

En gennemgang af
centrale juridiske og
økonomiske
problemstillinger i et
virksomhedsperspektiv

GDPR COMPLIANCE

Martin Stål Axelgård Nielsen

Vejledere: Kim Østergård & Henrik Lando



Kandidatafhandling
Cand. merc. jur.

Indhold

Abstract	4
1.1 Indledning	5
1.2 Problemformulering	7
1.2.1 Juridisk problemformulering	7
1.2.2 Økonomisk problemformulering	7
1.2.3 Integreret problemformulering	7
1.2 Metodeafsnit og opbygning	8
1.3.1 Juridisk metode	8
1.3.2 Økonomisk metode	8
1.3.3 Integreret metode	10
1.3.4 Opbygning af afhandlingen	10
1.3 Afgrænsning	11
1.4.1 Juridisk afgrænsning	11
1.4.2 Økonomisk afgrænsning	12
2. Apple & Sundhedsappen	13
2.1 Sundhedsappen	13
2.2 Apple test case	15
2.3 - Apples anonymitetspolitik	16
2.3.1 Uddrag af Apples anonymitetspolitik	16
2.4 Opsummering	20
3. Analyse af udvalgte regler	22
3.1 Forordningens anvendelsesområde	22
3.2 Oplysningernes juridiske karakter	24
3.2.1 Karakter af de indsamlede personoplysninger jf. Forordningens art.9	24
3.3 Forordningens regler om samtykke ved behandling af sundhedsdata	25
3.3.1 Hjemmelsgrundlag for behandlingen	26
3.3.2 Samtykkereglerne	26
3.4 Gennemsigtighedsprincippet	30
3.4.1 Gennemsigtighedsprincippet jf. art.12	30
3.5 Oplysningspligten jf. Forordningens art.13	31
3.6 Generelle behandlingsprincipper	34
4. Konsekvensanalyse og datasikkerhed	38
4.1.1 Risiko på indsamlingstidspunktet	40

4.1.2 Risiko over tid	40
4.1.3 Elementer der taler imod risiko	41
4.2 Den juridiske ramme omkring beskyttelse af oplysningerne	42
4.2.1 Privacy by design/default.....	42
4.2.2 Data Protection Officer	43
4.2.3 Sundhedsappens passende sikkerhedsniveau som følge af risikovurdering	43
4.2.4 Anden relevant lovhjemmel.....	44
4.3 Opsummering af Sundhedsappens niveau af sikkerhed	45
4.4 Juridisk konklusion	46
5. Forordningens sanktionsramme	48
5.1. Administrative bøder jf. Forordningens art.83	48
5.2 Korrigerende beføjelser art.58, stk.2	50
5.3 Frihedsberøvelse eller anden straf jf. art.84.....	51
5.4 Erstatningsansvar jf. art.82	51
6. Økonomisk non-compliance af Forordningens samtykkeregler.....	52
6.1 Apples økonomiske forhold til compliance med samtykkereglerne	53
6.1.1 Apples skadegørende handling (gain).....	53
6.1.2 Den procentvise chance for at blive opdaget(p)	55
6.1.3 Bødens størrelse(f) – direkte omkostninger.....	56
6.1.4 Anden straf – indirekte omkostninger ($t \times \lambda$)	57
6.1.5 Dårlig omtale	57
6.1.6 Udregning af Apples økonomiske forhold til non-compliance af samtykkereglerne	58
6.2 Mindre virksomheders økonomiske forhold til compliance af samtykkereglerne	59
6.2.1 Skadegørende handling(gain) foretaget af mindre virksomhed	60
6.2.2 Chancen for at blive opdaget i procent (p).....	60
6.2.3 Bødens størrelse(f).....	61
6.2.4 Dårlig omtale af mindre virksomheder	61
6.2.5 Udregning af mindre virksomheds økonomiske compliance af samtykkereglerne	61
6.3 Kritik af den praktiske anvendelse af modellen – Problem of valuation	62
6.4 Økonomisk konklusion	63
7. Den økonomisk optimale sanktionsramme.....	65
7.1 Økonomisk optimale anvendelse af sanktionsrammen for administrative bøder	67
7.2 Den administrative model	68
7.3 Den økonomisk optimale skadesdefinition	69

7.3.1 Forordningens skadesdefinition	69
7.3.2 Den delvis økonomiske skadesdefinition.....	70
7.4 Kritik af modellen	71
7.5 Målsætning med Forordningen	73
7.6 Integreret konklusion	74
8. Konklusion	77
Litteratur og henvisninger	80

Abstract

As its title indicates, this student master thesis evolves around the newly adopted legislative initiative by the name General Data Protection Regulative, also known In short as GDPR. The thesis is overall divided into three parts, a legal, an economic and finally a part that combines both legal and economic perspectives. The theme in each part focuses on the decision making of the data controller. In regard to this, it is the job of the companies that have data management as their business area, to decide how to live up to the demands of this new legislation, and it is critical to evaluate the economical part of this business side. For some business processes it may prove expensive to be in compliance, but the company has no choice and must either pay the price it costs to be in compliance, or not implement the business process in question.

In the decision making process of the risk-neutral business executive, the decision of non-compliance with GDPR, could also be part of the process. This would to some degree, be decided by the data controllers level of risk-neutrality. In the economic theory, the business is highly motivated by optimizing the profit. In that case, the decision making process could also include evaluation of how much of a risk the specific business process involves, in terms of being fined by the authorities. If non-compliance is part of the decision making process, other factors such as fine size, cost of compliance, and higher turnover following non-compliance should also be included in the economical evaluation of non-compliance. The authorities are sitting on the other site of the table, and have to evaluate their methods of controlling the environment of data treatment and exchange by setting fines. The assumption is that the higher the authorities budget is for control, the more the environment adapts to the legislation. However, in the case of GDPR, not all violations are bad for the environment and could in theory be allowed. To allow certain violations to not be sanctioned, should be compared to the motives for passing the legislation in order to figure out if this possibility is valid in practice.

