Datatilsynet har på nuværende tidspunkt, kun afgjort tre sager vedrørende overtrædelse af dataminimeringen. Formålet med afsnittet er ydermere at udlede, hvorvidt Datatilsynet anvender en gennemgående metode til afgørelse om der er sket behørig overholdelse af dataminimeringens principper.

3.4.2.2.4.1 TDC A/S afgørelse:

TDC A/S (omtales herefter TDC) blev undersøgt på baggrund af en klage fra en borger i 2016.¹⁶⁹ Klagen omhandlede behandlingen af borgerens personoplysninger. Sagens omdrejningspunkt var, at TDC registrerede trafik- og lokaliseringsdata, når denne borger tilkoblede internettet via sin mobiltelefon. I sagen fremgår det, at TDC har indsamlet lokaliseringsdata ved mobiltrafik. Der er her tale om, at TDC ikke kan separere alle sine lokationsdata fra hinanden, og hermed har indsamlet al lokationsdata. Borgeren udtaler, at TDC indsamler flere oplysninger end hvad der må findes nødvendigt for, at TDC kan overholde sine forpligtelser.

I TDC-afgørelsen udtaler Datatilsynet, at en opbygning af TDC's system, hvilken bevirker den manglende overholdelse af principperne i dataminimeringen, ikke kan anses som lovlig. Det forhold at, der måtte være omkostninger forbundet med en etablering af et nyt system, vægtes ikke højere end overholdelsen af principperne i dataminimeringen. Det statueres meget tydeligt ud fra TDC-afgørelsen, at vigtigheden for hensynet om, at virksomhederne skal opfylde og overholde principperne i dataminimeringen, går forud for virksomhedernes eventuelle store omkostninger forbundet herved. At et systems indretning bevirker til, at indsamlingen ikke kan forenes med principperne, bevirker med henvisning til denne afgørelse tydeligt, at virksomhederne er forpligtede til at etablere nye systemer til formålet. Det udledes endvidere af TDC-afgørelsen, at der klart og tydeligt skal være et formål med indsamlingen og behandling af personoplysningerne. I TDC-

¹⁶⁹ Afgørelse: Journalnummer: 2018-31-0070 "Klage over TDC's registrering af trafik- og lokaliseringsdata".

afgørelsen lægger Datatilsynet særligt vægt på, at TDC har indsamlet og behandlet en stor mængde data, som ikke har været begrænset til det, som må ses nødvendigt for at opfylde forpligtelserne efter logningsbekendtgørelsen. TDC udtaler endvidere selv, at de ikke har haft et klart formål med indsamlingen og behandlingen af den pågældende mængde data.

3.4.2.2.4.2 Taxa 4x35 afgørelse:

Taxa 4x35 afgørelsen blev publiceret den 18. marts 2019, og vedrører overtrædelse af dataminimeringen.¹⁷⁰ Denne afgørelse omhandler Taxa 4x35's opbevaring af deres kunders telefonnumre, hvor disse telefonnumre først slettes fem år efter afviklingen af taxaturen. Taxa 4x35 havde forlænget opbevaringsperioden af kundernes telefonnumre til at være i fem år, i stedet for to år, som er opbevaringsperioden for kundernes øvrige oplysninger. De havde forlænget opbevaringsperioden med det formål at bruge telefonnumrene som datagrundlag for forretningsudvikling i virksomheden, og som fælles referenceramme i deres system. Taxa 4x35 var selv af den opfattelse, at de levede op til principperne om dataminimering, men hvor Datatilsynet anså det som et brud på dataminimeringen. Datatilsynet fastslår i afgørelsen, at Taxa 4x35's forlængede opbevaringsperiode af kundernes telefonnumre, ikke kunne anses for nødvendig, set i lyset af opfyldelse af Taxa 4x35's formål om, at de skulle fungere som nøgle og fælles referenceramme for systemet. Datatilsynet mente, at mindre kunne have opfyldt selv samme formål.

Taxa 4x35 udtaler i afgørelsen, at mindre behandling kunne have opfyldt samme formål, men at deres system ikke kunne håndtere bagudrettet at udskifte telefonnummeret med mere lempelig data. Datatilsynet lægger vægt på, at Taxa 4x35 ikke kan fastlægge en behandlingshjemmel, som foreskriver denne opbevaringstid for telefonnumre. I afgørelsen lægger Datatilsynet forholdet, at Taxa 4x35's system ikke kan håndtere bagudrettet at ændre data samt det, at høje omkostninger ville være forbundet med en ny udvikling af systemet, ikke fritager Taxa 4x35 fra at skulle overholde principperne om dataminimering.

Det kan udledes af Taxa 4x35-afgørelsen, at der skal ske overholdelse af principperne tilstrækkelighed, relevans og begrænset til, hvad der er nødvendigt i dataminimeringen, selvom resultatet af dette vil påføre virksomheden store omkostninger, ved at de blandt andet vil skulle

¹⁷⁰ Afgørelse: Journalnummer: 2018-41-0016 "Tilsyn med Taxa 4x35's behandling af personoplysninger".

udvikle nye systemer. Det kan udledes, at hvad Taxa 4x35 fandt var i nødvendigt for at overholde dataminimeringen, ikke var det samme som Datatilsynet fandt nødvendigt.

3.4.2.2.4.3 Rejsekort A/S afgørelse:

Afgørelsen omhandlede Rejsekort A/S (omtales herefter Rejsekort), blev publiceret den 16. April 2019, og er den nyeste afgørelsen fra Datatilsynet vedrørende overtrædelse af princippet om dataminimeringen.¹⁷¹

Afgørelsen er foretaget på baggrund af en klage fra kunde hos Rejsekort, hvor den rejsende fandt Rejsekort's håndtering af klageres anmodning angående berigtigelse af personoplysninger utilstrækkelig. Klageren mente, at der i forbindelse med fejlregistrering af lokalitetsoplysninger, ikke skete tilstrækkelig berigtigelse af disse, hvilket klager påklagede over for Rejsekort. På baggrund af klagen, foretog Rejsekort en rettelse af rejseprisen, men henviste til, at det ikke fandtes teknisk muligt for dem at korrigere i selve klagerens rejsehistorik. Udover dette bemærker Rejsekort, at de allerede har iværksat flere tiltag og undersøgelser, til at skulle kunne forhindre dette i at skulle ske fremover. Derudover omtaler Rejsekort, at de hovedsageligt foretager korrigerende af rejseoplysninger på baggrund af, at hvert enkelt rejsende henvender sig og informerer om forkert registrering af rejse.

I forbindelse med princippet om dataminimering, udtaler Datatilsynet, at de ikke finder, at Rejsekortet i forbindelse med behandlingen af kundernes lokationsdata, ikke i tilstrækkeligt grad overholder dataminimeringen, idet at der ikke er sket tilstrækkelig berigtigelse af klagerens rejseoplysninger.

Datatilsynet har på baggrund af klagen udstedt to påbud til Rejsekort, hvilke skal være gennemført inden den 15. juni 2019. Disse påbud lyder på, at Rejsekort skal kunne imødekomme klagerens anmodning om at få berigtiget sine rejseoplysninger. Derudover skal Rejsekort inden denne dato informere Datatilsynet om, hvorledes de vil kunne sikre, at den generelle behandling af deres kunders lokalitetsoplysninger er i overensstemmelse med bestemmelserne i GDPR.

Det kan udledes af Rejsekort-afgørelsen, at der skal foretages en korrektion af IT-systemer for at kunne overholde bestemmelserne i GDPR, hvor dataminimering er inkluderet. Det bemærkes, at dette

¹⁷¹ Afgørelse: Journalnummer: 2018-31-0147 "Alvorlig kritik og påbud til Rejsekort A/S"

er et krav ved påbud, hvilket har den betydning, at hvis der ikke sker korrektion af Rejsekort's IT-systemer inden den fastlagte dato, kan Rejsekort efter GDPR artikel 83, stk. 6 pålægges administrative bøder på op til 20.000.000 EUR, eller op til fire procent af den samlede globale årlige omsætning i det foregående regnskabsår, jf. GDPR artikel 83, stk. 2 og 5. Det kan på baggrund af dette påbud udledes, at der skal ske korrigerende af Rejsekort's IT-systemer, uanset omkostningerne forbundet hermed.

Med afsæt i Taxa 4x35-, Rejsekort- og TDC-afgørelsen kan det analyseres frem til en (metodiske tilgang) vurderingsmetode, som datatilsynet anvender til at kunne vurdere, om der sker efterlevelse af GDPR. Det første angår, hvad formålet er med indsamlingen og opbevaringen, om er dette acceptabelt. Herefter kan det udledes, at datatilsynet har den tendens, at hvis virksomhederne har mulighed for at foretage en mindre indgribende behandling af personoplysninger, skal dette gøres, ligegyldigt til hvilken omkostning det pålægger virksomheden. Dette kan henføres til, at hvis bankerne har mulighed for at udvikle metoder, systemer eller processer. Hvor disse vil resultere i en mere korrekt og lempelig indsamling og behandling af personoplysningerne i forhold til bankernes formål om at bekæmpe hvidvask af penge, skal bankerne gøre dette, uagtet hvor mange ressourcer dette vil påføre bankerne.

3.5 Delkonklusion

Formålsfortolkningen for den skærpede kundekendskabsprocedure påviste, at det er meget klart, hvornår der skal foretages en skærpet kundekendskabsprocedure. Dette foreligger, når de danske banker vurderer, at der er tale om en øget risiko ved en kunde, og ved på forhånd fastlagte situationer, hvilke består i transaktioner fra højrisiko tredjelande, og hvis der er tale om PEP-kunder. Endvidere påviste den endog, at der er stor usikkerhed om, hvornår risikoen udgør en øget risiko, da dette er en subjektiv vurdering fra bank til bank.

Formålsfortolkningen af dataminimeringen viste, at behandling af personoplysninger ikke må gå forud for behandlingsformålet, hvorved der også foreligger en subjektiv vurdering fra de danske bankers side. De tre benyttede afgørelser fra Datatilsynet, påviste meget klart, at behandlingen skal være begrænset til at omfatte det relevante, tilstrækkeligt og nødvendige for formålet. Analysen

belyste problematikken omkring, at udførelsen af den skærpede kundekendskabsprocedure besværliggøres af, at principperne i dataminimeringen skal overholdes ved udførelsen. Det der ikke foreligger direkte klare retningslinjer for, hvor langt principper for behandling; relevant, tilstrækkeligt og begrænset til kun det nødvendige for formålet, går, giver dette bankerne en udfordring i deres indsats i at overholde dataminimeringen. De har endvidere ikke andet praksis at rette sig efter, end de tre afgørelser, der på nuværende tidspunkt foreligger fra Datatilsynet. Det som bankerne anser som korrekt overholdelse af principperne i dataminimeringen, er ikke ensbetydende med, at Datatilsynet er af samme mening. Dette kom tydeligt til udtryk i Datatilsynets tre afgørelser, hvorved virksomhederne mente, at de havde overholdt principperne for dataminimeringen, men hvor Datatilsynet var af modsat opfattelse. Endvidere ligger bankernes udfordring i, at de ved indsamling af personoplysninger på dette tidspunkt, ikke er bekendt med udfaldet af det indsamlede. Derfor har bankerne udfordringer ved at foretage vurdering af niveauet af personoplysningernes relevans, førend indsamlingen har fundet sted.

Ved at analysere gældende ret, er det påvist, at det kan være utroligt udfordrende for bankerne at balancere mellem disse to regelsæt. Årsagen er at det ene er baseret på en risikobaseret tilgang og det andet på en subjektiv vurdering, hvor disse to tilgange bliver anvendt til to vidt forskellige formål. Det kan konkluderes, at den risikobaserede tilgang skal anvendes, for at sikre en fleksibilitet i lovgivningen, og for bankerne til bekæmpelse af hvidvask af penge med henblik på hemmeligholdelse af deres forretningsprocedure, så kriminelle får sværere at omgå disse. GDPR finder det nødvendigt at blottlægge, hvordan bankerne behandler kundernes personoplysninger efter artikel 30-fortegnelsen. Ved denne fortegnelse skal bankerne holde dokumentation for deres formål med indsamling og behandling ved, at de skal kunne bevise og dokumentere, formålet for de personoplysninger som de indsamler og behandler.

Det kan udledes, at påvirkningen, som forekommer af dataminimeringen er, at dette begrænser bankernes mulighed, for at indhente personoplysninger med formålet, om at kunne bekæmpe hvidvask af penge. Dataminimeringen udfordrer og begrænser bankerne med henblik på kvaliteten af den skærpede kundekendskabsprocedure, at denne er fyldestgørende og grundig, idet bankerne samtidig skal overholde principperne i dataminimeringen.

Kapitel 4

Hvis der var tale om en perfekt verden med komplet information ville der ved bankernes bekæmpelse af hvidvask af penge, ikke foreligge nogen problematik angående bankernes overvågning af deres kunder.¹⁷² Dette er dog ikke tilfældet, idet der foreligger asymmetrisk information mellem bankerne og deres kunder.

Hvidvask af penge i samfundet; herunder hvidvask af penge gennem bankerne, er et alvorligt problem for samfundsøkonomien.¹⁷³ Dette har ledt til, at EU har intensiveret reguleringen for bekæmpelse af hvidvask af penge. I dette afsnit vil det være forholdet mellem bankerne og deres kunder, som søges analyseret; herunder om det vil være en nødvendighed at gennemtvinge statslig indgriben.

Det er konstateret, at hvidvask af penge er et stort samfundsmæssigt problem, idet at hvidvask af penge består i fem procent af det globale BNP.¹⁷⁴ Disse fem procent af den globale BNP består på bekostning af, at staten har håndhævet nogle forpligtelser i samfundet. Dette resulterer i, at der forekommer nogle eksternaliteter, der berører bankerne, hvilke kan have en negativ eller positiv indvirkning på bankerne. Når der forekommer en negativ eksternalitet, resulterer dette i, at der ikke sker optimal ressourceallokering.¹⁷⁵ Det vil sige, at ved forekomsten af denne eksternalitet, resulterer dette i et dødvægtstab¹⁷⁶ for samfundet.

Det søges i dette afsnit at anvende teorierne angående Signaling og Screening, sammenholdt med Principal-Agent teorien, for at søge at løse spillet med asymmetrisk information. P/A teorien anvendes til at analysere forholdet mellem de danske banker og deres kunder. Dette skal bidrage til at belyse den asymmetriske information, der foreligger ex ante og ex post mellem bankerne og deres kunder. Resultaterne af denne analyse, vil blive videreført til den integrerede analyse i kapitel 5.

¹⁷² Knudsen, Christian "Økonomisk Metodologi Bind 2 - Virksomhedsteori og Industriøkonomi" 2. Udg. 1997, side 56.

¹⁷³ Statsadvokaten, "Hvidvask i Danmark, Den nationale risikovurdering 2015", side 4.

¹⁷⁴ United Nations Office on Rugs and Crime "Money-Laundering and Globalization".

¹⁷⁵ Viscusi, W. Kip, Harrington, Jr., Joseph E. & Vernon, John M. "Economics of Regulation and Antitrust" 4. Udg, 2005, side 376.

¹⁷⁶ Skatteministeriet, "Skat December 2002", København 2002, side 31.

4.1 Bayesian spil

Med afsæt i den Neoklassiske teori, vil der i en perfekt verden være perfekt information.¹⁷⁷ Ved perfekt information betyder dette, at det ikke vil være nødvendigt for bankerne at skulle overvåge deres kunder, og indsamle informationer om dem. Årsagen til dette er at ved perfekt information, har bankerne adgang til de samme informationer om kunderne, som kunderne selv har. Derudover besidder bankerne også viden om alle kunders handlinger. Hvis der var tale om perfekt information, ville der ikke foreligge asymmetrisk information mellem bankerne og kunderne, men derimod symmetrisk information. Det ville i den forbindelse være muligt for bankerne at sætte indsatsen ind der, hvor graden af kriminalitet anses som størst.

Der foreligger ikke perfekt information mellem bankerne og deres kunder, men derimod asymmetrisk information. Årsagen til dette er, at der eksisterer kriminelle personer, som har til hensigt at svindle med finansielle midler ved at hvidvaske penge gennem bankerne. På denne baggrund, opstår der asymmetrisk information, hvor disse kriminelle kunder besidder information om dem selv, som bankerne ikke har kendskab til.

Ved hvidvask af penge, er der i denne afhandling tale om en negativ eksternalitet, hvoraf denne eksternalitet udgør en forurening af den finansielle sektor.¹⁷⁸ Som nævnt i indledningen til dette afsnit, så skaber denne negative eksternalitet et dødvægtstab. Dødvægtstabet forekommer når der sker hvidvask af penge og dermed ikke sker beskatning af disse penge. Resultatet af dette er, at BNP'en er lavere end den burde være set i forhold til, hvis der var sket beskatning af disse penge. Som også nævnt i indledningen til dette afsnit, er hvidvask af penge vurderet til at bestå af fem procent af den globale BNP.¹⁷⁹

Dødvægtstabets udspringer af den asymmetrisk information mellem bankerne og kunderne. Denne informationsasymmetri søges løst ved et Bayesian spil. Spillet vil udelukkende behandle kunder, som besidder en almindelig og en øget risiko for hvidvask af penge.

¹⁷⁷ Knudsen, Christian "Økonomisk Metodologi Bind 2 - Virksomhedsteori og Industriøkonomi" 2. Udg. 1997, side 56.

¹⁷⁸ Masciandaro, Donato "Money Laundering: The Economics of Regulation", 1999, side 225.

¹⁷⁹ United Nations Office on Drugs and Crime "Money-Laundering and Globalization".

Bankerne har ufuldstændig information om deres allerede eksisterende kunder og om de kunder, som skal etableres ved en forretningsforbindelse. Kunderne kan enten være type 1: Kriminel eller type 2: Ikke-kriminel. Den ufuldstændige information består i, at kunderne er bekendte med, hvilken kundetype de er og hvad deres payoffs er. Bankerne er omvendt kun bekendte med, at kunderne enten er type 1 eller type 2. Det antages, at der er 10 procent sandsynlighed for, at kunderne er type 1: Kriminel og 90 procent sandsynlighed for, at kunderne er type 2: Ikke-kriminel. Disse sandsynligheder består i den rationelle antagelse, at minoriteten af kunderne er kriminelle og majoriteten er ikke-kriminelle. Den ufuldstændige information skaber herved asymmetrisk information. Årsagen til at den asymmetriske information opstår, er fordi at kunderne har ret til beskyttelse af deres personoplysninger, når bankerne anmoder dem om at afgive disse.

Bankerne kan som udgangspunkt ikke adskille de to typer af kunder fra hinanden, fordi de ikke er bekendte med hvem der er hvem. Bankernes strategi vil dermed være den samme uanfægtet, hvilken type den pågældende kunde er. Det forhold at bankerne som udgangspunkt vil benytte sig af samme strategi over for alle deres kunder bevirker, at der er tale om en pooling strategi fra bankernes side af.¹⁸⁰

I denne afhandling vil der være tale om et sekventielt spil. Dette har den betydning, at kunderne og bankerne skiftevis foretager deres træk. Spillet indeholder perfekt information, da bankerne kan observere alle kundernes træk, og omvendt kan kunderne observere alle bankernes træk.¹⁸¹

Der opstilles et spil, som er baseret på bankernes overbevisninger og handlinger. Det antages, at kunderne og bankerne handler rationelt i forhold til deres overbevisninger, hvorfor målet er at finde frem til en Perfekt Bayesian ligevægt ved Bayes' regel.¹⁸² I dynamiske spil med ufuldstændig information, vil spillernes træk sommetider føre til, at deres ellers private information afsløres for modparten. Når privat information afsløres, vil modparten tage højde for den nye information.¹⁸³

¹⁸⁰ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 83.

¹⁸¹ Ibid. side 312.

¹⁸² Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 84.

¹⁸³ H. Scott Biermann, Louis Fernandez, "Game Theory With Economic Applications", second edition, side 321.