1.1 Indledning

Der indsamles data i dagens samfund som aldrig før, og eksperterne på området forventer, at denne udvikling vil fortsætte. Google estimerer nu, at vi har nået et niveau, hvor den årlige dataproduktion skal måles i zettabytes (trillioner af gigabytes). I 2012 var niveauet på 2,8 zettabytes, og niveauet forventes at blive fordoblet hvert andet år, indtil vi når niveauet 40 zettabytes i år 2021. Ud af denne enorme mængde må det antages, at en meget høj del heraf udgøres af persondata. Dette er ikke noget nyt, eftersom vi længe har været klar over, at virksomhederne gerne vil vide så meget som muligt om os, for at afsætte deres produkter. En foreløbig kulmination på dette er vedtagelse af Persondataforordningen 2016/679, som træder i kraft 25. maj 2018. Forordningen skal fremadrettet regulere området for behandling og indsamling af persondata, med virkning i EU-medlemsstaterne. Den formentlig største grund til, at den nye lovgivning er nødvendig er den folkelige følelse af, at behandlingen af persondata i det digitale domæne generelt mangler gennemsigtighed. Mangel på gennemsigtighed opstår, når data indsamles og bruges til formål, som den, der afgiver sine data, på indsamlingstidspunktet ikke havde nogen idé om ville foregå til dette formål. Et godt eksempel på dette findes i biografien "The Facebook Effect" skrevet af forfatteren David Kirkpatrick i 2011. En mand logger på tjenesten, og mødes til sin store overraskelse af et billede af sin kone, i en reklame der har det formål at tiltrække enlige mænd til en dating side. Det er oplevelser som denne, der bidrager til et fald i tilliden til brug af digitale services og et ønske fra befolkningen om at regulere netop dette område.

Fokus for denne afhandlings juridiske del er behandling af sundhedsdata i lyset af Forordningen. Det der gør sundhedsdata til et interessant område er, at udviklingen indenfor analyse af store data-set og kunstig intelligens har givet store forventninger til den indsigt, vi forventer at kunne få fra at analysere denne form for data i fremtiden². Indtil nu har det helt store gennembrud ladet vente på sig, og det er ikke indenfor periferien af denne afhandling, at spå om denne udvikling. Derimod fokuseres der på den type sundhedsdata, der på nuværende tidspunkt indsamles via apps på mobilen. Denne type data er interessante set i sammenhæng med, at markedet for de services, der indsamler denne type data, har udviklet sig med stor hast de senere år, både i antallet af udbydere, og mange forskellige typer af tilgængelige services på markedet. Et andet interessant element ved behandlingen af sundhedsdata er, at de indsamlede data om en enkelt person kan være uskyldige og generelt beskrivende, hvorimod de selv samme oplysninger om en anden person potentielt kunne fortælle noget afslørende om personens

¹ Datafication, transparency and trust in the digital domain s.3

² <https://www.computerworld.dk/art/242022/indsigt-salg-af-dine-sundhedsdata-er-et-spirende-kaempemarked-her-er-fire-vigtige-pointer>

helbred. Og en offentliggørelse af de selv samme oplysninger, kunne have helt andre konsekvenser, alt afhængig af hvem oplysningerne indsamles fra, og endnu mere interessant, hvordan disse analyseres. Konsekvensen af denne udvikling er, at den dataansvarlige der ønsker at tilbyde tjenester, som indebærer en behandling af sundhedsdata, skal være opmærksom på den risiko, sundhedsdata kan medføre for den registrerede og indrette sin databehandling derefter. Et mere specifikt fokus ved afhandlingens juridiske del, lægges på Apples sundhedsdata-app. Denne app kommer præ-installeret i iPhones, og må formodes anvendt af millioner af brugere i Danmark eftersom iPhone er en af de mest populære smartphones på markedet. I denne afhandling fokuseres på spørgsmålet, om denne app overholder Forordningens regler vedrørende samtykke, som fremgår i Forordningens art.7, samt art.4, nr.11. En lovmæssig korrekt behandling af persondata, vil dog ikke være tilstrækkelig, blot fordi samtykkereglerne overholdes. Artikel 83, som vedrører håndhævelse af Forordningen ved udskrivelse af administrative bøder foreskriver, at selvom en behandling overholder en type af regler, skal behandlingen ligeledes overholde en række af andre regler, og et korrekt afgivet samtykke efter samtykkereglerne er ikke tilstrækkeligt til, at Forordningen kan anses for overholdt. Derfor indeholder den juridiske analyse i denne afhandling ligeledes en undersøgelse af, om Appen overholder principperne vedrørende gennemsigtighed, samt oplysningspligten i Forordningens art.12-13. Da undersøgelsen baseres på appens virke før Forordningens ikrafttræden, vil afhandlingens fokus være på, at analysere, hvorledes behandlingen skal optimeres, så den er i overensstemmelse med de nye krav, Forordningen stiller.