Der er her tale om et spil om, hvordan bankerne og kunderne agerer, når kunderne, som den informerede part, har mulighed for at tilbageholde afgørende oplysninger.¹⁸⁴

Kundetyper

Type 1: En kriminel kunde

Type 2: En ikke-kriminel kunde

4.1.1 Signaling teori

I et Signaling spil besidder kunderne privat information, som bankerne ønsker at blive bekendte med.¹⁸⁵ Den private information består i, om de pågældende kunder er kriminelle eller ikke er kriminelle. Ved et Signaling spil er direkte kommunikation ikke en mulighed og kunderne vil derfor gerne signalere til bankerne, hvilken kundetype de er. Dette må kunderne gøre ved at engagere sig i aktiviteter, som kan indikere dette.¹⁸⁶ Et Signaling spil bruges derfor i denne afhandling til, at kunderne kan signalere deres private information til bankerne.¹⁸⁷

I dette Signaling spil bliver det analyseret, om det er muligt for bankerne at kunne skille de kriminelle og de ikke-kriminelle kunder ad, under forretningsforbindelsen levetid. Dette set i forhold til allokeringen af kundernes risiko; almindelige risikokunder eller øgede risikokunder. Det undersøges derfor, om kunderne kan signalere, hvilken type kunde de er, overfor bankerne. De ikke-kriminelle kunder vil signalere over for bankerne, at de ikke er kriminelle, ved at afgive sine personoplysninger til bankerne. De kriminelle kunder vil enten tilbageholde deres personoplysninger med formålet om at bevare deres identitet, eller også vil de efterligne de ikke-kriminelle kunder, i håbet om at blive allokeret som en ikke-kriminel kunde.

Ved et Signaling spil inddrages der en hypotetisk tredjepart, der kaldes for nature. Nature foretager det første træk i spillet.¹⁸⁸ Det er nature, som bestemmer, om kunderne er kriminelle eller ikke-kriminelle, men hvor kunderne med stadighed også er bekendt med deres kundetype. Årsagen til at inddrage nature i dette spil, er for at kunne omstille et spil med ufuldstændig information til et spil,

¹⁸⁴ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 80.

¹⁸⁵ Ibid. side 123.

¹⁸⁶ Aumann, Robert J. & Hart, Sergiu "Handbook of Game Theory with economic applications Volume II" 1. Udgave, 1994, side 851.

¹⁸⁷ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 123.

¹⁸⁸ Ibid.

der indeholder uperfekt information. Ved at gøre dette, kan spillet løses ud fra det Perfekte Bayesian ligevægt løsningskoncept. Herfra kan der udføres et extensive form spil, hvor kunderne har et træk og kan vælge mellem to muligheder,¹⁸⁹ enten at give informationer eller ikke at afgive informationer.

I et extensive form game, har vi opstillet to spillere udover nature. Spiller 1 (P1) som er kunderne, der selv er bekendte med, om de enten er kriminelle eller ikke-kriminelle og spiller 2 (P2), som er bankerne, der ikke har kendskab til P1's type. Det eneste bankerne er bekendt med er, at der er 10 procent sandsynlighed for, at den pågældende kunde er kriminel og 90 procent sandsynlighed for, at den pågældende kunde ikke er kriminel. Kunderne har følgende to strategier; enten at give bankerne sine personoplysninger eller at tilbageholde sine personoplysninger. Hertil har bankerne også to strategier; at vurdere den pågældende kunden som en øget risikokunde eller som en almindelig risikokunde. Det forhold, at bankerne skal vurdere kunderne som almindelig risiko kunder koster dem ikke noget, fordi bankerne ved alle deres kunder, skal foretage en kundekendskabsprocedure¹⁹⁰. Det koster derimod bankerne -2 at vurdere en kunde som øget risiko, da udarbejdelse af en skærpet kundekendskabsprocedure¹⁹¹ kræver ekstra ressourcer for bankerne. Hvis bankerne foretager en korrekt vurdering af kundernes type, får de en gevinst på +4, med det den begrundelse, at korrekt vurdering af kundernes type, sikrer en korrekt allokering af kunderne, hvorimod en fejlvurdering og herved også en fejlallokering af kundernes type, koster bankerne -2.

Hvis der er tale om kriminelle kunder, som afgiver personoplysninger, så koster det kunderne -2. Årsagen hertil er, at kriminelle kunderne ved afgivelse af deres personoplysninger risikerer at afsløre, at de er kriminelle. Hvis de kriminelle kunder vælger at tilbageholde deres personoplysninger, så giver det dem +1, da dette vil beskytte dem fra at blive afsløret som kriminel. Hvis de ikke-kriminelle kunder til gengæld vælger at afgive deres personoplysninger, får de en gevinst på +1, fordi de gerne vil signalere til bankerne, at de ikke er kriminelle. Omvendt vil det give de ikke-kriminelle kunder +0,5 at tilbageholde deres personoplysninger, og derved får de et payoff på +0,5, på baggrund af det forhold, at de risikerer at signalere noget forkert.

Uanfægtet hvilken type kunderne er, vil det give dem en gevinst på +2, at bankerne vurderer dem til at udgøre en almindelig risiko.

¹⁸⁹ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 126.

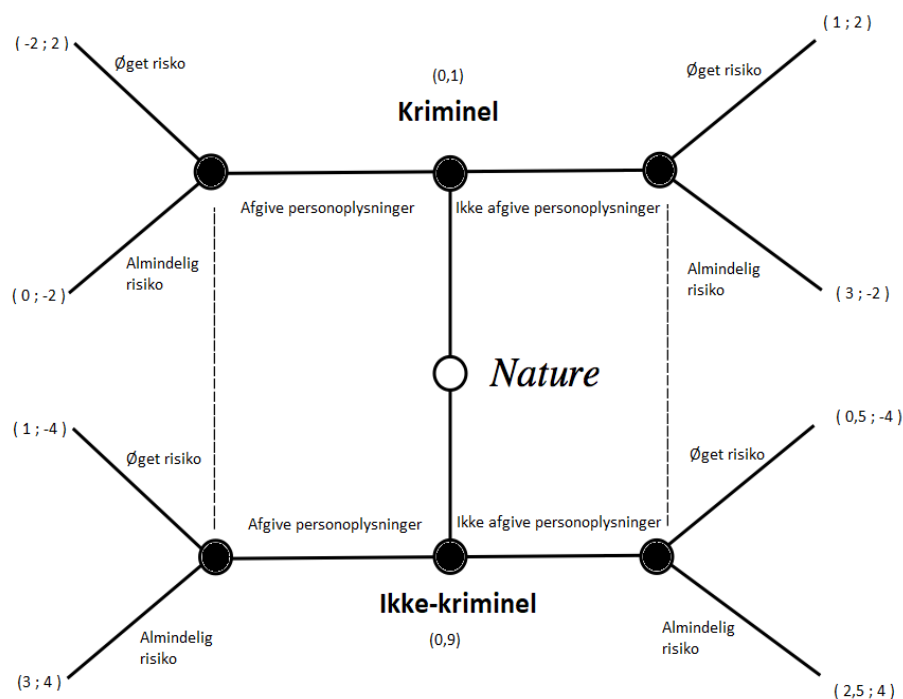
¹⁹⁰ Se afsnit 2.4.

¹⁹¹ Se afsnit 2.4

Payoffs for kunderne og bankerne vil derfor se således ud:

Kriminel /bank	Øget risiko	Almindelig risiko
Afgive personoplysninger	-2 ; 2	0 ; -2
Ikke afgive personoplysninger	1 ; 2	3 ; -2

Ikke-kriminel / bank	Øget risiko	Almindelig risiko
Afgive personoplysninger	1 ; -4	3 ; 4
Ikke afgive personoplysninger	0,5 ; -4	2,5 ; 4



Figur 4. Egen tilvirkning.

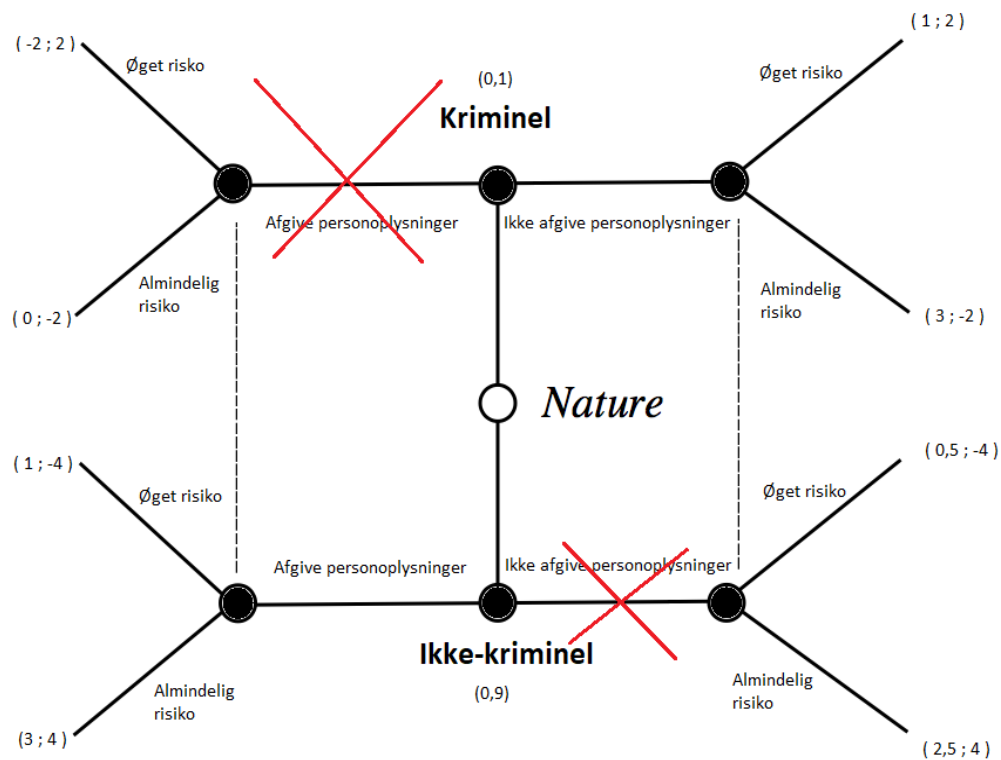
Der findes i dette spil disse 4 plausible strategier:

1. Kriminelle vil afgive personoplysninger
2. **Kriminelle vil ikke afgive personoplysninger**
3. **Ikke-kriminelle vil afgive personoplysninger**
4. Ikke-kriminelle vil ikke afgive personoplysninger

Strategi nr. 1 og nr. 4 kan elimineres, da disse ved inddragelse af Bayes' regel ikke anses for at være rationelle,¹⁹² samt fordi kunderne altid vil spille den strategi, som er deres Best Response. Best Response anses for at være strategier, som hver især er den bedste strategi til den anden spillers strategi.¹⁹³

¹⁹² Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 83.

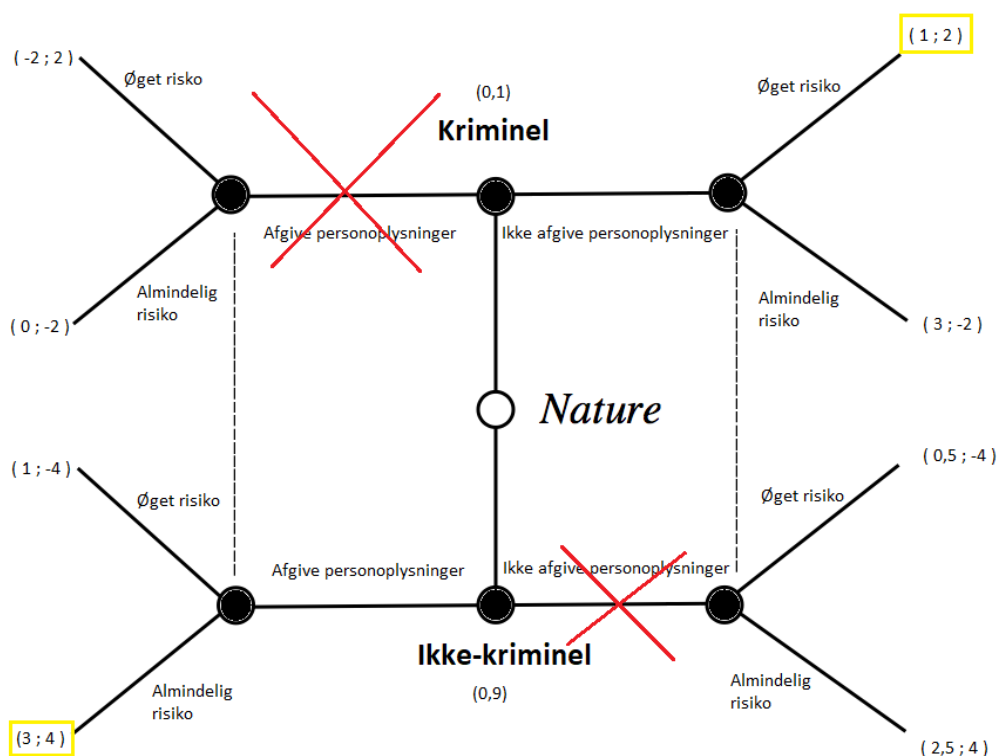
¹⁹³ Ibid. side 22.



Figur 5. Egen tilvirkning.

Nu skal bankernes overbevisninger udledes. Dette gøres ved at benytte Best Response metoden til at finde Nash ligevægtene for hver strategi.¹⁹⁴

¹⁹⁴ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 129.



Figur 6. Egen tilvirkning.

Separat ligevægt

Ud fra de fundne Nash ligevægte, kan der i dette spil, findes en separat ligevægt. Denne findes hvor de ikke-kriminelle kunder afgiver deres personoplysninger, hvorefter bankerne allokerer disse kunder som almindelige risikokunder. Omvendt vil de kriminelle kunder tilbageholde deres personoplysninger, hvorefter bankerne vil allokere disse kunder som om øgede risikokunder og dermed foretage en skærpet kundekendskabsprocedure af disse. Dette viser, at der findes en Perfekt Bayesian ligevægt i spillet, idet at overbevisninger og handlinger er i overensstemmelse med hinanden.¹⁹⁵ Hvis det kun er de ikke-kriminelle kunder, der afgiver deres personoplysninger i en ligevægt, så vil bankerne have en overbevisning om, at de kunder, som afgiver deres personoplysninger og de kunder, som ikke afgiver personoplysninger, begge er kriminelle kunder.

Det testes herefter, på baggrund af bankernes overbevisning, om dette er en Best Response strategi for kunderne.¹⁹⁶ De ikke-kriminelle kunder får et payoff på +3, når de afgiver personoplysninger.

¹⁹⁵ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 84.

¹⁹⁶ Ibid. side 130.

Dette er et højere payoff end $+0,5$, som de vil få ved ikke at afgive deres personoplysninger. Årsagen til, at de vil modtage et payoff på $+0,5$ er, at bankerne ved denne ligevægt har den overbevisning, at kunder som ikke afgiver personoplysninger, er kriminelle og derfor allokerer bankerne dem som øgede risikokunder. I denne foreslåede ligevægt for kriminelle kunder, der vælger ikke at afgive deres personoplysninger, opnår de et payoff på $+1$. Afgiver de derimod hvorimod deres personoplysninger, vil de få et payoff på $+0$. Denne separate ligevægt er også Best Response for kunderne. Det forhold at det er Best Response for kunderne bevirker, at de ikke vil have incitament til at afvige fra deres strategi og imitere den anden kundetype.

Pooling ligevægt

Det skal herefter testes, om der findes en pooling ligevægt i spillet, hvor begge kundetyper vil have incitament til at benytte den samme strategi.¹⁹⁷

Først startes der med at se på, om begge kundetyper vil vælge ikke at afgive sine personoplysninger. Det antages, at der er en pooling ligevægt, hvor begge kundetyper vælger ikke at afgive deres personoplysninger. Denne pooling ligevægt kræver, at bankerne har en overbevisning om, at kunder, som afgiver deres personoplysninger, er kriminelle. Denne overbevisning fra bankernes side er dog ikke antagelig. Årsagen til dette er, at de kriminelle kunder altid vil være bedre stillet, ved ikke at afgive deres personoplysninger, uanfægtet bankernes reaktion på dette. Årsagen til bankernes overbevisning om dette er, at de kriminelle kunder vil spille en dominerende strategi. Der er tale om en dominerende strategi, fordi de kriminelle kunder altid vil få et højere payoff ved ikke at afgive deres personoplysninger. Dette kan ses ved, at et payoff på $+1$ og $+3$ (ikke afgive personoplysninger) er højere end et payoff på -2 og 0 (afgive personoplysninger).

Bankerne kan dog godt have den overbevisning, at de kunder, som afgiver deres personoplysninger ikke er kriminelle. Dette fordi de ikke-kriminelle kunder opnår et payoff på $+3$, ved at afgive deres personoplysninger, frem for et payoff på $+2,5$, ved ikke at afgive deres personoplysninger. På baggrund af dette, vil de ikke-kriminelle kunder ikke afvige fra deres dominerende strategi. Dette bevirker, at bankerne vil have den overbevisning, at kunder, som afgiver sine personoplysninger, ikke er kriminelle. På baggrund af dette kan der findes en pooling ligevægt, hvorved begge kundetyper

¹⁹⁷ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 130.

ikke afgiver deres personoplysninger og omvendt heller ikke, hvor begge kundetyper afgiver deres personoplysninger.

Resultat på Signaling spillet

Ud fra dette Signaling spil kan det udledes, at der findes en separat ligevægt, men ingen pooling ligevægt. En separat ligevægt findes, hvor de ikke-kriminelle kunder afgiver deres personoplysninger, og hvor de kriminelle kunder modsat vis, ikke afgiver deres personoplysninger. Denne separate ligevægt udgør, at der i Signaling spillet, er tale om en Perfekt Bayesian ligevægt.¹⁹⁸ En pooling ligevægt findes ikke i spillet, da ingen af kundetyperne vil have incitament til at vælge den samme strategi. Dette består i, at begge kundetyper får et bedre payoff ved hver især at holde sig til deres Best Response strategi. Med dette resultat kan det udledes, at hvis kunderne er villige til at signalere, hvilken kundetype de er, så vil den asymmetriske information under forretningsforbindelsens levetid mindske og herved vil også dødvægtstabet mindske.

4.1.2 Screening teori

I dette spil er bankerne med stadighed den uinformerede part, og kunderne er den informerede part. Screening finder sted, når bankerne kan vælge at foretage handlinger, som vil påvirke kunderne til at handle på en måde, som vil afsløre deres private information, om hvilken type kunder de er.¹⁹⁹

I dette Screening spil undersøges det, om der er mulighed for, at bankerne kan screene kunderne ved etableringen af en forretningsforbindelse, ved at bede dem om at afgive deres personoplysninger. Dette vil give bankerne en mulighed for at kunne udlede information om kundernes type, ud fra deres respons til denne anmodning. Det undersøges derfor, om det er muligt at finde en separat ligevægt i spillet.

Ved et Screening spil, er det bankerne som den uinformerede spiller, der foretager første træk.²⁰⁰ I spillet bliver nature igen inddraget som samme karakter som i forrige Signaling spil.²⁰¹

¹⁹⁸ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 84.

¹⁹⁹ Ibid. side 123.

²⁰⁰ Ibid. side 153.

²⁰¹ Ibid. side 126.