Der findes mange forskellige forudsigelser omkring, hvor stor Forordningens gennemslagskraft bliver i forhold til den hidtidige direktiv-baserede lovgivning. Der er bred enighed om, at selve lovteksten, ikke har formået at adskille sig væsentligt fra sin forgænger, direktivet fra 1995, men at den egentlige ændring skal findes i håndhævelsen. Håndhævelsen af Forordningen skal primært ske ved at udskrive administrative bøder. Dette er afhandlingens primære fokus i for den økonomiske del. Ud over at håndhævelsen af Forordningen medfører en mulighed for at udskrive bøder, medfører de nye regler desuden, at virksomhederne ikke på samme måde som tidligere kan indsamle den samme mængde af data. Dette skyldes især oplysningspligten, som tvinger virksomhederne til at tydeliggøre den registreredes rettigheder samt kravet om gennemsigtighed. Samtidig skal de virksomheder, der behandler data, bruge mange ressourcer på at sikre, at behandlingen overholder Forordningens regler. Der er derfor tale om en betydelig økonomisk byrde for virksomhederne, uden at de modtager noget i retur, andet end den politiske langsigtede forventning om, at dataindsamlingen på sigt vil stige som følge af at tilliden genskabes, og derigennem skabe økonomisk vækst. Den økonomiske del af denne afhandling omhandler det samlede økonomiske regnestykke, virksomhederne skal forholde sig til med Forordningens ikrafttræden. Her er det

interessant at undersøge de forskelle der findes for mindre virksomheder, og virksomheder på størrelse med Apple, som man må formode har kapital til at betale bøder i den størrelsesorden, som Forordningen lægger op til med 4 % af det forrige års omsætning.

I den integrerede del af afhandlingen er fokus fortsat på sanktionsrammen. Forholdet mellem lovgiver og de dataansvarlige, kan opstilles på følgende måde. Anvender lovgiver mange penge på, at kontrollere de dataansvarlige, vil det være sværere for de dem at overtræde Forordningen. En høj kontrol af de dataansvarlige vil unægtelig medføre, at mange af de dataansvarlige som overholder loven, potentielt kunne have ladet være, og tjent flere penge på at gøre dette, endda helt uden at forsage skade. I den integrerede del af denne afhandling, opstilles en økonomisk model, hvorpå lovgiver kan anvende et økonomisk perspektiv omkring anvendelsen af sanktionsrammens for de administrative bøder. Denne sammenlignes med de individuelle målsætninger, som lovgiver og de dataansvarlige har, for at analysere om det er i deres interesse, at denne model anvendes.

1.2 Problemformulering

1.2.1 Juridisk problemformulering

Hvordan sikrer Apple, at deres app om sundhed overholder Persondataforordningens regler vedrørende samtykke?

- Hvordan sikrer Apple, at deres app om sundhed overholder Persondataforordningens regler vedrørende oplysningspligt?
- Hvordan sikrer Apple, at deres app om sundhed overholder Forordningens krav vedrørende gennemsigtighed?
- Hvilket niveau af sikkerhed skal appen om sundhed have, på baggrund af en konsekvensanalyse?

1.2.2. Økonomisk problemformulering

Under hvilke forudsætninger vil det være økonomisk optimalt for Apple, ikke at overholde Forordningens regler vedrørende samtykke?

- Under hvilke forudsætninger vil det være økonomisk optimalt for mindre virksomheder, ikke at overholde Forordningens regler vedrørende samtykke?

1.2.3 Integreret problemformulering

Hvordan vil en økonomisk tilgang omkring anvendelse af Forordningens sanktionsramme for administrative bøder være forenelig med henholdsvis virksomheden og lovgivers individuelle målsætninger?

1.2 Metodeafsnit og opbygning

BEMÆRK: Afhandlingens faktum tager udgangspunkt i hvordan Apple, før Forordningens ikrafttrædelse, behandlede Personoplysninger via Sundhedsappen. Dette skyldtes, at afhandlingens afleveringsdato er udskudt.

Forordningen har private personer som rettighedssubjekt, og virksomhederne som det primære pligtsubjekt. Der holdes en primært fokus hele vejen igennem specialet på virksomheden, men da den registrerede er rettighedssubjekt, kan det ikke undgås, at momenter i specialet vil vedrøre den registreredes rettigheder. Fokus i disse situationer er stadig på virksomheden, som skal tilpasse sin behandling. I den integrerede del placeres synsvinkel både på virksomhed og lovgiver. Dette gøres ud fra forudsætningen om, at det er relevant for virksomheden at kunne forudse lovgivers modsvar på at loven eventuelt ikke overholdes. Perspektivet er derfor indirekte, stadigvæk på virksomheden.

1.3.1 Juridisk metode

Denne afhandling går ud på at udlede og systematisere gældende ret (de lege lata). Fremgangsmetoden er den velkendte fra juridisk metode, med valg af faktum, regel, og slutteligt et resultat. Faktum i opgaven består af en redegørelse for den brugeroplevelse, som brugeren gives ved anvendelse af Sundhedsappen (Apples App om sundhed omtales herfra Sundhedsappen). Sundhedsappen analyseres så vidt muligt adskilt fra Iphone og Apple øvrige funktioner, men ved anonymitetspolitikken, som er generel for alle Apples produkter, er det ikke muligt at fokusere på Sundhedsappen isoleret. Her vil kun de relevante dele for Sundhedsappen blive inddraget.

Gældende ret udledes i denne opgave ved, at analysere lovteksten fra Forordningen samt betragtningerne. Forordningens artikler og betragtninger er meget brede, og fortolkningen af Forordningen er således ikke udledt i retspraksis endnu. Derfor inddrages fortolkningsbidrag fra litteraturen som en væsentlig retskilde, hvor det findes bedre, passende eller nødvendigt. Såfremt et område i Forordningen behandles, hvor direktivets lovgivning minder om Forordningens, vil der potentielt kunne inddrages retspraksis fra direktivet. Vurderingen af dette afhænger af, om det valgte faktum kan anvendes til at inddrage den gamle retspraksis, samt om det er muligt ved søgning at finde anvendeligt materiale.

1.3.2 Økonomisk metode

Den valgte økonomiske metode, der benyttes for afhandlingens økonomiske del, er den nye institutionelle økonomiske teori. Dette medfører et bevidst fravalg af den neo klassiske teori, da formålet med analysen

er, at præsentere et så realistisk billede som muligt. Især det forhold, at aktører er bundet rationelt, samt at der ikke foreligger perfekt information, gør denne teori optimal i forhold til den neo klassiske³. Den gamle institutionelle fravælges også, da aktørerne ikke har så stort fokus på profitoptimering. I afhandlingen forudsættes det netop, at aktørerne vægter profitoptimering højt, men ikke som den eneste prioritet. I den ny institutionelle, samt også den neo klassiske er dette en vigtig antagelse i forhold til aktøren, men den ny institutionelle teori afspejler det virkelige scenarie bedre. Det valgte analyseniveau er på virksomhedsniveau.

Den valgte økonomiske model stammer fra artiklen *The Economic Theory Of Public Enforcement Of Law*⁴. Modellen tilpasses og opererer indenfor for de rammer, som den ny institutionelle økonomiske teori forudsætter. For at lette fremtidig omtale af modellen, gives den betegnelsen i opgaven, Non-compliance modellen.

1.3.2.1 Non-compliance modellen

En virksomhed har mulighed for at tjene en større sum penge. Muligheden indebærer, at virksomheden skal foretage en skadegørende handling, som samtidig er forbudt ved lov. For at udregne om en skadegørende handling, kan betale sig, skal virksomheden kende til den forventede værdi af handlingen. Den forventede værdi kan udtrykkes, på følgende måde:

Værdi ved at foretage en skadegørende handling (g) - chance for opdagelse (p) x bødens størrelse (f). Er g højere end bødens størrelse, gange med den procentvise chance for opdagelse, vil det være økonomisk optimalt, at foretage handlingen.

At kende den forventede værdi er ikke altid tilstrækkeligt, for den dataansvarlige. Dette skyldtes, at virksomheden kan risikere, at der pålægges yderligere straf, i en anden form end bøde. Derfor må dette aspekt indgå i udregningen. Dermed kommer den forventede værdi af g til at være følgende:

$$g > p(f + (t \times \lambda))$$

Igen er det tilfældet, at g skal være højere end 0, for at en skadegørende handling er økonomisk optimal. Er værdien negativ, er handlingen ikke økonomisk efficient. Er værdien præcis 0, vil den risikoneutrale aktør

³ Klaus Nielsen s.105

⁴ Polinsky & Shavell - Individual behaviour s.5

være indifferent om handlingen foretages, hvor den risikoaverse vil have en merpræmie, fordi der forelægger risiko i forbindelse med handlingen.

Betydningen af de forskellige værdier:

g = Den opnåede værdi fra den skadegørende handling

p = Den procentvise chance for at blive opdaget (mål i procent)

f = Bødens størrelse

t = Fængselsstraffens længde målt i enhed (evt. måned eller år)

λ = Den tabte nytteværdi pr. enhed af den målte enhed af fængselsstraffens længde

1.3.3 Integreret metode

I den integrerede del af afhandlingen anvendes samme overordnede økonomiske videnskabsteoretiske udgangspunkt fra den økonomiske del, med den ny institutionelle økonomiske teori. Den valgte økonomiske model, stammer fra Polinskys bog *Introduction to law and economics* fra kapitlet *law enforcement using fines*⁵. På samme måde, som i den økonomiske del, inddrages en model, som tilpasses. Modsat tilfældet i den økonomiske del, indgår den valgte model i den integrerede del, anvendes modellen som et sammenligningsgrundlag. Dette skyldtes, at en anvendelse af modellen ikke kan overføres til den måde, som Persondata, praktisk, vil kunne håndhæves af lovgiver. Modellen inddrages, for derefter at opstille et løsningsforslag baseret på en lineær funktion, med formål om de dataansvarlige skal have de samme rammer, som i modellen.

Det juridiske bidrag stammer, som i den økonomiske del, ligeledes fra del 5 omkring sanktionsrammen, men ved at udlede gældende ret, modsat den økonomiske del hvor Forordningens artikler kun inddrages for at opstille de økonomiske rammer. Der er dermed tale om at den erhvervsjuridiske metode/ integrerede metode benyttes, da gældende ret udledes i samspil med økonomisk teori. Problemejer er virksomheden, men lovgivers motiver inddrages også, da det er dennes målsætninger der påvirker virksomhedens anvendelse af modellen.

1.3.4 Opbygning af afhandlingen

Afhandlingen er skrevet med tanke om, at opfylde kravet om lige dele af jura og økonomi. Den juridiske del starter i del 2 og sluttet i del 4. Den økonomiske del starter i del 5 og slutter i del 6. Den integrerede del

⁵ Polinsky s.81

findes i del 7, og omhandler ligeledes de juridiske elementer fra del 5. Afhandlingens del 8 er den afsluttende og konkluderende del.

Del 2 vedkommer den brugeroplevelse, brugeren har ved at tilgå appen for første gang. I bilag 1(Apple test case) vedlægges en udvalgt billedserie over alle relevante handlinger, og hvilke informationer brugeren gives indtil Sundhedsappen påbegynder indsamlingen af data. Der vedlægges ligeledes en kopi af Apples anonymitetspolitik, som er den police for at bruge tjenesten, som Apple beder deres brugere tage stilling til. Formålet med dette er at dokumentere alle de handlinger brugeren skal tage stilling til, samt de informationer brugeren gives inden benyttelse af tjenesten. I denne afhandling udgør disse to bilag afhandlingens faktum, og der inddrages de relevante elementer fra dette i den juridiske analyse.

Den juridiske analyse startes i del 2 med faktum og slutes med del 4 omkring datasikkerhed. Konklusionen placeres sidst i del 4, og denne er den juridiske konklusion gældende for hele den juridiske problemformulering.