I dette spil har kunderne fuldstændig information,²⁰² idet der er tale om et sekventielt spil, hvor kunderne kan observere bankernes tidligere foretagne træk, og hvor kunderne kender til deres egen type.²⁰³ Bankerne kender som nævnt ikke kundernes type, men de antager, at der er 10 procent sandsynlighed for, at kunderne er kriminelle og 90 procent sandsynlighed for, at kunderne ikke er kriminelle. Betydningen af den stiplede linje i spillet er, at bankerne ikke har kendskab til kundernes forrige foretagne træk.²⁰⁴

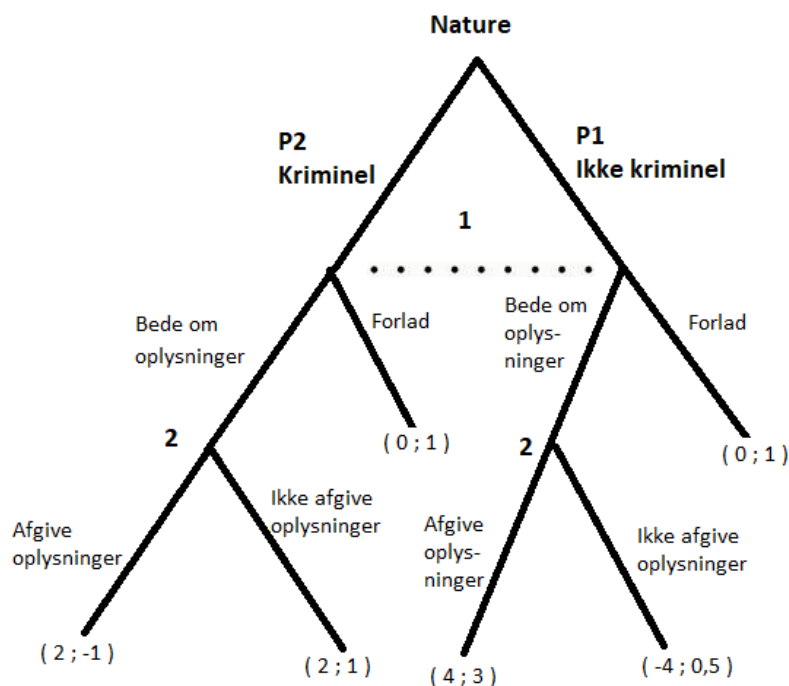
De payoffs som er benyttet i dette Screening spil, er approksimativt de samme som blev benyttet i Signaling spillet. Forskellen ligger i, at det antages, at bankerne altid foretager den korrekte risikovurdering af kunderne, baseret på kundernes respons til bankernes anmodning. Bankerne har i dette spil to træk til at kunne screene kunderne; enten beder bankerne kunderne om deres personoplysninger, eller også forlader bankerne spillet. Forlader bankerne spillet, vil dette resultere i, at bankerne ikke screener kunderne. Baseret på bankernes strategier, har kunderne også to strategier; enten afgiver de deres personoplysninger eller også tilbageholder de deres personoplysninger.

I spillet vil bankerne være spiller 1 (P1) og kunderne vil være spiller 2 (P2). Spillet vil se således ud:

²⁰² Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 153.

²⁰³ Ibid. side 312.

²⁰⁴ Ibid. side 126.



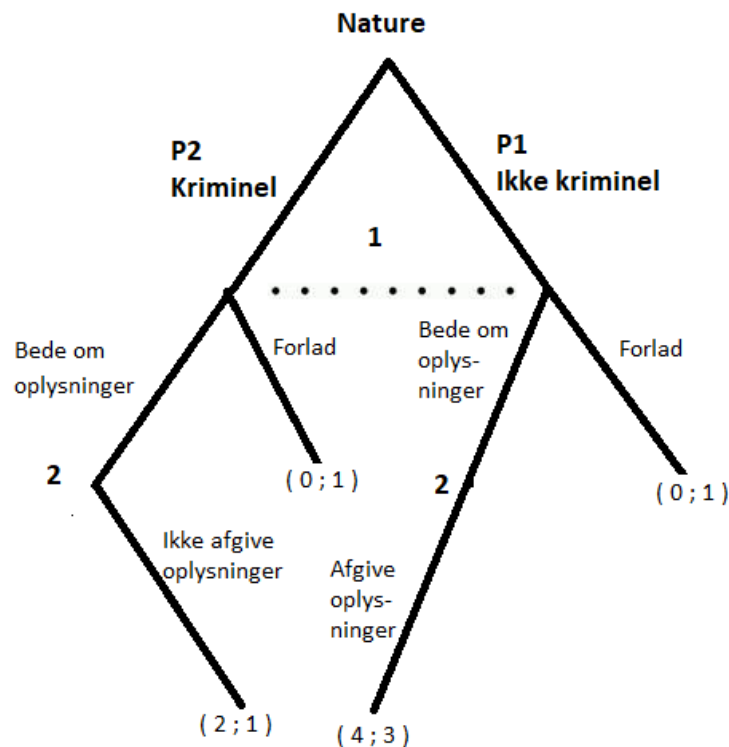
Figur 7. Egen tilvirkning.

For at kunderne kan udlede deres bedste strategier set i forhold til deres kundetype, benyttes kan de principperne for backwards induction. Backwards induction er en metode, hvor spillerne analyser deres mulige strategier, hvorved den strategi som vil resultere i det højeste payoff identificeres. Herefter omskrives spillet, så spillerne kun agter at benytte sig af disse strategier.²⁰⁵

Ved at benytte metoden backwards induction, findes de strategier, som resulterer i det højeste payoff for kunderne. Anmoder bankerne kunderne om deres personoplysninger, består de kriminelle kunders strategi i ikke at afgive deres personoplysninger. Årsagen til dette er, at et payoff på +1 er højere end -1. Hvis kunderne derimod ikke er kriminelle kunder, vil deres strategi bestå i at afgive deres personoplysninger ved anmodning herom fra bankerne. Årsagen herfor består i, at kunderne vil få et payoff på +3, fremfor et payoff på +0,5, ved ikke at afgive deres personoplysninger. Hvis bankerne benytter strategien; at de forlader spillet, vil kunderne ikke have mulighed for at foretage deres træk. Det er derfor ikke en mulig strategi for kunderne, omend de opnår et payoff på +1 herfor. Dette uanfægtet deres kundetype.

Spillet vil herefter blive omskrevet til at se således ud:

²⁰⁵ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 302.



Figur 8. Egen tilvirkning.

Nu er det bankerne, der skal udlede deres bedste strategi. For at udlede dette, skal bankerne have fokus på, hvad der fremadrettet kan ske i spillet. Bankerne kan benytte sig af to mulige strategier; at forlade spillet eller at bede kunderne om deres personoplysninger. Bankernes bedste strategi kan udledes på to måder. Den første metode er ved at udlede, hvilken af de to strategier, der for bankerne resulterer i det højeste forventede payoff. For at udregne de forventede payoffs, anvendes disse udregninger:²⁰⁶

$$U(\text{forlad}) = (0,1 * 0) + (0,9 * 0) = 0$$

$$U(\text{bede om personoplysninger}) = (0,1 * 2) + (0,9 * 4) = 3,8$$

Det kan ses i spillet, at hvis bankerne vælger strategien forlad, vil bankernes forventede payoff bestå i +0, uanfægtet kundetypen.

Ved bankernes anden strategi, at de beder kunderne om deres personoplysninger, vil bankerne med 10 procent sandsynlighed få et payoff på +2 og med 90 procent sandsynlighed få et payoff på +4.

²⁰⁶ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 154.

Dette resulterer i, at det forventede payoff for bankerne ved at benytte denne strategi, er på +3,8. Dette payoff på +3,8 er højere end det payoff, som bankerne vil få på +0 ved at benytte strategien forlad, og med udspring af dette, vil bankerne altid benytte strategien at bede kunderne om deres personoplysninger. Strategien at bankerne beder kunderne om deres personoplysninger, vil blive anvendt med den overbevisning, at kunderne med en sandsynlighed på 90 procent vil vise sig at være ikke-kriminelle kunder, og med en sandsynlighed på 10 procent, vil vise sig at være kriminelle.

Den anden metode, som kan benyttes til at finde bankernes bedste strategi, er ved at anvende bankernes forudgående overbevisninger. Som nævnt i afsnittet om Bayesian spillet, så forventes det med afsæt i Bayes' regel, at spillerne handler rationelt set i forhold til deres overbevisninger.²⁰⁷ Betydningen af dette er, at bankerne har den overbevisning, at de kriminelle kunder aldrig vil afgive deres personoplysninger og at de ikke-kriminelle kunder altid vil afgive deres personoplysninger. Med denne overbevisning, vil det være enkelt for bankerne at udvælge den strategi, som resulterer i det højeste payoff. Bankerne opnår et payoff på +2 for de kriminelle kunder, der ikke vil afgive deres personoplysninger og et payoff på +4 for de ikke-kriminelle kunder, der gerne vil afgive deres personoplysninger. Vælger bankerne at forlade spillet vil de få et payoff på +0. Strategien at bede kunderne om deres personoplysninger, vil derfor være bankernes bedste strategi baseret på Bayes' regel.

Som nævnt tidligere i dette spil, har de kriminelle og de ikke-kriminelle kunder hver især deres mulige strategier. De kriminelle kunder opnår det højeste payoff ved ikke at afgive deres personoplysninger, og de ikke-kriminelle kunder får det højeste payoff ved at afgive deres personoplysninger. Disse strategier er derfor Screening spillets Bayesian Nash ligevægte.²⁰⁸ Det er i dette spil muligt at udlede en separat ligevægt, da de to kundetyper ikke har incitament til at benytte sig af den samme strategi, når bankerne anmoder dem om deres personoplysninger. Kundetyperne har derimod incitament at benytte sig af differentierende strategier ved bankernes anmodning.

Resultat af Screening spil

Det kan udledes i dette Screening spil, at bankerne ved en Screening af kunderne, har mulighed for at kunne adskille de kriminelle og de ikke-kriminelle kunder fra hinanden. Årsagen til dette er, at de

²⁰⁷ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 154.

²⁰⁸ Ibid. side 310.

kriminelle og de ikke-kriminelle kunder vil respondere differentierende på bankernes forespørgsel, når bankerne anmoder dem om deres personoplysninger ved etableringen af forretningsforbindelsen. Resultatet af screening spillet er dermed, at det vil det være muligt for bankerne at udskille de kriminelle kunder fra de ikke-kriminelle kunder, hvilket vil medvirke til en formindskelse af den asymmetriske information og ligeså dødvægtstabet.

4.1.3 Principal-agent problemet

Som beskrevet i afsnit 1.4.3 vedrørende den økonomiske metode, så anvendes P/A teorien i denne afhandling med henblik på at forsøge at løse det opstillede Bayesian spil med ufuldstændig information. Den ufuldstændige information består i den asymmetriske information, der optræder i forholdet mellem bankerne og deres kunder. Afsnittet vil starte med at belyse og inddrage P/A teorien og dens elementer, hvorefter det vil ansues i sammenhæng med den foreliggende asymmetriske information. Først vil forholdet mellem bankerne og kunderne analyseres ud fra P/A teorien, hvorefter P/A teorien anvendes af mere dybdegående karakter. Her vil problematikken vedrørende den asymmetriske information forsøges løst gennem forskellige løsningsforslag. Afsluttende vil P/A teorien anvendes til analysering med inddragelse af ovenstående Signaling og Screening spil.

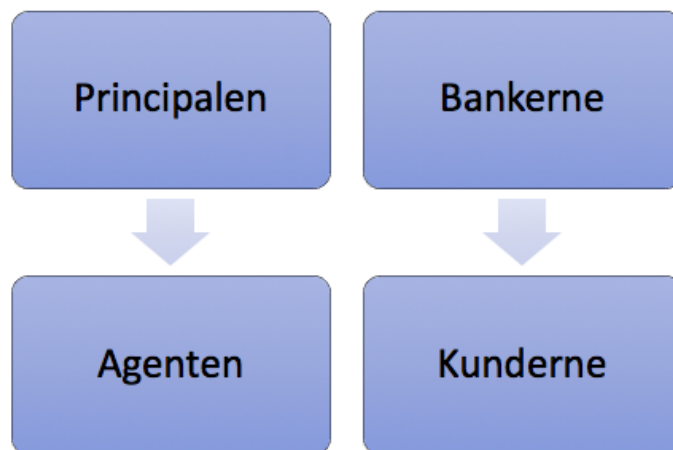
Et principal-agent forhold kendetegnes ved et forhold mellem to parter, hvoraf den ene part, agenten har information, som ikke er synlig for den anden part, principalen. Det er forholdet mellem disse to parter, som analyseres.²⁰⁹ P/A teorien bygger på den problematik, som kan opstå i forholdet mellem principalen og agenten angående hver parts interne viden, som ikke er synlig for modparten. På baggrund af dette opstår der asymmetrisk information.

4.1.3.1 Den asymmetriske information mellem bankerne og kunderne

I dette afsnit behandles situationerne, hvor en forretningsforbindelse mellem bankerne og kunderne skal etableres samt hvor der allerede foreligger en igangværende forretningsforbindelse mellem

²⁰⁹ Knudsen, Christian "Økonomisk metodologi bind 2 - virksomhedsteori og industriøkonomi" 2. Udg. 1997, side 164.

bankerne og kunderne. I begge situationer foreligger der asymmetrisk information. Formålet er at finde frem til, hvorledes bankerne i disse situationer kan undgå P/A problematikker, når de skal behandle kundernes personoplysninger til brug for udførelsen af en kundekendskabsprocedure, samt en eventuelt skærpet kundekendskabsprocedure.



Figur 9. Egen tilvirkning.

Det kan ses i figur 9, at bankerne er principalen, idet at bankerne ønsker at kunne kende forskel på kunderne set i forhold til deres risikoprofil for hvidvask af penge. Af denne grund vil agenten i dette forhold være kunderne, der ikke vil afgive deres personoplysninger.²¹⁰ Der kan forekomme modstridende incitament, og bankerne besidder som nævnt ikke nok information til at kunne adskille de almindelige og de øgede risikokunder fra hinanden.²¹¹

P/A teorien bygger på, at der er en informationsasymmetri i forholdet mellem principalen og agenten. Denne asymmetri er opstået fordi kunderne er bekendt med, om de hvidvasker penge eller om de ikke hvidvasker penge.²¹² Dette er bankerne ikke bekendt med, da det ikke er muligt for bankerne at observere kunderne fuldt ud og overvåge kunderne således, at denne asymmetriske information ikke indtræffer. Ved at benytte P/A teorien, søges det at udlede en måde, hvorpå incitamenterne mellem

²¹⁰ Knudsen, Christian "Økonomisk metodologi bind 2 - virksomhedsteori og industriøkonomi" 2. Udg. 1997, side 164.

²¹¹ Ibid.

²¹² Knudsen, Christian "Økonomisk metodologi bind 2 - virksomhedsteori og industriøkonomi" 2. Udg. 1997, side 164.

kunderne og bankerne kan forenes.²¹³ Dette gøres ved at påvirke kunderne til, i egen interesse, at handle således, at det er i overensstemmelse med bankernes interesser.²¹⁴

4.1.3.2 Adverse Selection og Moral Hazard

P/A teorien består hovedsageligt af to teoretiske begreber, der behandler problematikken ved asymmetrisk information; Adverse Selection og Moral Hazard.²¹⁵ Denne problematik forekommer, når agenten på bekostning af principalen, drager nytte af den viden, som principalen ikke har kendskab til.²¹⁶

Adverse Selection knytter sig til ex ante fasen, hvor den asymmetriske information eksisterer ved etablering af forretningsforbindelse.²¹⁷ Dette kan kaldes en ex ante usikkerhed. På dette tidspunkt vedrører usikkerheden, at kunderne besidder en mængde information, som det ikke er muligt for bankerne at observere.²¹⁸ Bankerne har dermed på dette tidspunkt ikke det fuldstændige kendskab til kundernes mængde af information eller kendskab til deres incitamenter. Dette bevirker, at der foreligger en informationsasymmetri i forholdet mellem bankerne og kunderne. Bankerne må derfor anvende tiltag, for at kunne varetage egne interesser; herunder kun at etablere en forretningsforbindelse med ikke-kriminelle kunder, og kunne genkende de kriminelle kunder. Adverse Selection problematikken opstår, når bankerne ikke har evner og viden nok til at kunne skelne de kriminelle og de ikke-kriminelle kunder fra hinanden.

Denne asymmetriske information kan medføre den konsekvens, at hvis det som eksempel²¹⁹ antages, at der er en række kunder, hvor en del af kunderne er kriminelle, andre er overhovedet ikke kriminelle og nogle ligger midt imellem disse to kundetyper. Da der foreligger denne informationsasymmetri i forholdet, vil bankerne ved etablering af en forretningsforbindelse ikke vide, hvor meget og hvilken information de skal anmode kunderne om. Har bankerne en mistanke om, at kunderne kunne være kriminelle, skal bankerne indsamle mere og anden information end ved ikke-kriminelle kunder.

²¹³ Ibid. side 165.

²¹⁴ Ibid. side 164-165.

²¹⁵ Ibid. side 165.

²¹⁶ Ibid. side 164.

²¹⁷ Ibid. side 165.

²¹⁸ Ibid.

²¹⁹ Dette eksempel er perspektiveret til det almene fænomen, som forefindes i forsikringsbranchen.

Bevirket af, at der foreligger informationsasymmetri, er bankerne ikke bekendt med, hvilken information de skal indsamle og omfanget af denne. Bankerne er derfor nødsaget til at udføre en gennemsnitlig indsamling for alle kunderne, der ønsker at etablere en forretningsforbindelse. Denne gennemsnitlige indsamling består i et gennemsnit mellem det som bankerne vil indsamle, hvis kunderne er kriminelle og det de vil indsamle, hvis kunderne ikke er kriminelle. Da kunderne selv er bekendt med deres kundetype, ønsker de ikke-kriminelle kunder ikke at afgive unødvendig og ikke relevant information fordi de ikke anser en relevans og nødvendighed forbundet med dette. Denne vil bevirke, at de ikke-kriminelle kunder falder fra ved denne gennemsnitsindsamling. Herefter vil gennemsnitsindsamlingen ændre sig til at omfatte, at bankerne ønsker at indsamle endnu mere information. På dette tidspunkt er det kun de midt imellem typer kunder, der er tilbage samt de kriminelle kunder. Således vil gennemsnitsindsamlingen fastsættes ud fra en et gennemsnit for bankernes indsamling af disse to kundetyper. Herved vil kunderne, der så nu er de mindst kriminelle kunder (midt imellem kunder) falde fra og således vil det fortsætte indtil, at det kun er de kriminelle kunder, der er tilbage. Det ses derfor, at der foreligger et informationsproblem.²²⁰ Der er forskellige løsningsforslag, som kan hjælpe til at forsøge at løse dette informationsproblem. Det er blandt andet forsøgt løst i afsnit 4.1.1 og 4.1.2 at løse dette informationsproblem ud fra et Signaling og Screening spil.²²¹

Moral Hazard knytter sig til ex post fasen, som foreligger efter, at der er sket etablering af forretningsforbindelsen, og kan herved anses som en ex post usikkerhed.²²² Det vil sige, at der ved Moral Hazard knytter sig et Hidden Action problem til, idet at principalen ex post ikke har viden om, hvad agenten foretager sig.²²³

Der findes to måder, hvorpå et Moral Hazard problem kan søges løst. Den ene metode, er ved at få forenet principalen og agentens incitamenter. Den anden metode består i at mindske den asymmetriske information, således at begge parter nogenlunde besidder samme mængde information. Hvis der mellem principalen og agenten foreligger samme incitament, ville der ikke forekomme

²²⁰ Knudsen, Christian "Økonomisk metodologi bind 2 - virksomhedsteori og industriøkonomi" 2. Udg. 1997, side 165.

²²¹ Ibid.

²²² Ibid. side 167.

²²³ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 153.