Del 5 er indledningen til både afhandlingens økonomiske del og afhandlingens integrerede del. I den økonomiske del(del 6) er formålet, at udlede de økonomiske rammer, som artiklerne i del 5 udleder. I den integrerede del(del 7), udledes gældende ret fra elementer af del 5, samt andre relevante områder i Forordningen.

1.3 Afgrænsning

Læseren af denne afhandling forudsættes, at have en almen viden om emnet. Der vil være områder hvor forskellige modeller, retsområder og begivenheder kunne være inddraget. Her bør læseren være opmærksom på, at Forordningen vedrør et meget stort anvendelsesområde, og afgrænsning foretages for at afhandlingen ikke bliver for omfattende.

1.4.1 Juridisk afgrænsning

Denne afhandling beskæftiger sig med den primære EU-ret i form af Forordningen og Præambelen.

Speciallovgivning, såsom Persondataloven, Sundhedsloven og lign inddrages som udgangspunkt ikke i analysen. Da der er tale om et juridisk-økonomisk speciale, vil der ikke blive foretaget egentlig dataanalyse, om end der redegøres for de muligheder, en analyse af de behandlede data ville kunne frembringe. Der inddrages heller ikke tekniske elementer omkring compliance arbejdet, såsom tilstrækkeligt niveau af

Firewall etc. Dette er især relevant i del 4 omkring compliance arbejdet, men gælder også afhandlingen generelt.

Selvom Apple har hovedsæde i Californien, inddrages forholdet omkring videregivelse af personoplysninger til tredjelande kun i meget begrænset omfang. Forholdet mellem den dataansvarlige og databehandleren, samt regler vedrørende børns samtykke gennemgås desuden heller ikke. Årsagen til dette er at den juridiske del bliver for omfattende.

Når en artikel fra Forordningen gennemgås, inddrages kun de dele af artiklen, der er relevante. De irrelevante dele udelades, og der foretages ikke en gennemgang med begrundelse for udeladelser. Dette ses især omkring del 4, hvor Forordningens art.5 gennemgås, men kan også blive tilfældet ved andre af Forordningens artikler hvor indholdet er åbenlyst irrelevant for afhandlingen.

1.4.2 Økonomisk afgrænsning

De tal der inddrages, både i økonomisk og integreret del, er primært fiktive på nær de anvendte bødesatser fra Forordningen, samt Apples omsætning forrige år. Den økonomiske og integrerede del af afhandlingen er inspireret af fremgangsmetoden bag de modeller der anvendes i Polinskys bog *Introduction to law and economics*. Der fokuseres på, at opstille overordnede rammer og analysere på hvordan tallene påvirker hinanden, samt de aktører det vedkommer. Derfor er tallenes nøjagtighed ikke vigtige. Det vigtige er, at såfremt en værdi har et bestemt niveau, er aktøren nødt til, at forholde sig til dette.

De økonomiske modeller der inddrages er kun dem der beskrives i det økonomiske metodeafsnit. Informationsøkonomiske modeller inddrages ikke, samt heller ikke økonomiske modeller fra kontraktretten ud over dem der nævnes i metodeafsnittet. Der fokuseres på, at opstille nogle modeller, som er baseret på nogle antagelser. Der redegøres for disse antagelser, og ud fra dette foretages analyse af beslutningsgrundlaget, som aktøren (virksomheden) kan agere ud fra.

2. Apple & Sundhedsappen

Sundhedsappen er en service, som Apple leverer via iPhone. Siden Apple lancerede deres første iPhone i 2007, er deres markedsandel kun vokset. Siden 2016 er deres antal af aktive enheder i brug vokset med 30% om året. Det anslås, at Apple i øjeblikket har 1,3 milliarder aktive enheder i brug på verdensplan. Dette tal omfatter både Macbooks, iPhones, Apple Watches, iPads, iPods etc. I en pressemeddelelse fra Apple 1. februar 2018, udtalte Apple, at de i det foregående kvartal havde solgt over 77 millioner iPhones, og at de havde en indtægt på 88,3 milliarder dollars i samme kvartal⁶. iPhones udgør for 19,3 % af salget af smartphones på verdensplan. Apple er således den største producent af smartphones i verden.

iPhone er en smartphone med mange indbyggede teknologier. Ud over de obligatoriske SMS og opkald, indeholder den også kamera, musikafspiller, internetforbindelse/ webbrowser (Safari), regnemaskine, GPS etc. En iPhone dækker derfor sædeles mange behov hos brugeren. En stor del af Apples succes med iPhone, er ud over dens design, de apps der kan installeres på telefonen. App's er en applikation, en tilføjelse af et softwareprogram, som man kan installere i telefonen. Deres formål er mange og forskellige, lige fra at hjælpe brugeren med at udføre en specifik opgave, eller underholdning i form af spil. I skrivende stund er der over 2 millioner apps på App Store, og i 2017 blev der downloadet over 178 milliarder apps på verdensplan. Man må derfor erkende, at apps er et fænomen, der er kommet for at blive, og noget som de fleste mennesker benytter sig af.

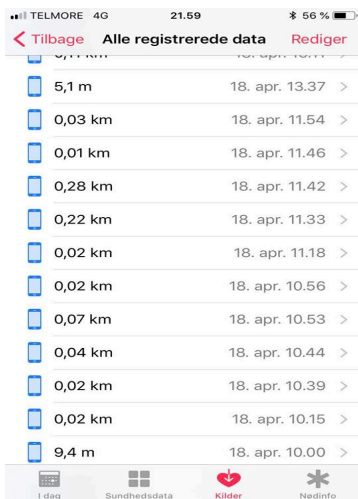
Denne del af afhandlingen omhandler de scenarier, som brugeren skal igennem, før der gives adgang til Sundhedsappen. Det er således brugerens oplevelse, og de ting han skal tage stilling til, der lægges til grund for, om Sundhedsappen overholder de udvalgte artikler i Forordningen, som gennemgås i afhandlingens del 3-4.