Adverse Selection og Moral Hazard problemer.²²⁴ Det vil være muligt at reducere risikoen for Adverse Selection og Moral Hazard problemer ved benyttelse af nedenstående foranstaltninger:

4.1.3.2.1 Tredjepartsvurdering

En objektiv vurdering fra en uafhængig tredjepart, kan være en foranstaltning til det Adverse Selection problem, der opstår hos bankerne ved etableringen af en forretningsforbindelse.²²⁵ Ved denne foranstaltning vil det være kunderne, som er påkrævet at skulle få foretaget en vurdering af en uafhængig tredjepart. Vurderingen vil kunderne skulle fremvise for bankerne, hvor bankerne herefter, uden at foretage en selvstændig vurdering af kunderne, kan etablere en forretningsforbindelse med pågældende kunde, såfremt bankerne ønsker dette. Denne foranstaltning vil medføre den effekt, at den vurdering som bankerne skal foretage af kunderne i forbindelse med etablering af en forretningsforbindelse bliver outsourcet til en uafhængig tredjepart. Dette vil dog ikke forhindre bankerne i at kunne foretage en yderligere vurdering af kunderne, med afsæt i denne uafhængige tredjepartsvurdering. Dette kan bidrage til at mindske Adverse Selection problemet, ved at kunderne skal kunne fremvise denne vurdering, og derigennem giver bankerne adgang til deres informationer. Det skal dog understreges, at denne uafhængige tredjepart, skal være en part, der ikke opnår gevinst af vurderingens udfald.

Det ses på andre markeder med informationsasymmetri, at en uafhængig tredjepartsvurdering gavner til at mindske informationsasymmetrien; for eksempel ved køb af en ejendom. Ved en ejendomshandel er køber ikke bekendt med andre fejl og mangler end, hvad ejendomsmægler og sælger har oplyst ham om. I dette eksempel er køber den uinformede part og sælger er den informerede part. For at køber kan søge at mindske den asymmetriske information, der foreligger mellem dem, kan køber kontakte en uafhængig byggesagkyndig. Denne uafhængige byggesagkyndige skal gennemgå ejendommen for eventuelle fejl og mangler, og må ikke selv udrede det fundne. Begrundelsen herfor er, at den byggesagkyndige ikke skal have incitament til hverken at

²²⁴ Laffont, Jean-Jacques & Martimort, David "The Theory of Incentives - the principal-agent model" 1. Udg. 2002, side 146.

²²⁵ Knudsen, Christian "Økonomisk metodologi bind 2 - virksomhedsteori og industriøkonomi" 2. Udg. 1997, side 166.

finde flere eller mindre fejl og mangler, end hvad korrekt er. I dette eksempel er købers køb af ejendommen dog ikke betinget af denne vurdering

Det kan opstå tvivl, om hvorvidt dette vil være for stort et krav at pålægge kunderne, at de skal få foretaget denne tredjepartsvurdering forud for en etablering i bankerne. Årsagen herfor er, at det ikke er kunderne, der besidder mindst information, men derimod bankerne, hvorfor det er bankerne, der ønsker at mindske informationsasymmetrien. Når eksempelvis danske statsborgere vil tage et kørekort. Her er de påkrævet ved lov, at skulle have en sundhedserklæring fra deres læge, som de skal kunne fremvise for at få et kørekort.²²⁶ I dette eksempel fremgår det, at det er borgerne selv, som er medvirkende til at mindske informationsasymmetrien angående deres helbred. Hvis denne tredjepartsvurdering blev et påkrav fremsat ved lov, vil kunderne være nødsaget til at få foretaget denne tredjepartsvurdering, hvis de ønsker etablering i bankerne. Der er her tale om en Signaling løsning. Dette ses endvidere i Signaling spillet i afsnit 4.1.1, at dette vil resultere i, at der forekommer en separat ligevægt, og at det herved vil være muligt for bankerne at kunne kende forskel på de respektive kunder, som ønsker etablerer sig i bankerne.

Der anskues dog et negativt aspekt ved denne tredjepartsvurdering, idet at den udelukkende vil mindske informationsasymmetrien ved etablering af forretningsforbindelse. Denne tredjepartsvurdering vil ikke have validitet efter, at der er sket etablering. Grunden herfor er, at kunderne har mulighed, for at ændre sig og handle anderledes, end hvad de var vurderet til på det pågældende tidspunkt, hvor tredjepartsvurderingen blev foretaget. Der vil med afsæt i dette opstå et Hidden Action problem.²²⁷

Denne foranstaltning vil ikke nødvendigvis være af særlig omkostningsmæssig karakter for bankerne. For bankerne vil dette ikke umiddelbart resultere i ekstra pålagte omkostninger, da det er kunderne, som vil skulle bære omkostningen for tredjepartsvurderingen. Der forekommer tvivl om, hvordan prissætningen af en sådan vurdering skal foretages, omend der være tale om en enkeltstående omkostning.

²²⁶ Kørekortbekendtgørelsen, nr 815 af 21/06/2017, § 32.

²²⁷ Hoppe, Eva I. & Schmitz, Patrick W. "Hidden action and outcome contractibility: An experimental test of moral hazard theory" Games and Economic behaviour 109 (2018), side 544.

Det kan med afsæt i ovenstående udledes, at dette Adverse Selection problem vil kunne søge løst ved, at staten eller bankerne påkræver, at kunderne ved etablering af en forretningsforbindelse skal have foretaget en vurdering hos en uafhængig tredjepart. Denne tredjepartsvurdering skal kunderne kunne fremvise for bankerne med formålet om at bankerne kan vurdere kundernes risiko. Dette vil være medvirkende til at mindske den asymmetriske information, der foreligger ex ante mellem bankerne og kunderne.

4.1.3.2.2 Overvågning

Det forhold, at bankerne overvåger kunderne, vil være en løsning til det Moral Hazard problem, der kan opstå efter etablering, idet at der forekommer en ex post usikkerhed.²²⁸ Problematikken består i, at bankerne ikke vil være bevidne om hvorvidt kunderne efter etablering, har i sinde at foretage hvidvask af penge gennem bankerne. Dette består i et Hidden Action problem.²²⁹ Løsningen hvorved at bankerne skal foretage en fuld overvågning af kunderne efter etablering vil kunne mindske Hidden Action problematikken. Årsagen hertil er, at bankerne vil have mulighed for at kunne observere kundernes handlinger og transaktioner. Ved at bankerne har mulighed for dette, kan dette mindske ex post usikkerheden, idet at bankerne vil komme i besiddelse af mere information om kunderne, og heraf mindskes den asymmetriske information, der foreligger mellem parterne.

Det ses, at overvågning anvendes i mange brancher, hyppigst i et arbejdsgiver- og arbejdstagerforhold. Her er arbejdsgiverne er principalen og arbejdstagerne er agenten. Arbejdsgiverne vil typisk sikre, at arbejdstagerne handler i arbejdsgivernes interesse.²³⁰ For at finde frem til, om dette er tilfældet, kan arbejdsgiverne overvåge arbejdstagerne.²³¹ På denne vis mindskes den informationsasymmetri, som foreligger.

²²⁸ Linder, Stefan & Foss, Nicolai, J. "Agency Theory" SMG working paper No. 7/2013, side 11.

²²⁹ Hoppe, Eva I. & Schmitz, Patrick W. "Hidden action and outcome contractibility: An experimental test of moral hazard theory" Games and Economic behaviour 109 (2018), side 544.

²³⁰ Møller, Michael & Nielsen, Niels C. "Din Økonomi. En bog om tid og penge" 4. Udg. 1. opl. 2015, side 188.

²³¹ Anderson, E. & R.L. Oliver "Perspectives on behavior-based versus outcome-based sales force control systems." Journal of Marketing, 51(October), 1987, side 76.

Ved bankernes anvendelse af overvågning af kunderne, vil det være muligt for bankerne at overvåge om kundernes transaktioner, er i overensstemmelse med bankernes interesse om at bekæmpe hvidvask af penge. Derudover vil det være muligt for bankerne ved overvågning, at opdage mistænksomme transaktioner hos kunderne, hvor dette vil kunne bruges som belæg for iværksættelse af en undersøgelse af kunderne. Det antages dog, at bankernes overvågning af kunderne, ikke kan udføres på et fuldt ud tilfredsstillende niveau, da overvågningen ikke vil kunne eliminere informationsasymmetrien fuldstændig mellem bankerne og kunderne. Grunden herfor er, at der anvendes kontanter i samfundet. I 2015 bestod 20 procent af den samlede omsætning i detailhandlen fra kontantbetalinger.²³² Der hvor problematikken opstår, er i situationer, hvor kunderne udfører arbejde, hvorved de modtager betaling i form af kontanter, som de ikke betaler skat af. Disse kontantbetalinger vil ikke være mulige for bankerne at overvåge. Dette medfører, at der med stadighed kan forekomme informationsasymmetri mellem kunderne og bankerne, selvom der foretages fuld overvågning af kundernes bankaktiviteter. Denne problematik kan søges løst, hvis bankerne havde ansatte til fysisk at forfølge kunderne, og på denne vis overvåge alle kunderne kontantaktiviteter. Dog anses dette for at være omkostningsfuldt for bankerne og findes derfor ikke som en efficient løsning.

Denne overvågningsforanstaltning til Moral Hazard problematikken, kan anses for at være en god løsning. Dette med den begrundelse, at bankerne skal foretage fuld overvågning af kundernes bankaktiviteter, for at forhindre et Hidden Action problem. Overvågningen antages ikke at være særlig omkostningsfuld for bankerne at udføre. Årsagen hertil er, at det som nævnt kun vil være muligt at overvåge de elektroniske bankaktiviteter, hvorved dette antages at kunne foregå gennem bankernes egne IT-systemer.

Ved overvågning af kunderne vil den asymmetriske information mellem bankerne og kunderne kunne mindskes. Det findes ikke, at det kan fuldstændig udligne informationsasymmetrien, idet at der anvendes kontanter i samfundet, hvilke det ikke vil være muligt for bankerne at overvåge.

²³² Betalingsrådet "Rapport om Kontanternes Rolle i Samfundet" Juni 2016, Nationalbanken, side 5.

4.1.3.2.3 Indgåelse af kontrakt

Med formålet om at udligne den asymmetriske information, der foreligger mellem bankerne og kunderne som både en ex ante og en ex post usikkerhed, kan dette søges gjort ved, at bankerne forsøger at forene kundernes incitamenter med sine egne. Bankerne kan ved etablering af forretningsforbindelser kræve af kunderne, at der indgår en kontrakt med bankerne, konciperet af bankerne. Bankerne kan ved indgåelse af en kontrakt med kunderne søge at påvirke kunderne til at forene deres incitamenter bankernes.²³³ Bankerne vil gennem kontrakten søge at give kunderne incitament til ikke at ville benytte den asymmetriske information, som de besidder, og bankerne ikke har kendskab til. Denne forening af incitamenterne kan bankerne søge at opnå ved, at de i kontrakten opstiller sanktioner, som vil indtræde, hvis kunderne bryder kontrakten.²³⁴ Idet at bankerne ikke er bekendt med kundernes type, opstilles disse sanktioner af en sådan størrelse, der vil være til meget stor ugunst for kunderne. Sanktionernes størrelse fastsættes således, så kriminelle kunder ikke vil have incitament til at bryde kontrakten. Grunden herfor er, at sanktionerne skal være til så stor ugunst for kunderne, at det ikke vil være efficient for dem at bryde kontrakten. Udgør størrelsen på sanktionerne mindre end hvad udbyttet for hvidvask af penge gør, vil sanktionerne ikke forhindre, at kriminelle kunder bryder kontrakten. Ikke-kriminelle kunder vil ikke finde det problematisk at indgå denne kontrakt med bankerne, da de ikke har til hensigt at bryde kontakten samt det forhold, at de ønsker at signalere over for bankerne, at de ikke er kriminelle.

Hvis bankerne betinger, at der ved etablering af en forretningsforbindelse, skal indgås en kontrakt, vil dette kunne udligne den asymmetriske information. Dette med argumentation for, at de kriminelle kunder ikke vil have incitament til at indgå en kontrakt med bankerne, som indeholder meget ugunstige sanktioner, hvis kunderne bryder kontrakten. De ikke-kriminelle kunder vil ikke se en problematik forbundet hermed, da de ikke agter at bryde kontrakten. Ud fra dette vil kunderne ved at betinge en kontrakt ved etablering kunne screene kunderne og adskille kundetyperne fra hinanden. til at bryde kontrakten.

²³³ Müller, Ralf & Turner, J. Rodney "The impact of principal-agent relationship and contract type on communication between project owner and manager" *International Journal of Project Management*, 2005, vol 23(5), side 399.

²³⁴ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 150.

Tiltaget bevirker dermed til at mindske den asymmetriske information, der foreligger som en Adverse Selection og Moral Hazard; herved informationsasymmetrien ved etableringen og gennem forretningsforbindelsens levetid.

4.1.3.2.4 Bevisbyrde

Ved benyttelse af P/A teorien, er det muligt at pålægge agenten bevisbyrden. Dette med formålet om, at agenten skal besidde samme incitament som principalen. Ved forekomsten af et asymmetrisk informationsproblem, kan dette søges løst ved at pålægge kunderne bevisbyrden. Ved at pålægge kunderne bevisbyrden, vil det være kunderne, som skal påvise, at deres likvide midler ikke stammer fra kriminelle aktiviteter. Denne bevisbyrde kan eksempelvis pålægges kunderne ved, at de skal kunne fremvise kvitteringer eller anden form for dokumentation for hver kontant indbetaling i bankerne. Som et andet tiltag til, at kunderne skal bære bevisbyrden for sine bankaktiviteter, kan dette ske ved, at kunderne ved elektroniske transaktioner, skal kunne påvise dokumentation for formålet med den pågældende transaktion.

Formålet og det ønskede resultat af dette tiltag fra bankernes side er, at det skal udligne den asymmetriske information, der foreligger mellem bankerne og kunderne. Ved bankernes besiddelse af information vedrørende alle kundernes transaktioner, vil bankerne have mulighed for at mindske den asymmetriske information betydeligt. Dette med argumentation i, at bankerne ikke længere vil besidde tvivlsspørgsmål angående kundernes midlers oprindelse. Ved at pålægge kunderne dette dokumentationskrav, vil det ikke være muligt for kunderne at foretage transaktioner uden, at disse transaktioner efterfølgende skal dokumenteres overfor bankerne. Det må antages, at kunderne udviser en opportunistisk²³⁵ og diskretionær opførelse. Med dette menes der, at kunderne vil ændre på deres opførsel med formålet, om at optimere egen profit og følge egne interesser.²³⁶ På baggrund af dette, vil kunderne, for at optimere deres profit og interesser altid sikre sig, at de kan fremvise dokumentation for deres transaktioner, da det ellers vil være umuligt for kunderne at foretage transaktioner gennem bankerne.

²³⁵ Pauline T. Kim "Beyond Principal-Agent Theories: Law and The Judicial Hierarchy" Vol. 105, No. 2, side 545.

²³⁶ Knudsen, Christian "Økonomisk metodologi bind 2 - virksomhedsteori og industriøkonomi" 2. Udg. 1997, side 164.

Kravet om bevisbyrde kan betragtes som, at bankerne konstant foretager en screening af sine kunder. Ved anvendelse af denne metode, vil det desuden være muligt for bankerne at kunne adskille de kriminelle kunder fra de ikke-kriminelle kunder. Dette med begrundelse i, at det må antages, at de kriminelle kunder ikke vil kunne fremvise dokumentation for oprindelsen af deres likvide midler. Af denne årsag, vil det ikke være muligt for de kriminelle kunder at anvende bankerne til at foretage hvidvask af penge.

Dette løsningsforslag søger både at løse det problem, der foreligger ex ante og ex post. Bankerne kan vælge at kræve, at de kunderne i forbindelse med etablering af en forretningsforbindelse skal kunne fremvise bevis for, hvor deres formue stammer fra. Beviskravet opstilles med formålet, om at mindske den informationsasymmetri, som knytter sig til ex ante usikkerheden. Herudover kan bankerne under forretningsforbindelsens levetid kræve bevis og dokumentation for alle udgående og indgående transaktioner samt for kontante bankaktiviteter. Resultatet vil være, at både Adverse Selection, Moral Hazard og Hidden Action problemet løses.

Ved at pålægge kunderne bevisbyrden, vil det være muligt for bankerne at kunne mindske den asymmetriske information betydeligt. Det vil i den forbindelse også være muligt for bankerne at screene deres kunder med henblik på at udlede, hvem der foretager hvidvask af penge gennem bankerne.

4.2 Delkonklusion

Det kan konkluderes ved anvendelse af P/A teorien, at det er muligt at løse det opstillede Bayesian spil med asymmetrisk information. Løsningen skal ske på baggrund af en kombination af, at kunderne signalerer over for bankerne, at de ikke er kriminelle og herved uden anmodning fra bankerne, afgiver deres personoplysninger til bankerne. Dette i kombination med, at bankerne screener de kunderne ved etablering af en forretningsforbindelse. Denne screening foregår ved, at bankerne anmoder de potentielle kunder, om vedkommendes personoplysninger. Begge forslag til udligning af den asymmetriske information, omhandler den asymmetri, der foreligger ved etablering af en mulig forretningsforbindelse.

Signaling og Screening metoderne skal sammenholdes med de elementer, som findes i P/A teorien. Dette med formålet om at mindske den asymmetriske information på bedste vis. Ved anvendelse af P/A teorien, omhandler dette anvendelsen af påkrævede tredjepartsvurderinger, overvågning af kunderne, indgåelse af kontrakter med de potentielle kunder, og at bankerne indfører et krav om bevis for kunders midlers oprindelse i forbindelse med deres transaktioner.

Bankerne kan betinge kunderne, at hvis de ønsker at etablere sig i bankerne, skal de forinden have fået foretaget tredjepartsvurdering hos en uafhængig part. Denne vurdering skal omfatte den vurdering, som bankerne ellers selv ville være pålagt at skulle udføre ved etablering af en forretningsforbindelse. Ved at bankerne udliciterer denne vurdering mindskes den asymmetriske information, som foreligger mellem bankerne og kunderne ved etableringstidspunktet.

Overvågning af kunderne foregår under forretningsforbindelsens levetid. Løsningen indebærer, at bankerne skal overvåge kunderne, for så vidt muligt at kunne kende kundernes forhold og forhindre Hidden Action problemet, som forekommer efter, at der er sket etablering.

Bankerne kan ved etablering af en forretningsforbindelse betinge kunderne at skulle indgå en kontrakt med dem. I denne kontrakt vil bankerne have mulighed for at inkludere sanktioner ved brud på kontrakten. Disse sanktioner skal udgøre et beløb, som er højere end gevinsten som kriminelle kunder opnår ved hvidvask af penge. Sanktionerne kan bidrage til at mindske den asymmetriske information, der foreligger mellem kunderne og bankerne. Indgåelsen af kontrakten mellem bankerne og kunderne mindsker informationsasymmetrien, der foreligger ved etablering af forretningsforbindelserne, men sanktionerne består som en gældende klausul i kontrakten under hele forretningsforbindelsens levetid. Bankerne vil have mulighed for at screene kunderne, og ikke-kriminelle kunder vil have mulighed for at signalere over for bankerne, at de ikke er kriminelle ved at indgå i kontraktsforholdet. Med argumentation i ovenstående, er der derfor tale om en løsning, som henvender sig til både ex ante og ex post problematikkerne.

Sidste løsningsforslag består i, bankerne skal indføre en betingelse om, at kunderne skal bære bevisbyrden for deres likvide midlers oprindelse, hvilket skal ske i form af dokumentation, som kunderne skal kunne foreligge ved hver transaktion, udgående som indgående. Dette løsningsforslag henvender sig også til det Hidden Action problem, der forekommer.

Alle disse tiltag, foretaget i en kombination, vil være medvirkende til at mindske den asymmetriske information, der foreligger mellem kunderne og bankerne, og derfor bevirker disse tiltag til at løse det opstillede Bayesian spil. Det er blevet analyseret frem til, at dette er den optimale løsning til den asymmetriske information, som forekommer i afhandlingens Bayesian spil. Løsningen findes optimal da den forhindrer, at der opstår asymmetrisk information både ex ante og ex post. Løsningen er den mest efficiente løsning under den antagelse, at denne løsning ikke er mere omkostningsfuld end hvad hvidvask af penge koster samfundet. Med dette vil det sige, at omkostningerne forbundet med løsningsforslagene, ikke må overstige mere end fem procent af den globale BNP.

Kapitel 5

På baggrund af den juridiske analyse, skabes der er et negativt billede, vedrørende samarbejdet mellem bekæmpelse af hvidvask og forsøget på at beskytte individet ved behandling af deres personoplysninger. Det ses, at begge lovhjemler respektere hinanden, hvor GDPR tillader behandling af personoplysninger i forbindelse med bekæmpelse af hvidvask, dog med det forbehold, at principperne i forordningen overholdes, jf. GDPR artikel 6, stk.1, litra c og e. I 4AMLD står det udtrykkeligt, at tiltag, der skal udføres i kampen mod bekæmpelse af hvidvask af penge, skal ske med respekt for databeskyttelsesforordningen.²³⁷

Det ses, at bankerne ved etablering af en ny forretningsforbindelse med kunderne, skal foretage en kundekendskabsprocedure, jf. 4AMLD artikel 11. Hvis bankerne finder det relevant, skal denne kundekendskabsprocedure udvides til ydermere at omfatte en skærpet kundekendskabsprocedure, jf. 4AMLD artikel 18 ff. Formålet med denne procedure er at vurdere kundernes risikoprofil, og endvidere vurdere, om kunderne skal anses som øgede risiko kunder. Ved bankernes udførelse af en kundekendskabsprocedure, består indsamlingen til brug for denne, på baggrund af en vurdering af kunderne, ud fra en risikobaseret tilgang. Årsagen til, at 4AMLD tilsiger, at den risikobaserede tilgang skal benyttes, er med formålet, om at sikre en dynamisk og fleksibel lovgivning, som har til formål at forhindre, at kriminelle får mulighed, for at omgå lovgivningen.²³⁸ Hvis de kriminelle var bekendte med bankernes tilgang til udførelse af proceduren, ville dette besværliggøre bankernes arbejde, for at bekæmpe hvidvask af penge, da de kriminelle ville kunne planlægge at omgå loven.

Bankernes udførelsen af den skærpede kundekendskabsprocedure er underlagt princippet om dataminimering efter GDPR. Dataminimeringens principper kræver, at behandling af personoplysninger skal være tilstrækkelig, relevant og være begrænset til, hvad der er nødvendigt i forhold til de formål, som de behandles til, jf. GDPR artikel 5, stk. 1, litra c. Dataminimeringens principper lægger op til, at bankerne skal foretage en vurdering af den behandling, som de agter at foretage. Bankerne skal sikre at behandling findes i overensstemmelse med dataminimeringens principper. Dataminimeringen lægger samtidig op til, at bankerne skal foretage en subjektiv vurdering ved udførelsen af den skærpede kundekendskabsprocedure vedrørende, hvilke personoplysninger de

²³⁷ 4AMLD, præambelbetragtning nr. 65.

²³⁸ Jf. afsnit 3.1, formålsfortolkning af 4AMLD og GDPR.

skal indsamle om kunderne. Resultatet af den juridiske analyse påviste, at dataminimeringen påvirker formålet med den skærpede kundekendskabsprocedure. Den skærpede kundekendskabsprocedure kræver indsamling af store mængder af personoplysninger, for at kunne sikre korrekt risikovurdering af kunderne, både ved etableringen af forretningsforbindelsen, men også under forholdets levetid.

Der forekommer asymmetrisk information, baseret på, at kunderne har adgang til flere personoplysninger end bankerne. Informationsasymmetrien forekommer både ved forretningsforbindelsens etablering, men også under forretningsforbindelsens løbetid. Det dødvægtstab²³⁹, der skabes på baggrund af informationsasymmetrien, kan mindskes, ved at søge at udligne eller mindske informationsasymmetrien, som foreligger mellem bankerne og kunderne. Den asymmetriske information kan søges mindsket ved, at kunderne signalerer til bankerne, hvilken type kunde vedkommende er, om bankerne burde nære mistanke for mulig hvidvask af penge. Denne signalering består i, at kunderne af egen fri vilje afgiver personoplysninger til bankerne, uden bankernes anmodning herom. Modsat kundernes mulighed for at signalere deres type til bankerne, har bankerne mulighed for at screene deres kunder. Dette foregår ved, at bankerne anmoder kunderne, om afgivelse af vedkommendes personoplysninger. Ved anmodning om dette, vil det udelukkende være de kriminelle kunder, som ikke vil afgive personoplysninger, hvorved bankerne på baggrund af dette, vil kunne adskille kundetyperne fra hinanden.

Det vil derudover være muligt for bankerne at kunne mindske den asymmetriske information, der opstår ved etableringen af forretningsforbindelsen. Det søges gjort ved, at bankerne i forbindelse med etableringen af en forretningsforbindelse kræver, at kunderne får foretaget en vurdering af kundernes risiko for mulig hvidvask af penge hos en uafhængig tredjepart. Denne uafhængige tredjepart foretager udelukkende disse vurderinger som profession. Informationsasymmetrien kan også forsøges mindsket ved, at bankerne kræver kunderne at indgå en kontrakt i forbindelse med etableringen i bankerne. Denne kontrakt skal opstille ugunstige sanktioner, som indtræder, hvis kunderne bryder kontrakten. Kunder der er bevidste om at ville hvidvaske penge gennem bankerne, vil ved etableringstidspunktet ikke have incitament til at indgå kontrakten, dette med belæg i sanktionernes størrelse. Den informationsasymmetri, der foreligger ex post, i løbet af forretningsforbindelsens levetid, kan forhindres ved, at der sker fuld overvågning af kunderne, indførelsen af sanktioner og pålægge kunderne bevisbyrden for dennes transaktioner.

²³⁹ Det samfundsmæssige dødvægtstab, ved forekomsten af hvidvask af penge.

På baggrund af resultatet i den juridiske analyse, som fremviste gældende ret og de modstridende hensyn bag lovhjemlerne, sammenholdes dette med resultatet i den økonomiske analyse, som kom frem til det resultat, at en kombination af Signaling og Screening spillet samt de nævnte segmenter, som tilsammen vil kunne medvirke til at mindske den asymmetriske information.

Resultaterne fra den juridiske analyse sammenholdes med resultatet af den økonomiske analyse med formålet om at udlede den efficiente løsning til udførelsen af den skærpede kundekendskabsprocedure, men hvor udførelsen sker med overholdelse af principperne i dataminimeringen.

5.1 Løsninger sammenholdt med gældende ret

I dette afsnit søges det at analysere, om de løsningsforslag, som blev fundet i kapitel 4, kan anvendes i praksis, og om bankerne i forbindelse hermed, overholder principperne om dataminimeringen. Derudover undersøges det, hvilken løsning, som findes mest efficient for bankerne, og hvilken der kunne medvirke til at mindske det samfundsmæssige dødvægtstab. Dette sker under den antagelse, at lovgiverne angående hvidvask af penge, er gunstige for samfundet at udføre. Under denne antagelse, søges det at belyse, hvilke muligheder, der findes.

5.1.1 Signaling

Ved anvendelse af signaling, vil det forekomme, at det er kunderne, som skal udvise initiativet.²⁴⁰ Dette vil kunne ske ved, at kunderne frivilligt vælger at afgive personoplysninger, uden at bankerne skal tage initiativ til indsamling. Det er påvist under den økonomiske analyse, at hvis signaling forekommer, har bankerne mulighed, for at kunne kende forskel på kunderne, om det er kriminelle eller ikke-kriminelle kunder. Kriminelle kunder vil aldrig frivilligt afgive sine personoplysninger, idet det antages, at bankerne umiddelbart vil have mulighed for at vurdere kunderne som øgede risiko kunder og herunder muligvis kunder, der hvidvasker penge gennem bankerne. Økonomisk vil det, at kunderne afgiver sine personoplysninger frivilligt uden anmodning fra bankerne, løse den

²⁴⁰ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 124.

asymmetriske information, som opstår mellem bankerne og kunderne ved etableringen af forretningsforbindelsen. Ved denne løsning vil dødvægtstabet i samfundet mindskes og ikke udlignes. Årsagen til at dødvægtstabet ikke udlignes er, at hvidvask af penge, som foregår efter der er sket etablering af forretningsforbindelsen, ikke fanges af denne løsning. Betydningen af dette er, at det kun er den asymmetriske information, som forekommer før etableringen, som forsvinder, hvor der stadig findes asymmetrisk information under forretningsforbindelsens levetid.

Hvis denne løsning skal anvendes, kræves det at potentielle kunder som sagt, skal tage initiativ til afgive sine personoplysninger til bankerne. Dette initiativ vil juridisk være i overensstemmelse med reglerne i GDPR, idet, der er tale om en frivillig afgivelse af personoplysninger. Det vil dog være tvivlsomt, om denne metode juridisk vil kunne anvendes, da principperne om dataminimering, stadig finder anvendelse, selvom der er tale om en frivillig afgivelse af personoplysningerne. Det kan være svært for bankerne at vurdere, hvilke oplysninger, som kunderne frivilligt afgiver, er relevante set i forhold til behandlingsformålet, jf. GDPR artikel 5, stk. 1, litra c. Derudover, hvis kunderne afgiver personoplysninger uden, at bankerne anmoder om disse, er der en stor sandsynlighed for, at kunderne afgiver flere oplysninger end der findes tilstrækkeligt og nødvendigt set i forhold formålet for behandlingen, jf. GDPR artikel 5, stk. 1, litra c. Dette har af den betydning, at bankerne ikke vil kunne foretage en adskillelse af personoplysningerne, før der allerede er sket indsamling af disse og derved sker der overtrædelse af dataminimeringen. Selvom det omhandler, at det er de potentielle kunder, som afgiver personoplysninger til bankerne, skal der ved behandling af personoplysningerne, stadig være tale om en proportional behandling af disse.²⁴¹

Det er ikke muligt for bankerne at fastlægge, hvilke personoplysninger, der anvendes, ved kundernes signalering, da dette vil resultere i, at løsningen ikke vil være en signalering løsning. Hvis bankerne præciserer omfanget af personoplysninger, som anvendes, vil formålet bag 4AMLD's risikobaserede tilgang være overflydelig. Hensynet bag denne tilgang er at sikre, at kriminelle ikke kender til processen og udvikle metoder til, hvorledes de kan omgå loven.

Hvis der skal forekomme en mulig signalering fra kunderne, hvor der ikke sker overtrædelse af dataminimeringen for bankerne, skal kunderne selv foretage en vurdering af hvilke personoplysninger, som anses for tilstrækkelige, relevante og nødvendige til formålet. Hvis dette var

²⁴¹ Jf. GDPR præambelbetragtning nr. 4.

tilfældet, vil denne løsning være uanvendelig. Årsagen er at kunderne selv vurderer, hvad de vil oplyse bankerne, hvor de kriminelle derfor har mulighed for at omgå lovgivningen, ved at foretage en vurdering af, hvad de selv finder relevant. De kriminelle kunder kan herved oplyse færre personoplysninger end hvad, bankerne i realiteten har behov for. Ved sådan en metode, vil de kriminelle kunder have incitament til at imitere de ikke-kriminelle kunder og dermed ikke blive afsløret. Dette vil derfor ikke være en løsning, som anses som værende hverken effektiv eller efficient. Årsagen til dette er, at den informationsasymmetri, som forelå, stadig vil være til stede og ikke være reduceret, hvilket betyder, at dødvægtstabet er uændret.

For at en signaleringsløsning skal anses for brugbar, skal der være tale om, at kunderne frivilligt afgiver alle personoplysninger, hvilket betyder, at der vil indtræde komplet information mellem bankerne og de potentielle kunder. Løsningen kan dog ikke anses for at være mulig, da princippet om dataminimering beskytter de fysiske personer ved behandling af personoplysninger,²⁴² hvor kunderne er berettiget til ikke at oplyse alle deres personoplysninger, og kun de personoplysninger, som kan betragtes for at være tilstrækkelige og relevante, og derudover være begrænset til hvad der findes nødvendigt, jf. GDPR artikel 5, stk. 1, litra c.

5.1.2 Screening

Ved at foretage en screening, er det til forskel for signaling, at det er bankerne, der skal tage initiativet.²⁴³ For at bankerne kan screene kunderne, sker dette på baggrund, at de anmoder de potentielle kunder om deres personoplysninger. Baseret på om kunderne vælger at afgive sit samtykke til, at bankerne må indsamle dennes personoplysninger eller ikke, er det muligt for bankerne at udlede hvilken type kunder, som forekommer, om det er kriminelle eller ikke-kriminelle kunder. Der er her tale om en løsning, som henvender sig til den informationsasymmetri, der foreligger før etableringen af forretningsforbindelsen. Dette har af betydning, at der fortsat findes informationsasymmetri mellem kunderne og bankerne under forretningsforbindelsens levetid.

²⁴² Jf. GDPR præambelbetragtning nr. 2.

²⁴³ Baird, Douglas G. m.fl. "Game Theory and the Law" 1. Udg. 1998, side 153.

Foretager bankerne en screening af kunderne og forventer, at disse kunder samtykker til at afgive alle sine personoplysninger, er resultatet, at samfundets dødvægtstab mindskes, da det er muligt at kunne adskille de potentielle kunder fra hinanden. Dette vil opfange mange af de kriminelle kunder, og således kan mindske hvidvask af penge og påvirke dødvægtstabet i samfundet. Hvis bankerne foretager en god screening ex ante, kan det resultere i, at hvidvask af penge ex post, forhindres. Bankernes foretagelse af screening af kunderne, kan løse ex ante problemet. Dette kan dog ikke anses som en brugbar løsning for bankerne, årsagen herfor er, at principperne i dataminimering bearbejder denne løsning. Hvis kunderne samtykker til, at bankerne får adgang til alle personoplysninger, vil dette ikke være i overensstemmelse med dataminimeringen, da bankerne ikke foretager en aktiv vurdering, om personoplysninger bankerne modtager og behandler er relevante og nødvendige. Det vil sige, at bankernes behandling af personoplysninger er mere vidtgående, end hvad GDPR og dataminimeringen tillader.

Hvis denne løsning skal være mulig i forhold til overholdelse af princippet om dataminimeringen, skal bankerne under screeningen bede om bestemte personoplysninger, hvor det herfra skal være muligt for bankerne at adskille kundetyperne fra hinanden. Denne screeningsmetode vil ikke kunne løse informationsasymmetrien, grunden til dette er, at disse bestemte oplysninger, som bankerne skal anmode om, skal være så vidtgående at de kriminelle ikke har incitament til at afgive disse. Derudover må anmodningen ikke være så vidtgående, at bankerne overtræder principperne om dataminimering, ved kunder som ikke er kriminelle. Udfaldet af dette, vil i sidste ende være en subjektiv vurdering af kunderne individuelt, og derfor ikke føre til nogen løsning for bankerne eller for den asymmetriske information.

Hvis bankerne derimod vælger at screene kunderne, ved at pålægge kunderne bevisbyrden for deres transaktioner, vil dette kunne mindske ex post problemet og den asymmetriske information. Dette kunne forekomme ved blandt andet at bestå i dokumentation for hver pengetransaktion, som foretages af kunderne. Økonomisk kan dette anses for at være utroligt tæt på det at have komplet information, idet at bankernes dokumentationskrav for transaktioner, kan anses for at overvåge pengenes oprindelse. Ved anvendelse af denne metode, har bankerne mulighed, for at screene pengene, som anvendes, denne screening bidrager til at kunne identificere pengenes oprindelse.

Et dokumentationskrav fra bankerne, ved indbetaling og transaktion af penge, vil dette ikke komme i karambolage med principperne om dataminimering. Formålet ved at skulle kræve dokumentation er for at sikre, at alle indbetalinger af penge foretaget af kunder, er erhvervet lovligt. Det kan argumenteres for, at et krav om dokumentation ved indbetalinger overholder princippet om tilstrækkelighed i forhold til indsamlingsformålet. Det kan derudover betragtes som en relevant indsamling, da dette bidrager til at afkræfte, at pengene er forbundet med kriminalitet. Som nævnt, er formålet at sikre, at pengene er erhvervet lovligt, derfor er det nødvendigt for bankerne at indsamle dokumentation, og det er begrænset til hvad anses for nødvendigt, eftersom bankerne kun indkræver dokumentation for den omhandlende indbetaling. Dokumentationskravet kan på baggrund af dette, anses for at være i overensstemmelse med princippet om dataminimering, jf. GDPR artikel 5, stk. 1, litra c.

Anvendes denne screeningsmetode, ved at screene kundernes indbetalinger, kan dette reducere dødvægtstabet i samfundet. Det kan dog forekomme, at der kommer flere kontanter i samfundet, hvis der ikke er mulighed for at kunne indbetale penge, som kunder ikke kan dokumentere, vil disse florere i samfundet som kontanter. Der er derfor usikkerhed om, hvor meget af dødvægtstabet, bankernes screening vil kunne medvirke til at reducere. Dog kan det ikke anses for at være en omkostningstung metode, set i forhold til omkostningerne hvidvask af penge påføre den globale BNP.

5.1.3 Uafhængig vurdering af tredjepart

Dette løsningsforslag knytter sig til den informationsasymmetri, der foreligger ved ex ante tidspunktet. Det er påkrævet, at de potentielle kunder forinden etableringen af en forretningsforbindelse hos bankerne, skal have fået foretaget en vurdering af sin risiko for hvidvask af penge, hos en uafhængig tredjepart. Motivet for at pålægge de potentielle kunder dette er, at det kan resultere i, at der ved dette påkrav, sker en adskillelse af de kriminelle og ikke-kriminelle kunder. Ved at bankerne betinger de potentielle kunder dette, i forbindelse med etablering af en ny forretningsforbindelse, vil dette separere kundetyperne, hvor de ikke-kriminelle kunder ikke ser nogen fare ved at lade sig vurdere, men hvorimod kriminelle kunder ser en trussel forbundet hermed, da dette ville kunne afsløre dennes type af kunde.

En vurdering af en uafhængig tredjepart løser som sagt kun problemet, som forekommer ex ante, derfor vil denne vurdering efter etableringen af kunderne ikke have nogen værdi, da kunder efter etablering, kan begå kriminalitet.

I denne situation er bankerne den uinformerede part, eftersom det er kunderne, der besidder informationen om, hvorvidt kunderne er kriminelle eller ikke er kriminelle. Det antages at kunderne ikke har samme interesse som bankerne, i at blive vurderet hos en uafhængig tredjepart. Vurdering fra en uafhængig tredjepart, kan foretages på to måder. Det kan foregå ved, at det bliver et påkrav fra staten,²⁴⁴ eller det kan finde sted ved, at bankerne gør det til en betingelse for, at kunderne kan etablere sig som kunde i bankerne.

Som eksempel på et lignende påkrav som staten har fastsat, kan der perspektiveres til når en borger ønsker at tage et kørekort. Her er det et påkrav fra staten, at borgeren skal kunne fremvise en sundhedserklæring udfærdiget af lægen, for at kunne erhverve et kørekort.²⁴⁵ For at perspektivere kravet om sundhedserklæring til denne løsning, kan staten kræve, at når kunder ønsker at etablere sig i bankerne er det, at kunderne kan fremvise en vurdering fra en uafhængig tredjepart. Hvis det er staten, der betinger bankerne, at der skal foreligge denne vurdering af kunderne ved etablering, vil kunderne ikke have et valg, om hvorvidt de ønsker denne vurdering foretaget eller ej. Det vil være et påkrav, der gælder ved etablering af en forretningsforbindelse i alle danske banker, og kunderne vil dermed ikke kunne undgå at skulle have foretaget denne vurdering, ved etablering i en dansk bank.

Består vurderingen i et påkrav fra staten, vil det ikke længere være bankerne, som er den part, der direkte kræver vurderingen af kunderne, men i stedet er det staten der pålægger bankerne, at kravet er opfyldt. Herved skal bankerne afgive instruks, om behandling til den uafhængige tredjepart ved udarbejdelsen af denne vurdering. Baggrunden for dette er, at staten pålægger bankerne dette krav, og bankerne kan ikke selv foretage vurderingen, men nødsaget til få udført vurderingen hos en uafhængig tredjepart. Bankerne vil ikke kunne efterleve de forpligtelser, som staten pålægger dem, hvis ikke den uafhængige tredjepart handler efter bankernes beføjelser og instrukser.²⁴⁶ Bankerne vil

²⁴⁴ Knudsen, Christian "Økonomisk metodologi bind 2 - virksomhedsteori og industriøkonomi" 2. Udg. 1997, side 166.