2.1 Sundhedsappen

Når brugeren erhverver sig en ny iPhone er der nogle præ-installerede apps på telefonen. Apps som Apple har besluttet, at man skal have på telefonen, heriblandt Sundhedsappen. Disse Apps kan ikke slettes. De vil ligge i baggrunden af telefonen og opsamle data, uanset om brugeren har interesse i det. Apple lader dog brugeren vælge, om han vil dele sine data med Apple, eller om de skal forblive i telefonen, og brugeren skal træffe et aktivt valg i forbindelse med dette.

⁶ <https://www.apple.com/newsroom/2018/02/apple-reports-first-quarter-results/>

I 2014 blev iOS 8 lanceret, og den indeholdt Sundhedsappen. Formålet med App'en er at holde styr på alle brugerens sundhedsoplysninger. Sundhedsappen fungerer på tværs af enheder, og fungerer derfor sammen med Apple iWatch, som f.eks. kan monitorere brugerens puls. Brugeren har desuden mulighed for at indtaste data og personoplysninger, samt trække data fra andre apps ind i Sundhedsappen. Endda brugerens lægejournaler kan overføres til Sundhedsappen. Telefonen registrerer via Sundhedsappen, hvor megen tid der bruges på at sove, hvor mange skridt der er gået, og mange andre oplysninger, alt afhængig af om brugeren tillader det. Omkring den daglige aktivitet foretager Sundhedsappen også en opstilling af, hvor mange skridt der er gået på specifikke tidspunkter i løbet af dagen, så brugeren uddybende kan se, på hvilke tidspunkter af døgnet han er mest aktiv. I dag, 18. april kan det aflæses at forfatteren til denne afhandling har tilbagelagt ca. 0,5 km mellem kl.10-13.



Alle registrerede data	
5,1 m	18. apr. 13.37
0,03 km	18. apr. 11.54
0,01 km	18. apr. 11.46
0,28 km	18. apr. 11.42
0,22 km	18. apr. 11.33
0,02 km	18. apr. 11.18
0,02 km	18. apr. 10.56
0,07 km	18. apr. 10.53
0,04 km	18. apr. 10.44
0,02 km	18. apr. 10.39
0,02 km	18. apr. 10.15
9,4 m	18. apr. 10.00

Indsamlingen foregår ved hjælp af en række sensorer. De data, som Sundhedsappen indsamler/kreerer, inddeles i fire overordnede kategorier: aktivitet, søvn, mindfulness og ernæring.

Apple indsamler og anvender en masse forskellige data, hvilket også fremgår af deres anonymitetspolitik (Uddybes i afsnit 2.3). Grundlæggende er Apples mål med iPhone og Sundhedsappen, at have så mange brugere som muligt. Des flere brugere, jo mere data vil dette generere til Apple. En del af formålet med Sundhedsappen er, at Apple har indset, at sundhedsbranchen har svært ved at skaffe data fra velvillige patienter/test-subjekter. Sundhedsappen er derfor ikke kun lavet for at optimere iPhone som produkt, men også for at Apple kan sælge data til forskning via deres Research Kit, som er et program, forskere kan bruge til at få indsigt ud af de indtastede data i Sundhedsappen⁷.

⁷ <http://lydogbillede.dk/nyheter/apple-health/apple-tager-fat-om-hele-sundheden/>

2.2 Apple test case

For at vurdere om persondataforordningen overholdes, opstilles her en undersøgelse med udgangspunkt i installering af ny iPhone. Der ønskes at inddrage de relevante handlinger brugeren skal igennem, samt hvad brugeren giver tilladelse til.

Ved opstart af telefonen, bliver brugeren bedt om at læse fire forskellige politikker:

- A. Vilkår og betingelser for iOS
- B. Vilkår og betingelser for iCloud
- C. Vilkår og betingelser for Game Center
- D. Anonymitetspolitik

Kun Apple's anonymitetspolitik er relevant for denne afhandling, da de andre vedrører andre tjenester i iPhone.

Brugeren får et link, hvor han kan gå ind og læse anonymitetspolitikken for derefter at gå tilbage til opsætning og godkendelse. Det anbefales her at læse politikken igennem og man får også her mulighed for, at få politikken sendt til sin e-mail. Vælger brugeren her ikke "accepter", kan telefonen ikke benyttes. Det er derfor en nødvendig handling fra brugeren at godkende indholdet af denne politik⁸.

Herefter skal man tage stilling til, hvorvidt man vil dele de oplysninger, der bliver indsamlet i telefonen, med Apple⁹. Man kan vælge mellem "Del med Apple", eller "Del ikke". Det er her ikke nødvendigt at dele oplysninger med Apple.

Dernæst gives brugeren adgang til telefonens hjemmeskærm. Her fra kan der klikkes adgang til Sundhedsappen, hvorefter brugeren får muligheden for at indtaste sine oplysninger:

- Fornavn
- Efternavn
- Fødselsdagsdato
- Køn
- Højde

⁸ Bilag 1 – Apple Test Case nr. 10 - 12

⁹ Bilag 1 – Apple Test case nr.15

- Vægt

Derefter indsamles løbende og automatisk oplysninger baseret på den registreredes aktivitet:

Søvn i antal timer/min

Fysisk aktivitet i antal skridt og distance opgivet i km¹⁰

Slutteligt mødes brugeren af nedenstående besked, hvor Apple igen beder brugeren om at dele sine oplysninger:

Forbedre Sundhed og aktivitet

"Vil du hjælpe Apple med at forbedre sundheds og fitness funktionerne ved at dele dine aktivitets og træningsdata samt begrænsede sundhedsrelaterede data? Du kan altid stoppe deling i indstillinger.

Valgmuligheder: "Tillad", "Læs mere", "Tillad ikke"

Brugeren informeres her om, at Apple ønsker adgang til de lagrede informationer. Formålet angives som værende for at forbedre sundheds og fitness funktionerne.

2.3 - Apples anonymitetspolitik

Apple gør brug af en generel anonymitetspolitik for alle deres produkter, hvorfor ingen specifik anonymitetspolitik gælder for Sundhedsappen. Sundhedsappen nævnes ikke ved navn ikke i denne politik, men derimod henvises der til tjenester og services i en samlebetegnelse. Apple's anonymitetspolitik fylder 22.690 tegn (ca.10 sider efter CBS-standard), og en komplet analyse af anonymitetspolitikken kunne muligvis udgøre en afhandling i sig selv. Brugeren gives mulighed for at få tilsendt Apple's anonymitetspolitik pr. mail. Denne politik sendes ikke til brugeren i PDF-format, men derimod kopieret direkte ind i mailen. Nedenfor gengives de vigtigste elementer.

2.3.1 Uddrag af Apples anonymitetspolitik

I dette afsnit undersøges, hvilke oplysninger Apple indsamler med Sundhedsappen, og hvad disse benyttes til. De valgte uddrag sker med henblik på at benytte dem i den analytiske del af afhandlingen (del 3).

¹⁰ Bilag 1 - Apple test case nr. 20, 22

Anonymitetspolitikken er delt op i 17 afsnit med titler på hver kategori. Der gives ikke nogen nummereret opdeling i hvert afsnit, men derimod benyttes overskrifter. Disse er følgende:

1. Indsamling og brug af personlige oplysninger
2. Hvilke personlige oplysninger indsamler vi?
3. Brug af personlige oplysninger
4. Indsamling og brug af ikke-personlige oplysninger
5. Cookies og andre former for teknologi
6. Videregivelse af oplysninger til tredjepart
7. Serviceudbydere
8. Andre
9. Beskyttelse af personlige oplysninger
10. Dine personlige oplysningers integritet og opbevaring
11. Adgang til personlige oplysninger
12. Børn og uddannelse
13. Lokalt baserede tjenester
14. Websites og tjenester for tredjeparter
15. Internationale brugere
16. Apples politik til beskyttelse af din anonymitet
17. Spørgsmål om anonymitet

Indledningsvis skal det nævnes, at kategori 1-3 omkring personlige oplysninger er sammenflydende. Dette gælder både titel, (som minder om hinanden) og indhold.

Afsnit 1 – Indsamling og brug af personlige oplysninger:

"Du bliver muligvis bedt om at angive dine personlige oplysninger, når du kommunikerer med Apple eller en virksomhed, der er tilknyttet Apple. Apple og Apple's tilknyttede virksomheder udveksler muligvis disse personlige oplysninger indbyrdes og bruger dem i overensstemmelse med nærværende Anonymitetspolitik"

I forhold til denne del af anonymitetspolitikken bør det nævnes, at Apple har over 90 datterselskaber, bl.a. Siri, Beats by Dre, Shazam, NeXT samt en lang række andre virksomheder af varierende størrelse. Apple skriver hermed, at de personlige oplysninger deles med over 90 virksomheder.

Afsnit 1 - Fortsat:

Brugeren informeres yderligere om, at han fravælge at afgive oplysninger til Apple:

"Det er ikke påkrævet, at du udleverer de personlige oplysninger, som vi har bedt om, men hvis du ikke gør det, kan vi i mange tilfælde ikke hjælpe dig med vores produkter eller tjenester eller besvare dine eventuelle spørgsmål"

Brugeren kan altså undlade at afgive sine personlige oplysninger, men det vil ifølge Apple ikke være i brugerens egen interesse, at benytte sig af denne mulighed.

Afsnit 2 – Hvilke personlige oplysninger indsamler vi:

"Når du opretter et Apple-id, ansøger om købskredit, køber et produkt, downloader en softwareopdatering, melder dig til en lektion i en Apple Store-butik, kontakter os eller deltager i en onlinerundspørge, indsamler vi en række oplysninger, inkl. navn, adresse, telefonnummer, e-mailadresse, foretrukken kontaktmetode og kreditkortoplysninger"

Her bør det bemærkes at Apple bruger formuleringen **inkl.** omkring de indsamlede oplysninger. Man kunne argumentere for at det med denne formulering, ikke er nemt at vide om Apple indsamler yderligere oplysninger.

Afsnit 3 – Brug af personlige oplysninger:

Apple skriver i afsnit 3 en række formål med indsamlingen af personlige oplysninger. En sammenfatning af alle formål Apple nævner omkring indsamling af de personlige oplysninger kan gives her:

- *"holde dig informeret om Apples sidste nye produkter, softwareopdateringer og kommende begivenheder"*
- *"skabe, udvikle, styre, levere og forbedre vores produkter, tjenester, indhold og **reklamering** samt til forebyggelse mod tab og til bekæmpelse af svindel"*
- *"bekræfte din identitet, til at hjælpe dig med at identificere brugere og til **at finde frem til passende tjenester**"*
- *"interne formål, eksempelvis revision, **dataanalyse og research, for at forbedre Apple's produkter, tjenester og kundekommunikation**"*

Der er dermed tale om en masse forskellige formål, som formuleres meget bredt. Ud fra dette er det svært at vide, i hvor stort omfang brugerens data vil blive benyttet til de forskellige formål, og om de overhovedet vil blive brugt.