²⁴⁵ Kørekortbekendtgørelsen, nr 815 af 21/06/2017 § 32.

²⁴⁶ Vejledning om dataansvarlig og databehandler, af Justitsministeriet og Datatilsynet, november 2017. Side 9.

dermed anses som den dataansvarlige part og den uafhængige tredjepart vil fungere som databehandler på vegne af bankerne, jævnfør GDPR artikel 4, stk. 1, nr. 7 og 8. Det er dermed bankerne, der pålægges et ansvar for, at behandlingen foregår i overensstemmelse med principperne i dataminimeringen. Anses principperne i dataminimeringen ikke for overholdt ved vurderingen, er bankerne ansvarlig for dette - også selvom vurderingen består i et påkrav fra staten.

Er det derimod bankerne, der betinger, at kunderne skal have foretaget vurderingen ved etableringen. Foreligger der her ikke et påkrav fra staten, og hvert enkelte bank har valgfrihed, om hvorvidt de ønsker at fastsætte denne vurdering som en betingelse for etablering af en forretningsforbindelse. Med afsæt i valgfriheden for den enkelte bank om påkrav til vurderingen, må bankerne anses som værende den dataansvarlige, og den uafhængige tredjepart anses som databehandler, idet det er bankerne, der påkræver vurderingen og bestemmer formålet med denne, jf. GDPR artikel 4, stk. 1, nr. 7 og 8.

Det kan antages, at banker der ikke vælger at indføre dette som et krav, vil være de banker, hvor kriminelle kunder vil søge hen mod. Bankerne der indfører påkravet, vil således have en højere sikkerhed i, at kunder, som er etableret i den pågældende bank, ikke er kriminelle. Det antages, at de kriminelle vil fravælge risikoen for, at den uafhængige tredjepart allokerer dem som en høj risiko for hvidvask af penge ved vurderingen, og at de kriminelle kunder derfor vælger at etablere sig i en bank, som ikke pålægger et krav om vurderingen hos en uafhængig tredjepart.

Ved indsamling og behandling af kundernes personoplysninger, ved vurderingen af kundernes risiko for hvidvask af penge, er der ingen garanti for, at de indsamlede personoplysninger er indsamlet til kun at omfatte, hvad der er nødvendigt for at opfylde formålet. Det er samme vurdering der skal ske på baggrund af indsamlingen, som når det er bankerne selv, der skal foretage et kundekendskabsprocedure, og på baggrund af dette indsamler personoplysninger om kunderne. Dermed kan det ikke fastslås på forhånd for indsamlingen, om den pågældende indsamling er sket med overholdelse af dataminimeringens principper, det er en subjektiv vurdering som den uafhængige tredjepart skal foretage, med de henhørende instrukser fra den pågældende bank.

Det kan derfor anskues, at omend kravet stilles fra staten, eller om det er den enkelte bank, der tilvælger kravet, vil bankerne fungere som dataansvarlig for vurderingen, og vil derfor være den

ansvarlige for, at vurderingen sker med overholdelse af dataminimeringens principper.²⁴⁷ Endvidere kan det anses, at fastsættes vurderingen som et påkrav fra staten, vil det dermed gælde for alle de danske banker og formålet med, at det skal kunne mindske den asymmetriske information som kunderne besidder. Dette vil have en større effekt herved, kontra hvis det er et krav som bankerne selv vælger, om de vil fastsætte, da de kriminelle kunder herved blot vil søge etablering i de banker, som ikke har fastsat dette krav.

5.1.4 Overvågning

Med henvisning til 4AMLD artikel 13, stk. 1, litra d sammenholdt med hvidvaskloven § 11, stk. 1, nr. 5, er det et krav fremsat ved lov, at bankerne ved bekæmpelse af hvidvask af penge, skal foretage vedvarende overvågning af deres kunders bankaktiviteter.²⁴⁸ Det tiltag, at bankerne skal overvåge deres kunders bankaktiviteter knytter sig til den informationsasymmetri, der foreligger efter forretningsforbindelsens etablering, hvorved formålet herfor er at mindske den asymmetriske information.

Ved at bankerne overvåger deres kunder, vil dette være medvirkende til at mindske informationsasymmetrien, da bankerne ved overvågning af kundernes bankaktiviteter, vil komme tættere på at besidde samme information som kunderne. Det vil ikke kunne udligne informationsasymmetrien fuldt ud, da hvidvask af penge ikke kun foregår gennem elektroniske finanser, men også foregår med rede penge. Dette opfanges ikke via en overvågning af kundernes bankaktiviteter gennem bankernes IT-systemer. Ydermere vil bankerne med henvisning til dataminimeringens principper ikke have hjemmel, til at kunne foretage fuld overvågning af kundernes bankaktiviteter. Fuld overvågning af kunderne vil ikke kunne anses, for at være i overensstemmelse med dataminimeringens principper. Selvom overvågningen skal foretages med afsæt i dette princip, vil det som sagt mindske informationsasymmetrien mellem bankerne og kunderne, og burde det også mindske det dødvægtstab, som findes i samfundet.

²⁴⁷ Dall, Nis P. & Langemark, Jesper "Persondataforordningen - en håndbog for praktikere" 2. Udg. 2018, side 142.

²⁴⁸ Finanstilsynet, "Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven), oktober 2018, side 68.

Omfanget og den metodiske tilgang for overvågningen skal være knyttet til kundernes risikoprofil. Det vil sige, at overvågningen skal tilrettelægges med afsæt i kundernes risikoprofil.²⁴⁹ Ændrer kundernes risikoprofil sig under overvågningen til for eksempel at gå fra, at den pågældende kunde er allokeret som en almindelig risiko til at udgøre en øget risiko, skal overvågning opgraderes til at omfatte det niveau af overvågning, der påkræves ved øget risiko kunder.

Det forhold, at bankerne overvåger sine kunder, vil formentlig medføre til, at de får indsamlet og behandlet personoplysninger om kunderne, som ikke altid vil findes begrænset til, hvad der måtte antages for at kunne opfylde formålet. Der kan tales for, at det forhold, at bankerne skal tilrettelægge overvågningen ud fra kundernes risikogruppe, at dette bevirker til, at bankernes muligheder for at overholde dataminimeringens principper øges kontra, hvis overvågningen bestod i samme omfang uanfægtet kundernes risikogruppe.

Økonomisk vil det mest efficiente være en fuld overvågning med komplet information, da dette vil fjerne informationsasymmetrien og dødvægtstabet. Dette er dog ikke muligt efter GDPR, da denne kun tillader en overvågning der er tilstrækkelig, relevant og begrænset til at omhandle, hvad der er nødvendigt for at opnå formålet.

5.1.5 Indgåelse af en kontrakt

Kunderne besidder information om vedkommende selv, som bankerne ikke har kendskab til. Derudover har kunderne viden, om kunderne påtænker at hvidvaske penge igennem bankerne efter, at der er sket etablering af en forretningsforbindelse. Bankerne ønsker, at kunderne ikke drager nytte af den information, som bankerne ikke har kendskab til. Bankernes mål er herved at påvirke kunderne til at have samme incitamenter som bankerne har.²⁵⁰ Bankerne vil søge en måde, hvorved det ikke vil

²⁴⁹ Finanstilsynet, "Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven), oktober 2018, side 68.

²⁵⁰ Müller, Ralf & Turner, J. Rodney "The impact of principal-agent relationship and contract type on communication between project owner and manager" International Journal of Project Management, 2005, vol 23(5), side 399.

være efficient for kunderne at hvidvaske penge, men hvor det i stedet vil være mere efficient for kunderne at forblive ikke-kriminelle kunder.

Hvis bankerne kræver, at kunderne ved etablering af forretningsforbindelsen, skal indgå en kontrakt med bankerne, vil bankerne igennem denne kontrakt kunne forsøge at få kundernes incitamenter forenet med bankernes. Bankerne vil gennem kontrakten kunne forsøge at udforme den således, at kunderne ikke ønsker at gøre brug af den skjulte information, som vedkommende besidder. Måden hvorpå bankerne vil gøre dette er ved, at bankerne i kontrakten opstiller sanktioner for brud på kontrakten. Disse sanktioner opstilles med det formål, at det ikke skal være efficient for kunderne at bryde kontrakten. Kunderne, uanfægtet om vedkommende er kriminel eller ikke-kriminel, skal have incitament til ikke at ville bryde kontrakten. For at skabe dette incitament for kunderne, skal sanktionerne være af en sådan art, at det vil være ugunstigt for kunderne at bryde kontrakten. Sanktionerne skal være så markant tunge, at det ikke vil være efficient for kunderne at foretage hvidvask af penge gennem bankerne, når dette samtidig vil betyde, at kunderne bryder kontrakten og ifalder sanktionerne. Hvis sanktionerne er af en sådan art, at det vil udgøre en betydeligt større sum end, hvad kunder, som hvidvasker penge, måtte kunne opnå af gevinst, vil det ikke længere være efficient for kunderne at bryde kontrakten. Når først kunderne har underskrevet kontrakten, er de bundet af sin underskrift²⁵¹, og kan ikke trække denne underskrift tilbage.

Hvis privatkunder, der hvidvasker penge, bliver erklæret skyldig i dette, vil straffen for overtrædelsen består i enten en bøde eller i fængsel på op til 1 år og 6 måneder.²⁵² I grove og særlige tilfælde, kan fængselsstraffen stige til at omfatte 8 år.²⁵³ Kunder, der hvidvasker penge gennem bankerne, tager en væsentlig risiko for at blive fanget i denne handling, og blive straffet herefter. Vedkommende foretager hvidvask af penge, velvidende om den risiko, der medfølger. Kriminelle kunder, der er risikovillig nok til at foretage hvidvask penge, med kendskab til strafferammen, vil kræve en betydelig fordel for ikke at hvidvaske penge. Det kan være tvivlsomt om en sanktion vil have betydning for kriminelle kunder. Der kan tales for, at allerede ved det forhold, at vedkommende agter at foretage hvidvask af penge, at vedkommende derved udviser, at vedkommende ikke bliver berørt af den straf, denne ifalder, hvis dette opdages. Med argumentation i dette, skal sanktion være passende i forhold til, at de kriminelle kunder påtænker at hvidvaske penge sammenholdt med straffen for

²⁵¹ Aftalelovens § 1.

²⁵² Straffelovens § 290 a, stk. 1.

²⁵³ Straffelovens § 290 a, stk. 2.

hvidvask af penge. Det kan derfor overvejes om de kriminelle kunder, der allerede påtænker at hvidvaske penge, ændrer adfærd på baggrund af en sanktion pålagt af bankerne.

5.3 Kampen mellem 4AMLD og GDPR

Som nævnt tidligere ses det, at hvidvask af penge består i fem procent af den globale BNP.²⁵⁴ Dette resulterer i forekomsten af et dødvægtstab i samfundet.²⁵⁵ Dette dødvægtstab er resultatet i at det hvidvask af penge indtræffer, dette betragtes for at være en negativ eksternalitet, som kan anses for at forurene den finansielle sektor.²⁵⁶ Ved benyttelse af 4AMLD for at bekæmpe hvidvask af penge, burde dette mindske omkostningerne, som er pålagt bankerne og den finansielle sektor.²⁵⁷ 4AMLD antages at indebære en positiv effekt på det finansielle system, og hermed også forekomme som en reducerende effekt på hvidvask af penge.²⁵⁸ Det bemærkes derfor, at 4AMLD burde have den indvirkning at reducere omfanget af hvidvask af penge, hvorimod hvidvask af penge optræder som en eksternalitet, som hindrer, at dødvægtstabet forsvinder. Da både 4AMLD og GDPR er EU-reguleringer, er dette en samfundsmæssig prioritering fra EU's side. Årsagen findes ved, at det ikke er muligt for bankerne at overholde begge reguleringer og samtidig fjerne dødvægtstabet fuldstændig, på baggrund af at GDPR altid vil resultere i, at der foreligger et dødvægtstab på baggrund af den asymmetriske information.

Det fremgår klart efter den juridiske og økonomiske analyse, at der i dette tilfælde findes to reguleringer, som i et hvis omfang, modarbejder efficiensen af hinanden. For at kunne løse problemet, som eksisterer mellem bekæmpelse af hvidvask af penge og beskyttelse af fysiske personer ved behandling af personoplysninger, vil det være nødvendigt at finde en retsøkonomisk løsning. Retsøkonomisk teori behandler anvendelsen af økonomiske principper i forhold til den retlige regulering.²⁵⁹ Formålet med den retsøkonomiske metode er at foretage en analyse af retsreglerne i en økonomisk kontekst, hvor formålet er at klarlægge de gældende reglers økonomiske effekt, og hvad

²⁵⁴ United Nations Office on Drugs and Crime "Money-Laundering and Globalization".

²⁵⁵ Skatteministeriet, "Skat Decembber 2002", København 2002, side 31.

²⁵⁶ Masciandaro, Donato "Money Laundering: The Economics of Regulation", 1999, side 225.

²⁵⁷ Ibid. side 233.

²⁵⁸ Ibid.

²⁵⁹ Riis, Thomas "Ophavsret og Retsøkonomi - Immaterielle Goder I Kulturøkonomisk Belysning" 1. Udg, 1. Oplag, 1996, side 28.

mulige ændringer har i et samfundsmæssigt perspektiv.²⁶⁰ Den retsøkonomiske tilgang søger at analysere den økonomiske efficiens, i forhold til juridiske regler og at forklare reglernes betydning for samfundet.²⁶¹ Analysen tager udgangspunkt i forholdet mellem 4AMLD og GDPR, for at vurdere samfundets værdi, ved at bekæmpe hvidvask af penge og inddragelse af principperne om dataminimering.

Det kan ses i afsnit 5.1 at de spilteoretiske løsninger, ikke kan findes mulige at anvende, på baggrund af principperne i dataminimeringen, resultere i at behandlingen af personoplysninger sker mere vidtgående end, hvad lovreglen tillader. Der ses en mulig anvendelse af, at bankerne kan foretage en screening af sine kunder, ved at pålægge kunderne bevisbyrden, hvilket kræver dokumentation fra kunderne angående deres indbetalinger i bankerne. Segmenterne angående kundernes signaliering, herunder afgivelse af alle personoplysninger og overvågning af bankerne, kan anvendes i et begrænset omfang. Der findes ingen restriktioner i GDPR til hinder for, at bankerne pålægger kunderne sanktioner ved hvidvask af penge. Dog finder princippet om dataminimering anvendelse ved overvågning af kunderne, idet at behandlingen af personoplysninger altid skal leve op til forordningens principper.²⁶² Det er efter 4AMLD pålagt bankerne at skulle foretage en vedvarende overvågning af kunderne, jf. 4AMLD artikel 13, stk. 1, litra d, dette skal samtidig leve op til dataminimeringen.

For at den økonomiske løsning skal være mest mulig optimal, skal det være ved anvendelse af en kombination af de nævnte segmenter. Det findes derimod klart, at nogle segmenter til løsning af den asymmetriske information, ikke kan anvendes, da dette vil findes i strid med de juridiske regler.²⁶³ Det søges at analysere, om det er muligt at anvende elementer i den økonomiske løsning, hvis det er muligt at justere på lovgivningen eller løsningen. Derudover søges det undersøgt, om bekæmpelse af hvidvask af penge er efficient for samfundet, i forhold til det tab samfundet lider ved hvidvask af penge.

²⁶⁰ Tvarnø, Christina D. og Nielsen Ruth, "Retskilder & Retsteorier", 5. udgave, 2017, side 430.

²⁶¹ Ibid.

²⁶² Datatilsynet "Hvad er dine forpligtelser".

²⁶³ Jævnfør afsnit 5.1.

5.2.1 Mulighederne for fravigelse af GDPR

Det blev i afsnit 5.1.4 belyst, at det ikke vil være muligt for bankerne at foretage en fuld overvågning af kunderne, men kun i det omfang, at det findes tilstrækkeligt, relevant og begrænset til, hvad der findes nødvendigt for formålet. Det er derudover ikke muligt for kunderne at afgive deres informationer frivilligt til bankerne, da det ikke kan være muligt for bankerne at sortere personoplysninger før modtagelsen af disse, og derfor vil det være vanskeligt for bankerne at kunne overholde principperne om dataminimering.

For at der kan foretages en brugbar overvågning af kunderne, til behandling af kundernes personoplysninger, kan bankerne som udgangspunkt kun foretage overvågning af kunderne i det omfang, at der er tale om det er tilstrækkeligt, relevant og nødvendigt jf. GDPR art. 5, stk. 1, litra c. Det skal dog bemærkes, at GDPR's anvendelsesområde angående overvågning kun omhandler medlemsstaternes borgernes adfærd inden for EU.²⁶⁴ Dette er af den betydning, at hvis overvågningen omhandler kunders²⁶⁵ adfærd uden for EU, så finder forordningen ikke anvendelse på denne adfærd.²⁶⁶ Bankerne har, på baggrund af dette, mulighed for at overvåge bestemte kunder, uden at GDPR finder anvendelse ved behandlingen. Ved at justere på overvågningen som løsningsforslag, vil det være muligt at mindske en andel af den asymmetriske information. Det vil være muligt for bankerne at foretage fuld overvågning af transaktioner, som foregår i lande uden for EU. Hvis der er tale om internationale banker, kan disse banker ved benyttelse af dette, komme tættere på at løse problemet angående den asymmetriske information, som findes mellem bankerne og kunderne.

Udover overvågning, fandtes det ikke muligt, at kunderne foretager en signalering til bankerne angående deres personoplysninger, dette på baggrund af restriktionerne i dataminimeringen. Det kan diskuteres, om det er muligt, at kunderne selv frivilligt afgiver deres rettighed til beskyttelse. Resultatet af dette er, at bankerne kan få adgang til alle deres personoplysninger både i en midlertidig periode og ved fremtidige behandlinger, til anvendelse ved bekæmpelse af hvidvask af penge. Hvis kunderne til gengæld fik en kompensation for at afgive deres rettighed, i form af en nedsættelse af eksempelvis deres renter, kan der på denne måde vil der være tale om, at bankerne og kunderne går sammen for at bekæmpe hvidvask af penge. De vil tilsammen ekskludere de kriminelle kunder, men

²⁶⁴ GDPR præambelbetragtning nr. 24.

²⁶⁵ Her er der både tale om EU-borgere og tredjelandsborgere.

²⁶⁶ Dall, Nis P. & Langemark, Jesper "Persondataforordningen - en håndbog for praktikere" 2. Udg. 2018, side 47.

da GDPR er beskyttelsespræceptiv findes dette ikke muligt. At GDPR er beskyttelsespræceptiv bevirker dette, at det ikke er muligt for kunderne at afgive sine rettigheder som forordningen tillægger kunderne, til skade for dem selv.²⁶⁷ Det vil derudover ikke være muligt for kunderne at afgive retten til dataminimering. Årsagen hertil er, at dataminimeringen forekommer som et princip i GDPR, og er bygget op omkring det EU-retlige princip om proportionalitet.²⁶⁸

Det ses med afsæt i ovenstående, at der er mulighed, for at bankerne kan løse det problem som GDPR opstiller, angående overvågning af kunderne. Det vil være muligt for bankerne at overvåge kunderne, som opererer i lande uden for EU, og herved kan en del af den asymmetriske information mindskes. Der findes ikke mulighed, for at kunderne kan foretage en signalering til bankerne, da bankerne ikke kan sortere i de indgivne personoplysninger, og det er ikke mulighed for kunderne at afgive sin ret til beskyttelse.

5.3.1 Omkostninger i forbindelse med bekæmpelse af hvidvask af penge

I dette afsnit ønskes det belyst, hvilke omkostninger tiltagene til bekæmpelse af hvidvask efter 4AMLD, pålægger samfundet, herunder bankerne. Det ønskes yderligere belyst, om disse omkostninger, sammenholdt med det påviste dødvægtstab på fem procent af den globale BNP, om disse omkostninger er hensigtsmæssige i forhold til det tab, som hvidvask af penge udgør.

5.3.1.1 Omkostninger ved at overholde dataminimeringen

Det kan ses i den juridiske analyse, at overholdelse af principperne i dataminimeringen er et krav til bankerne.²⁶⁹ Det kan være byrdefuldt for bankerne at skulle afholde omkostninger, for at overholde dataminimeringen, eftersom at bankerne efter 4AMLD blandt andet skal foretage en skærpet kundekendskabsprocedure ud fra en subjektiv vurdering. Ved udførelsen af hver kundekendskabsprocedure, både ved etablering af forretningsforbindelsen og under forretningsforbindelsens levetid, skal bankerne ved procedure foretage en vurdering af de

²⁶⁷ Bønsing, Sten "Almindelig Forvaltningsret" 4. Udg. 2018, Side 14.

²⁶⁸ GDPR præambelbetragtning nr. 4.

²⁶⁹ Datatilsynet "Hvad er dine forpligtelser".

personoplysninger som bankerne behandlinger med sikring for at kunne overholde dataminimeringen.²⁷⁰

Bankerne skal anvende mange ressourcer på at indsamle kundernes personoplysninger og foretage en vurdering, om disse er i overensstemmelse med dataminimeringens principper. Det kan også ses i et notat fra Erhvervs- og Vækstministeriet, at der kan forekomme øgede administrative omkostninger for de finansielle institutter. Den mest byrdefulde udgift vil være at skulle indføre den risikobaserede tilgang og at udvikle IT-systemer, som kan integrere denne tilgang.²⁷¹ De systemer, som udvikles i forbindelse med den risikobaserede tilgang, skal også have for øje at overholde princippet om dataminimering,²⁷² hvorefter dette tilføjer yderligere omkostninger til bankerne.

Datatilsynet har i tre afgørelser²⁷³ pointeret, at virksomheder er pålagt at skulle udvikle eller opdatere deres IT-systemer, således at disse systemer overholder princippet om dataminimering, og behandlingen ikke må findes mere vidtgående end lovgivningen tillader. Hvis det er muligt, skal der udvikles nye systemer, som kan bevirke til at minimere og præcisere behandlingen af personoplysninger. Ved udvikling af disse nye systemer betragtes omkostninger forbundet hermed at være undermineret af overholdelsen af dataminimeringen.²⁷⁴

Ved at sammenholde disse to forpligtelser, der er pålagt bankerne, involverer begge øgede omkostninger ved at skulle bekæmpe hvidvask af penge, og at sikre behandlingen af fysiske personers personoplysninger, iagttager princippet om dataminimering.

Det kan skabe tvivl, om det er efficient for bankerne at afholde begge omkostninger, som forekommer ved bekæmpe hvidvask af penge ved efterlevelse af 4AMLD, idet der forekommer øgede omkostninger ved efterlevelse af denne. Herudover resulterer princippet om dataminimering i yderligere øgede omkostninger. Hvis omkostningerne ved at bekæmpe hvidvask af penge, overstiger

²⁷⁰ Datatilsynet ”Hvad er dine forpligtelser”.

²⁷¹ Erhvervs- og vækstministeriet, ”Grund- og nærhedsnotat til folketingets Europavalg - Fjerde revision af direktiv om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge og finansiering af terrorisme”, 25. Marts 2013, side 8.

²⁷² Datatilsynet ”Hvad er dine forpligtelser”.

²⁷³ Afgørelse: Journalnummer: 2018-31-0070 ”Klage over TDC’s registrering af trafik- og lokaliseringsdata” og Afgørelse: Journalnummer: 2018-41-0016 ”Tilsyn med Taxa 4x35’s behandling af personoplysninger”. Og Afgørelse: Journalnummer: 2018-31-0147 ”Alvorlig kritik og påbud til Rejsekort A/S”.

²⁷⁴ Se afsnit 3.4.2.2.4 Afgørelser.

tabet på fem procent som hvidvask forårsager globalt, vil det ikke findes efficient for bankerne at bekæmpe hvidvask af penge. Det kan antages, at i jo højere grad bankerne bekæmper hvidvask af penge, jo flere omkostninger skal de afholde i forbindelse med dataminimering af personoplysninger. Dette er begrundet i, at ved bekæmpelse af hvidvask skal der ske indsamling af personoplysninger og i jo større omfang der indsamles personoplysninger, desto flere omkostninger skal bankerne afholde i forbindelse, med at vurdere behandlingen af disse personoplysninger. Det ses derfor, at hvis omkostninger overstiger tabet ved hvidvask af penge, så vil det ikke findes efficient for bankerne at bekæmpe hvidvask.

5.3.1.2 De bødeforlæg ved overtrædelse af GDPR og 4AMLD

Datatilsynet er pålagt at skulle sikre, at der ved overtrædelse af GDPR's regler, pålægges de pågældende virksomheder administrative bøder. Dette skal ske på effektiv vis, således at bødens størrelse findes rimelig set i forhold til overtrædelsen, men samtidig også fungerer som en afskrækning, jf. GDPR artikel 83, stk. 1. Finder Datatilsynet, at bankerne har overtrådt GDPR artikel 5, stk. 1, litra c, risikerer bankerne at blive pålagt administrative bøder på op til 20.000.000 EUR eller på et beløb svarende til maksimum fire procent af deres samlede globale omsætning fra det foregående år, såfremt dette måtte udgøre et større beløb end 20.000.000 EUR, jf. GDPR, artikel 83, stk. 5, litra a. Ved udmålingen af de administrative bøder, skal Datatilsynet ved afgørelsen tage stilling til flere krav, hvilke blandt andet indebærer, at de skal tage hensyn til overtrædelsens karakter, omfang samt konsekvensen som overtrædelsen har medført, og om den pågældende virksomhed har forsøgt at begrænse skaderne, jf. GDPR artikel 83, stk. 2, litra a-k.

4AMLD artikel 59, stk. 1, litra a-d bestemmer, at ved grov, gentagen eller systematisk overtrædelse af bestemte artikler i 4AMLD. Sker der blandt andet overtrædelse af 4AMLD artikel 18 vedrørende den skærpede kundekendskabsprocedure, er det op til det enkelte medlemsland at sikre, at den forpligtede enhed, herunder bankerne, pålægges administrative sanktioner og andre foranstaltninger. 4AMLD artikel 59, stk. 2, litra a-e opstiller minimumskrav for, hvad de administrative sanktioner og eventuelt andre foranstaltninger som minimum skal bestå af, ved overtrædelse af de i 4AMLD artikel 59, stk. 1, litra a-d oplistede artikler. Hovedreglen for hvad minimumkravene består i, er bankerne ikke omfattet af, da de er et kreditinstitut. For kreditinstitutter gælder der mere skærpede minimumskrav for bødepraksisen end for andre forpligtede enheder. Herved består bødepraksis i

administrative bøder på minimum 5.000.000 EUR, eller eventuelt en bøde på et beløb svarende til minimum 10 procent af deres samlede årsomsætning, udmålt i deres seneste godkendte regnskab, jf. GDPR artikel 59, stk. 3.

Medlemsstaterne har bemyndigelse til at give den kompetente myndighed, herunder Finanstilsynet, beføjelse til, at de må pålægge bankerne en administrativ bøde på en sum, som de finder passende, så længe den består i det minimumsbeløb som nævnt ovenfor.²⁷⁵ Af hvidvasklovens kommentar 423 fremgår det, at hverken selve hvidvaskloven eller forarbejderne til denne, har oplyst fastlagte kriterier for bødeudmålingen. Det kan udledes ud fra praksis, at bødeudmålingen er varierende afhængig af overtrædelsens karakter.²⁷⁶ Ved sager, der omhandler systematiske mangler, viser praksis til og med slutningen af 2018, at bødeudmålingen fastsættes ud fra et besparelsesprincip²⁷⁷ plus et dertilhørende tillæg på 100 procent, således at virksomheden vil ifalde en bøde på summen af det dobbelte af, hvad de sparede ved ikke at overholde hvidvaskloven og 4AMLD.²⁷⁸ En systematisk besparelse kan bestå, at den forpligtede virksomheds bekæmpelse af hvidvask, har bestået i væsentlige mangler, for eksempel ved ingen overvågning eller hvor overvågningen findes utilstrækkelig.²⁷⁹ ²⁸⁰ Praksis fra 2019 viser, at ved systematiske mangler, udmåles bødeudlæg med afsæt i virksomhedens nettoomsætning på det tidspunkt, hvor overtrædelsen blev foretaget samt virksomhedens generelle økonomiske forhold, sammenholdt med karakteren, omfanget og graden af grovhed for overtrædelsen.

Af kommentar 423 til hvidvaskloven fremgår det, at udmåling af minimumskrav til bødeudlægget skal inddeles i fem kategoriseringer med opdeling efter virksomhedens nettoomsætning, hvorved virksomhedens størrelse skal fastsætte minimumskravet for bødens størrelse. Er det muligt at beregne og vil summen af bøden være højere med en udmåling i transaktionsprincippet²⁸¹ end ved besparelsesprincippet, skal bødens størrelse fastsættes med udgangspunkt i dette. Formålet med den praksis, er for at skærpe bødeniveauet, særligt ved større finansielle virksomheder, der har opnået

²⁷⁵ 4AMLD, artikel 59, stk. 4.

²⁷⁶ Hvidvasklovens kommentar (423).

²⁷⁷ Det som virksomheden har sparet ved ikke at efterleve hvidvasklovens og 4AMLD's forpligtelser.

²⁷⁸ Hvidvasklovens kommentar (423).

²⁷⁹ Ibid.

²⁸⁰ Jensen, Rasmus M. & Uhlig, Christian S. "Lovforslag: Skærpede bøder for at overtræde hvidvaskloven" 17. september 2018, Plesner.

²⁸¹ Gevinsten ved overtrædelse af hvidvasklovens og 4AMLD's regler skal være bogført i det år, hvor den overtrædelsen fandt sted.

økonomisk gevinst ved overtrædelsen, for at sikre, at de ikke vil have lysten til at overtræde 4AMLD igen. I sidste ende vil det dog, uanfægtet retningslinjerne for fastsættelse af bødens sum, altid være domstolenes konkrete vurdering af sagens omstændigheder, der vil afgøre bødens størrelse.²⁸²

De to bødeforlæg, som forfalder ved overtrædelse af henholdsvis GDPR og 4AMLD, skal sammenholdes med hinanden. Det skal vurderes hvilken af lovreguleringerne, som vil betragtes som den mest efficiente for bankerne at overholde. Vurderingen skal være baseret på det bødekrav, bankerne kan risikere ved overtrædelse for hver af de respektive regelsæt. Vurderingen skal bestå i konkrete behandlinger, da der for overtrædelse kun er fastsat minimumsbegrænsninger for bødens størrelse, så bødens størrelse beror på en konkret vurdering af den enkelte sag. Bankerne skal søge at overholde begge regelsæt, men bevirker overholdelsen af GDPR deres kamp mod hvidvask i så høj en grad, at det ikke længere findes efficient, er bankerne nødsaget til at tage højde for, hvilke bødemæssige risici, der foreligger ved, at de må prioritere overholdelse af den ene lov fremfor den anden.

5.3.1.3 Konsekvensanalyse

Der foreligger efter GDPR artikel 35, stk. 1 en forpligtelse for den dataansvarlige, til at foretage en konsekvensanalyse af sine behandlingsaktiviteter med henblik på at vurdere, om behandlingen vil være til skade for den registreredes rettigheder. Bankerne med henvisning til GDPR artikel 35, stk. 10, fritages for at skulle foretage denne konsekvensanalyse, da deres behandlingshjemmel er at finde i GDPR artikel 6, stk. 1, litra c og e, at deres behandling er påkrævet ved et retsgrundlag i EU-retten eller national ret. Derudover foreligger der en konsekvensanalyse vedrørende databeskyttelsen, som er udarbejdet i forbindelse med en generel konsekvensanalyse på baggrund med vedtagelsen af retsgrundlaget.

Endvidere er bankerne ikke pålagt en pligt, til at skulle foretage denne konsekvensanalyse, men det fritager dem ikke retten til frivilligt at foretage konsekvensanalysen forud for deres behandlingsaktiviteter, jf. GDPR artikel 35, stk. 10. Findes der ved en konsekvensanalyse, at bankernes planlagte behandling vil udgøre en høj risiko for den pågældende kundes rettigheder, skal

²⁸² Hvidvasklovens kommentar (423).

bankerne forud for behandlingen anmode Datatilsynet om en høring, jf. GDPR artikel 36, stk. 1 og 2. Datatilsynet skal herved afgøre, om bankernes planlagte behandling vil være i overensstemmelse med GDPR's lovregler. Afgør Datatilsynet, at bankernes planlagte behandling må kunne anses, for ikke at overskride GDPR's lovregler, vil dette ikke være en sikring for, at behandlingen ikke, når den er endt, vil kunne risikere at udgøre en overtrædelse af GDPR's regler. Det er ingen garanti forbundet med Datatilsynets høringssvar. Enddog vil bankerne, hvis foretager denne konsekvensanalyse og her finder en høj risiko for overtrædelse af kundernes rettigheder, og på baggrund af dette anmoder Datatilsynet om en høring, have noget at rette sin behandling efter. Således vil Datatilsynets høringssvar ikke foreligge som en forsikring for, at bankernes behandling er i overensstemmelse med GDPR's regler, men den vil foreligge som et pejlemærke til, om bankerne foretager behandlingen på behørigvis.

Den negative faktor som vil foreligge ved, at bankerne foretager en konsekvensanalyse, er de omkostninger, der vil være forbundet med udførelsen af denne. Omkostningerne til udførelsen af konsekvensanalysen skal sammenholdes med risikoen og bødens størrelse, der vil foreligge ved, at bankerne ikke har udført behandlingen på behørigvis efter GDPR, og derved pålægges en bøde.

Det tiltag, at bankerne foretager en konsekvensanalyse forud for sin behandling af kundernes personoplysninger, vil medvirke til, at bankerne forsøger på betydelig vis at overholde GDPR's regler. Dette er for at sikre, at de mindsker risikoen for, at deres udførelse af den skærpede kundekendskabsprocedure ikke foretages på korrekt vis.

Foreligger det, at det vil være for omkostningsfuldt for bankerne at skulle udføre en konsekvensanalyse, som en form for forhåndsgodkendelse for bankerne. Formålet herfor er, at bankerne forsøger at sikre sig, at deres behandling af personoplysninger ved udførelse af den skærpede kundekendskabsprocedure, er i overensstemmelse med GDPR's regler. Der fremgår af Erhvervs- og vækstministeriets grund- og nærhedsnotat, at overholdelse af 4AMLD allerede på daværende tidspunkt blev vurderet til at blive omkostningsfuldt at overholde.²⁸³ Der forekommer tvivl angående omkostningerne, der er forbundet med overholdelse af hvidvask af penge, om disse omkostninger vil overstige det tab på fem procent af det globale BNP, som hvidvask af penge

²⁸³ Erhvervs- og vækstministeriet, "Grund- og nærhedsnotat til folketingets Europavalg - Fjerde revision af direktiv om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge og finansiering af terrorisme", 25. Marts 2013, side 8.

medfører. Overstiger omkostningerne til bekæmpelse af hvidvask af penge tabet på fem procent af det globale BNP, som hvidvask af penge forårsager, vil det ikke være efficient at allokere ressourcer til bekæmpe hvidvask af penge.

5.3 Delkonklusion

Formålet med det nærværende kapitel har været at analysere, om den mest mulige optimale økonomiske løsning på den asymmetriske information, kan finde anvendelse, når løsningen sammenholdes med gældende ret. Derudover blev det anskuet fra et retsøkonomisk perspektiv, hvorledes det ikke længere findes efficient at foretage bekæmpelse hvidvask af penge. Det er udledt i analysen, at den mest mulige optimale økonomiske løsning, ikke kan finde anvendelse som en kombineret løsning, men at enkelte segmenter i den økonomiske løsning vil kunne finde anvendelse, til at mindske den asymmetriske information. Der findes mulighed for, at bankerne kan kræve, at kunderne skal have foretaget en kundevurdering af en uafhængig tredjepart, til formålet at skulle mindske informationsasymmetrien ex ante. Signaling løsningen findes ikke mulig at anvende, da bankerne ved modtagelse af oplysninger fra kunderne, ikke vil have mulighed for at kunne sortere i relevansen af disse, og derved vil overtræde princippet om dataminimering. Dette ville heller ikke kunne realiseres på baggrund af at de potentielle kunder afgiver deres rettighed, da det ikke findes muligt, at kunderne giver afkald af sine rettigheder, da GDPR er beskyttelsespræceptiv. Der er ingen bestemmelser i GDPR, der forhindrer anvendelsen af sanktionering af kunderne ved kontraktindgåelse, og at kunderne pålægges bevisbyrden for deres likvide midlers oprindelse. Det forekommer, at der foreligger restriktioner for bankernes overvågning af sine kunder. Der er i 4AMLD adgang for bankerne til at foretage en vedvarende overvågning, hvilket dog ikke fritager bankerne for at overholde dataminimeringens principper. Eftersom at GDPR har EU som geografisk anvendelsesområde. Dette har af betydning, at bankerne har mulighed, for at foretage overvågning af EU-borgere og tredjelandsborgeres adfærd uden for EU, uden at være forpligtet til at overholde GDPR. Med disse begrænsninger, som findes i GDPR, vil det ikke være muligt at anvende den mest mulige optimale økonomiske løsning efficient. Der opstår tvivl, om dataminimeringen findes efficient, idet overholdelse af denne kan forekomme ekstremt byrdefuldt for bankerne.

Der kan foretages en vurdering efter hvor stort et bødeforlæg, der kan forekomme, og hvor omkostningsfuldt det er for bankerne at udvikle IT-systemer til overholdelse af princippet om

dataminimering. Hertil skal disse IT-systemer kunne minimere og præcisere bankernes behandling af personoplysninger.

Det skal derudover opvejes, om det er fordelagtigt for bankerne at udarbejde en konsekvensanalyse til godkendelse af Datatilsynet, dette uden sikkerhed for, at bankernes proces er korrekt, idet Datatilsynets svar kan sidestilles med at være vejledende. Omkostningerne forbundet med udførelsen af bekæmpelse af hvidvask af penge, skal derfor sammenholdes med det samfundsmæssige tab, som eksisterer på baggrund af hvidvask af penge. Hvis bekæmpelsen er mere omkostningsfuldt end gevinsten ved at bekæmpe hvidvask, antages det ikke at være efficient for bankerne at gennemføre foranstaltninger til at bekæmpe hvidvask af penge.

Konklusion

Formålet med afhandlingen har overordnet været at analysere, i hvilken grad beskyttelsen i dataminimeringen påvirker efficiensen af den skærpede kundekendskabsprocedure, som bankerne skal foretage i forbindelse med bekæmpelse af hvidvask af penge.

Til besvarelse af ovenstående, har afhandlingen analyseret, hvad gældende ret er, samt hvilke formål udarbejdelsen af lovteksterne forfølger. Denne analyse har vist, at 4AMLD har til formål at skærpe reglerne, som anvendes i forbindelse med at forhindre og bekæmpe hvidvask af penge. Dette er for at undgå skade på den finansielle sektor, hvor dette udgør en trussel af det indre marked og den internationale udvikling. Bekæmpelsen skal ske på baggrund af, at komplicerede forhold forenkles og regler søges at være fleksible. Formålet med anvendelsen af GDPR er at sikre fysiske personers beskyttelse ved behandling af deres personoplysninger, hvor dette sker på baggrund af en ensartet beskyttelsesramme i alle EU-lande. Formålene med reguleringerne bliver realiseret ved at benytte blandt andet den skærpede kundekendskabsprocedure og dataminimering.

Den skærpede kundekendskabsprocedure er opbygget efter den risikobaserede tilgang, som skal sikre bankerne en skønskompetence. Det er analyseret, at formålet med at have fokus på den risikobaserede tilgang, er at sikre fleksibilitet i lovgivningen, samt at sikre at kriminelle ikke kan omgå reglerne. Analysen viser, at principperne for dataminimeringen er baserede på, at bankerne skal foretage en subjektiv vurdering af tilstrækkelighed, relevans og om behandlingen af personoplysninger er begrænset til, hvad der findes nødvendigt for formålet. Det viste sig, at der ikke findes en direkte kollision af de behandlede lovregler i 4AMLD og GDPR, men at dataminimeringen begrænser udførelsen af den skærpede kundekendskabsprocedure. Dette er konstateret på baggrund af, at bankerne skal sikre, at der indsamles personoplysninger, samt at proceduren for dette ikke er kendt for omverdenen; herunder de der påtænker at hvidvaske penge. Dataminimeringen og Datatilsynet kræver, at behandlingen minimeres, og at principperne i dataminimeringen overholdes uanset omkostninger forbundet herved. Derudover forpligter GDPR bankerne til at føre en artikel 30-fortegnelse angående deres behandling af personoplysninger.

Afhandlingen har identificeret, at der foreligger en asymmetrisk information mellem bankerne og kunderne i forbindelse med bekæmpelsen af hvidvask af penge. Den asymmetriske information

bevirker, at bankerne ikke kan adskille de ikke-kriminelle kunder fra de kriminelle kunder. Analysen har vist, at den asymmetriske information forekommer både ex ante og ex post, idet bankerne er påkrævet at udføre den skærpede kundekendskabsprocedure både ved etableringen af forretningsforbindelsen samt under forretningsforbindelsens levetid. Den efterfølgende analyse af den asymmetriske information viste, at denne informationsasymmetri kan løses ved en kombineret anvendelse af segmenterne Signalerings og Screening spil og P/A teorien. Analysen viser, at ved anvendelse af signalering fra kunderne; ved afgivelse af alle personoplysninger og en vurdering af en uafhængig tredjepart kan forhindre den asymmetriske information ex ante. Analysen viste endvidere, at bankerne ved at anmode kunderne om afgivelse af alle deres personoplysninger, kan screene dem og derved forhindre den asymmetriske information ex ante. Ved at kunderne skal pålægges sanktioner og bevisbyrden for likvide midlers oprindelse samt det forhold, at bankerne foretager overvågning af deres kunder, kan ex post hindre den asymmetriske information i at opstå. Det kan derfor konkluderes, at en kombination af alle segmenterne er den mest mulige optimale løsning på den asymmetriske information; herunder løsningen på dødvægtstab i samfundet.

Derefter blev det identificeret i afhandlingen, om denne mest mulige optimale løsning var mulig at realisere i forhold til gældende ret. Der kunne ikke findes restriktioner i GDPR, til hinder for, at bankerne pålægger kunderne bevisbyrden og sanktioner for hvidvask af penge. Der forelå dog restriktioner mod, at kunderne kunne have mulighed, for at afgive alle deres personoplysninger og rettigheder til bankerne for at signalere, hvilken type kunderne er. Årsagen til denne restriktion er begrundet i, at GDPR er en beskyttelsespræceptiv lov, og derfor vil det ikke være muligt, at kunderne afgiver sine rettigheder til beskyttelse, idet bankerne med stadighed vil skulle overholde dataminimeringsprincipper. Det andet segment som ikke kan anvendes uden begrænsninger, er overvågning. Overvågning kan anvendes i det omfang, at det efterlever princippet om dataminimering. Det er dog muligt at overvåge kundernes adfærd, hvis det foregår uden for EU, eftersom at GDPR's geografiske anvendelsesområde er borgeres adfærd inden for EU. Disse begrænsninger har den betydning, at den tidligere nævnte mest mulige optimale løsning ikke kan anvendes fuldkommen, og at dødvægtstab ikke kan elimineres. Det ses dog, at de fleste segmenter kan anvendes. Der skal ligeledes foretages en vurdering på baggrund af de omkostninger, som forekommer ved efterlevelse af reguleringen. Hvis disse omkostninger overstiger tabet som samfundet lider som konsekvens af hvidvask af penge, vil det ikke anses efficient for bankerne at bekæmpe hvidvask af penge.

Det kan afslutningsvis konkluderes, at principperne for dataminimering har den påvirkning, at de begrænser både udførelsen af den skærpede kundekendskabsprocedure samt efficiensen af denne. Denne begrænsning sker på baggrund af de restriktioner, som dataminimeringen sætter for den nævnte mulige optimale løsning på den asymmetriske information, samt de omkostninger der er forbundet med efterlevelse af dataminimeringen.

Perspektivering

Denne afhandling har beskrevet og analyseret i hvilken grad beskyttelsen i dataminimeringen, påvirker effciensen af den skærpede kundekendskabsprocedure som bankerne skal foretage ved bekæmpelse af hvidvask af penge, for derved at være kommet frem til resultatet som beskrevet i konklusionen. De tiltag som bankerne pålægges at skulle udføre i kampen mod bekæmpelse af hvidvask af penge, er ligeledes tiltag, som er pålagt bankerne efter 4AMLD at skulle foretage med formålet om at bekæmpe finansiering af terror.²⁸⁴

I relation til afhandlingens tilblivelse, har spørgsmålet rejst sig hos os, om afhandlingens analyser og konklusion havde været af samme resultat, såfremt afhandlingens udgangspunkt havde været finansiering af terrorisme, i stedet for hvidvask af penge.

Finansiering af terror er efter 4AMLD artikel 1, stk. 5 defineret ved “...*levering eller indsamling af midler på en hvilken som helst måde, både direkte og indirekte, med den hensigt at anvende dem eller med viden om, at de vil blive anvendt, helt eller delvis, til at gennemføre en af de strafbare handlinger, der er omhandlet i artikel 1-4 i Rådets rammeafgørelse 2002/475/RIA (1).*”

Det ønskes i dette afsnit at perspektivere afhandlingens konklusion til, om dataminimeringen i GDPR ville have påvirket udførelsen af den skærpede kundekendskabsprocedure i samme grad, hvis udgangspunktet for den skærpede kundekendskabsprocedure havde været at bekæmpe finansiering af terror. Der stilles ydermere spørgsmål til, om den vurdering, som bankerne med overvejelse kunne foretage sig i forhold til afvejningen, om det ville være mest efficient for bankerne at lægge sit fokus i overholdelse af GDPR eller 4AMLD, om dette resultat havde været det samme, hvis hensynet bag 4AMLD havde været bekæmpelse af finansiering af terror og endvidere, om bankerne ville allokere mindre eller flere ressourcer ud til bekæmpelse af finansiering af terrorisme end hvad de gør til bekæmpelse af hvidvask af penge.

Det kan skabe tvivl om de subjektive vurderinger, som blive foretaget både ved udførelsen af skærpede kundekendskabsprocedure, og ved vurdering af overholdelse af princippet om dataminimering, vil være mere lempelige hvis formålet var at bekæmpe finansiering af terror, frem for bekæmpelse af hvidvask af penge. Det antages, at der vil kigges mere mellem linjerne, hvis der

²⁸⁴ Jf. 4AMLD, artikel 1, stk. 1.

er tale om finansiering af terror, da dette antages at have en større personlig effekt på mennesker end hvidvask af penge. Derudover antages det, at mennesker finder terrorisme mere skadeligt end hvidvask af penge, og derfor har en større lyst til at bekæmpe dette. Vores antagelse er derfor, at der vil foreligge mere lempelig vurdering af overholdelse af de to regelsæt, hvis formålet med behandling af personoplysninger, var at bekæmpe finansiering af terrorisme.

Litteraturliste

Bøger:

- **Aumann**, Robert J. & Hart, Sergiu “Handbook of Game Theory with economic applications Volume II” 1. Udgave, 1994, Elsevier Science B.V.
- **Axelsen**, Jens “Engelsk-Dansk Ordbog”, 13 ugd. 2003, Gyldendal.
- **Baird**, Douglas G. m.fl. “Game Theory and the Law” 1. Udg. 1998, Harvard University Press.
- **Bierman**, H. Scott & Fernandez, Louis “Game Theory With Economic Applications”, 2. Udg. 1998, Pearson.
- **Blume**, Peter “Retssystemet og juridisk metode” 3. udg. 2016, Jurist- og Økonomforbundets forlag.
- **Blume**, Peter “Den nye persondataret” 1. Udg. 2016, Jurist- og Økonomforbundets forlag.
- **Blume**, Peter “Den nye persondataret forordning 2016/679 om databeskyttelse lov 502/2018 om databeskyttelse” 2. udg. 2018, Jurist- og økonomforbundets Forlag.
- **Bounds**, Gregory M. og Malyshev, Nikolai, “OECD Reviews of Regulatory Reform Risk and Regulatory Policy: Improving the Governance of Risk” 2010, Organization for Economic Cooperation and Development.
- **Bønsing**, Sten “Almindelig Forvaltningsret” 4. Udg. 1. opl. 2018, Jurist- og Økonomforbundets forlag.
- **Chapman**, Rose “Anti-Money Laundering A Practical Guide To Reducing Organizational Risk” 1. udgave, 2018, Kogan Page.
- **Cox**, Dennis “Handbook of Anti Money Laundering”, 1. udg, 2015, Wiley.
- **Dall**, Nis P. & Langemark, Jesper “Persondataforordningen - en håndbog for praktikere” 2. udgave, 2018, Ex Tuto.
- **Knudsen**, Christian “Økonomisk metodologi bind 1 - Videnskabsteori og Forklaringstyper” 2. Udg. 2017, Jurist - og Økononforbundets forlag.
- **Knudsen**, Christian “Økonomisk metodologi bind 2 - virksomhedsteori og industriøkonomi” 2. Udg. 1997, Jurist - og Økononforbundets forlag.
- **Laffont**, Jean-Jacques & Martimort, David “The Theory of Incentives - the principal-agent model” 1. Udg. 2002, Princeton University Press.

- **Møller**, Michael & Nielsen, Niels C. “Din Økonomi. En bog om tid og penge” 4. Udg. 1. opl. 2015, Akademisk Forlag.
- **Riis**, Thomas “Ophavsret og Retsøkonomi - Immaterielle Goder I Kulturøkonomisk Belysning” 1. Udg. 1. Oplag, 1996, Gadjura.
- **Tvarnø**, Christina D. og Nielsen Ruth, “Retskilder & Retsteorier”, 4. udgave, 2014, Jurist- og Økonomforbundets forlag.
- **Tvarnø**, Christina D. og Nielsen Ruth, “Retskilder & Retsteorier”, 5. udgave, 2017, Jurist- og Økonomforbundets forlag.
- **Viscusi**, W. Kip, Harrington, Jr., Joseph E. & Vernon, John M. “Economics of Regulation and Antitrust” 4. Udg, 2005, The MIT Press.

Regulering:

- **(2012/C 326/02)** Den Europæiske Unions Charter Om Grundlæggende Rettigheder
- **2016/679/EU** Europa-Parlamentets og Rådets forordning af 27. april 2016. (Databeskyttelsesforordningen)
- **2015/849/EU** Europa-Parlamentets og Rådets direktiv af 20. maj 2015 (Hvidvaskdirektivet)
- **2016/1675/EU** Kommissionens delegerede forordning, af 14. juli 2016
- **LBK nr 1156 af 20/09/2018** (Straffeloven)
- **Kørekortbekendtgørelsen**, nr. 815 af 21/06/2017

Videnskabelige artikler:

- **Anderson**, E. & R.L. Oliver “Perspectives on behavior-based versus outcome-based sales force control systems.” Journal of Marketing, 51(October), 1987, page 76-88.
- **Hoppe**, Eva I. & Schmitz, Patrick W. “Hidden action and outcome contractibility: An experimental test of moral hazard theory” Games and Economic behaviour 109 (2018), page 544-564
- **Linder**, Stefan & Foss, Nicolai, J. “Agency Theory” SMG working paper No. 7/2013, Department of Strategic Management and Globalization Copenhagen Business School

- **Masciandaro**, Donato “Money Laundering: the Economics of Regulation”, 1999, European Journal of Law and Economics, Vol. 7 No. 2, page 225-240.
- **Müller**, Ralf & Turner, J. Rodney “The impact of principal-agent relationship and contract type on communication between project owner and manager” International Journal of Project Management, 2005, vol 23(5), page 398-403.
- **Pauline T. Kim** “Beyond Principal-Agent Theories: Law and The Judicial Hierarchy” Vol. 105, No. 2, Northwestern University Law Review, page 545.
- **Simonova**, Anna “The risk-based approach to anti-money laundering: problems and solutions” 2011, Journal of Money Laundering Control, Vol. 14, 4. udg. page 346-358
- **Gourley**, Patrick “Farmer Brown v. Rancher Wyatt: Teaching the Coase Theorem” The Journal of Economic Education, Volume 49, 2. Udg. 2018

Artikler:

- **Christensen**, Thomas Bo, “Professor om mediedækning af hvidvaskesag: “Noget af det mest ensidige i danske erhvervshistorie” af FinansWatch, offentliggjort d. 03.09.2018. (besøgt d. 12.05.2019) https://finanswatch.dk/Finansnyt/Pengeinstitutter/Danske_Bank/article10843721.ece
- **United Nations Office on Drugs and Crime** “Money-Laundering and Globalization” (besøgt d. 02-05-2019) <https://www.unodc.org/unodc/en/money-laundering/globalization.html>
- **Jensen**, Rasmus M. & Uhlig, Christian S. “Lovforslag: Skærpede bøder for at overtræde hvidvaskloven” 17. september 2018, Plesner. (besøgt d. 05-05-2019) https://www.plesner.com/insights/artikler/2018/09/lovforslag-skaerpede-boeder-forat-overtraede-hvidvaskloven?sc_lang=da-DK
- **KHF Jura** “Persondataforordningen, en vejledning om de nye regler for ikke-jurister”. (besøgt d. 17.03.2019) www.persondatavejledning.dk
- **Datatilsynet** ”Hvad er dine forpligtelser” (besøgt d. 04-05-2019) <https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-dine-forpligtelser/>
- **Finanstilsynet** ”Indberetninger til SØIK” oprettet 08. juli 2009, opdateret 07. november 2018 (besøgt d. 09-05-2019)

[https://www.finanstilsynet.dk/Tilsyn/Information-om-udvalgte-](https://www.finanstilsynet.dk/Tilsyn/Information-om-udvalgte-tilsynsomraader/Hvidvask/Indberetning-om-hvidvask/Indberetninger-til-SoeIK)

[tilsynsomraader/Hvidvask/Indberetning-om-hvidvask/Indberetninger-til-SoeIK](https://www.finanstilsynet.dk/Tilsyn/Information-om-udvalgte-tilsynsomraader/Hvidvask/Indberetning-om-hvidvask/Indberetninger-til-SoeIK)

- **Kromann Reumert** “Den nye databeskyttelsesforordning start jeres compliance-tjek med disse 6 trin” (besøgt d. 10-04-2019)
<https://www.kromannreumert.com/Insights/2016/Den-nye-persondataforordning>
- **Bruun & Hjejle**, “Rapport om non-resident portefølgen i Danske Banks estitiske filial”, 19. September 2018,
- **Skovbo**, Eva A. ”Advokaten 1 – Bør advokater forstå sig på retsøkonomi?” Advokat Samfundet, 2004 (besøgt d. 02-05-2019)
<https://www.advokatsamfundet.dk/Service/Publikationer/Tidligere%20artikler/2004/Advokaten%201/Boer%20advokater%20forstaa%20sig%20paa%20retsoekonomi.aspx>

Forarbejder, vejledninger, beslutninger og meddelelser:

- **COM(2012) 11 final**, “Forslag til Europa-Parlamentets og Rådets Forordning om databeskyttelse”
- **COM(2013) 45 final** “Forslag til Europa-Parlamentets og Rådets Forordning om forebyggende foranstaltninger med anvendelse af finansielle system til hvidvaskning af penge og finansiering af terrorisme”
- **SWD(2018) 362 final**, “Commission staff working document methodology for identifying high risk third countries under directive (EU)2015/849”
- **Betænkning nr. 1565** ”Betænkning om Databeskyttelsesforordningen (2016/679) - og de retlige rammer for dansk lovgivning” del 1, bind 1.
- **LFB 2017-04-20 nr 168** ”Retshåndhævende myndigheders behandling af personoplysninger” (gennemførelse af direktiv om databeskyttelse på retshåndhævelsesområdet)
- **Finanstilsynet** “Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terror (hvidvaskloven)”, oktober 2018.
- **Finanstilsynet** ”PEP-liste” Oprettet 29. december 2017, opdateret 10. maj, 2019
<https://www.finanstilsynet.dk/Tal-og-Fakta/PEP-liste?fbclid=IwAR07Jij0p99eLklIE7UwMEJ4ff-yes2FT0MFqJnFwXF1yAnVZOn5CzP7TVY>
- **The FATF Recommendations**: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, 2012

- **Datatilsynet og Justitsministeriet**, “Konsekvensanalyse”, marts 2018
- **Erhvervsstyrelsen, Justitsministeriet, Digitaliseringsstyrelsen og Datatilsynet**, “Databeskyttelsesforordningen, en introduktion til de kommende, nye regler om beskyttelse af personoplysninger” Oktober 2017.
- **Erhvervs- og vækstministeriet** “Grund- og nærhedsnotat til folketingets Europavalg - Fjerde revision af direktiv om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge og finansiering af terrorisme”, 25. Marts 2013
- **Statsadvokaten** “Hvidvask i Danmark, Den nationale risikovurdering 2015”.
- **Statsadvokaten** “Hvidvask i Danmark, Den nationale risikovurdering 2018”
- **Skatteministeriet**, “Skat December 2002”, København 2002,
- **Jouroá, Vêra** “Anti-Money Laundering: EU list of high-risk third countries” 2019, European Commission, fact sheet.
- **The Wolfsberg Group** “The Wolfsberg Group, ICC and BAFT Trade Finance Principles” 2017.
- **Betalingsrådet** “Rapport om Kontanternes Rolle i Samfundet” Juni 2016, Nationalbanken.

Afgørelser:

- Afgørelse **2018-41-0016** “Tilsyn med Taxa 4x35's behandling af personoplysninger”, Publiceret 18-03-2019.
- Afgørelse **2018-31-0147** “Alvorlig kritik og påbud til Rejsekort A/S” Publiceret 16-04-2019.
- Afgørelse **2018-31-0070** ”Klage over TDC's registrering af trafik- og lokaliseringsdata”Publiceret 11-02-2019.
- Afgørelse **2007-42-0049** “Vedrørende monitorering logning af 1-1 kommunikation på www.arto.com” Publiceret 20-01-2010.

Billeder:

- **Figur 1**
 - www.freepik.com/free-photos-vectors/bank

- www.appmachine.com/blog/general-data-protection-regulation/?fbclid=IwAR3q8stiZgd4JsJ8jp2OGJZpGaMMKi4_Dl6iLqUU-G4-eSh0d8Ra-IVDPQ
- www.internationalbanker.com/finance/the-top-anti-money-laundering-and-sanctions-compliance-challenges-for-financial-institutions-in-2018-and-beyond/?fbclid=IwAR2HI4fOr7ytDf-57m6LQSp11AqtXSHdQHobaGlbb0JVZW03UKgcumVjHr0
- www.istockphoto.com/gb/illustrations/surveillance-camera-pillar?mediatype=illustration&phrase=surveillance%20camera%20pillar&sort=mostpopular
- www.firmaparkering.dk/losning-bank/
- **Figur 2**
 - www.freepik.com/free-photos-vectors/bank
 - www.firmaparkering.dk/losning-bank/
 - https://www.freepik.com/free-vector/skyscraper-offices-set_1531733.htm