Afsnit 4 – Indsamling og brug af ikke-personlige oplysninger:

Dette afsnit er omkring brugen af ikke-personlige oplysninger. Disse defineres af Apple som følger:

"oplysninger på en måde, der i sig selv ikke kan forbindes med en enkelt person"

Ved at læse videre omkring eksempler med brug af denne type oplysninger kan de ikke- personlige oplysninger aflæses til at være:

"beskæftigelse, sprog, postnummer, områdenummer, henvisende URL, lokalitet og tidszone, enhedens unikke identifikationsnummer"

Selvom størstedelen af disse oplysninger ikke kan benyttes individuelt, til at identificere en person, bør der alligevel stilles spørgsmålstejn ved om det altid er tilfældet. En persons beskæftigelse kunne være en oplysning hvor der vil være mulighed for at opnå identifikation, såfremt vedkommendes stilling er sjælden. Der nævnes desuden heller ikke om disse oplysninger kombineres. Benyttes disse oplysninger med hinanden, vil chancen for identifikation blive forhøjet.

Formål med de ikke-personlige oplysninger angives at være:

*"Disse oplysninger bruges muligvis til at forbedre relevansen af resultaterne fra vores tjenester. **Men sådanne oplysninger vil ikke blive knyttet til din IP-adresse. Bortset fra i begrænsede tilfælde for at sikre kvaliteten af vores tjenester på internettet**"*

Dette afsnit gør det ikke let for brugeren at vide, hvornår oplysninger knyttes til IP-adressen, da det ikke nævnes hvilke situationer der udgør de begrænsede tilfælde.

*"Vi indsamler muligvis oplysninger om kundeaktivitet på vores websted, iCloud-tjenester, iTunes Store, App Store, Mac App Store, App Store til Apple TV, iBooks Store og i vores andre produkter og tjenester. Disse oplysninger samles og bruges som en hjælp i **vores bestræbelser på at give kunderne mere nyttige oplysninger og få indsigt i, hvilke dele af vores websted, produkter og tjenester de primært er interesserede i**"*

Apple har med dette, igen, valgt at benytte en meget bred formulering omkring deres formål med behandlingen af de ikke-personlige oplysninger. Sundhedsappen må her være omfattet af formuleringen *"andre tjenester"*. Her benyttes desuden formuleringen *muligvis* omkring behandlingen, som gør at brugeren ikke ved i hvor høj grad dette vil forekomme, og om det overhovedet vil forekomme.

Afsnit 6 – videregivelse af oplysninger til tredjepart:

"Apple videregiver kun personlige oplysninger med henblik på levering og forbedring af vores produkter, tjenester og annoncering, og oplysningerne videregives ikke til tredjepart med henblik på disses markedsføring"

Det må ses som positivt at Apple ikke lader andre virksomheder benytte de personlige oplysninger til markedsføring. I dette nævnes dog intet om de ikke-personlige oplysninger.

2.4 Opsummering

Apple oplyser direkte til brugeren inden brug af Sundhedsappen, at han kan vælge at dele sine data med Apple. Det formål som her angives direkte til brugeren, om at hans data kan benyttes til at optimerer fitness-funktionerne, er meget kortfattet i forhold til alle de formål, som Apple nævner i deres anonymitetspolitik. Her nævnes både, at Apple udveksler oplysninger med interne datterselskaber/partnere, og at oplysningerne benyttes til annoncering. Apple har ikke en selvstændig anonymitetspolitik til Sundhedsappen, men en generel politik for alle deres tjenester. Apple har mange tjenester tilknyttet iPhone. Derfor skal brugeren kigge under samlebetegnelsen tjenester og services. Dette besværliggør processen for brugeren, når han skal finde ud af, hvad Apple gør med hans data. Denne politik er ikke let at forstå, og brugeren skal bruge tid på at sætte sig ind i, med hvilket formål hans data bliver indsamlet og behandlet. De to budskaber, den direkte anmodning om samtykke, samt de mange forskellige budskaber i anonymitetspolitikken, stemmer ikke overens. Der nævnes flere sammenhænge i forbindelse med hvordan data benyttes i anonymitetspolitikken, end det formål brugeren gives direkte, når der spørges omkring deling. Dette er heller ikke overraskende, eftersom anonymitetspolitikken omhandler mange andre services end Sundhedsappen. Skulle brugeren læse denne politik, kan en ordlydsfortolkning føre til, at læseren fortolker det som, at Apple anvender de behandlede data, til andre ting end det formål brugeren oplyses om, når han skal give sit samtykke til Sundhedsappen.

Apple har udviklet Research Kit, så forskere kan lave undersøgelser med ud fra de data der opsamles af Sundhedsappen. Dette foregår ved at forskerne opretter Apps, som fungerer sammen med

Sundhedsappen, og kan få data fra Sundhedsappen. Ifølge Apple gives brugernes oplysninger dog ikke automatisk til forskerne. Forskerne skal selv have tilladelse til at benytte brugerens data, og have samtykke direkte fra brugerne, ved at de downloader de specifikke apps, og svarer på anmodning om dette igennem disse Apps¹¹.

¹¹ <https://www.apple.com/researchkit/>

3. Analyse af udvalgte regler

Denne del af afhandlingen omhandler den, praktiske, juridiske analyse af de udvalgte regler i Forordningen. Fokus lægges på, om Sundhedsappen overholder reglerne om samtykke, princippet om gennemsigtighed samt oplysningspligten. Det er disse regler, der primært skal være overholdt for at sikre, at en behandling er lovlig. Dette skyldes, at alle artikler er omfattet af Forordningens oversigt over overtrædelser, jf. art. 83 stk.4-5, som potentielt medfører en bødestraf på op til 4 % af det foregående års omsætning. Derfor vil det være ligegyldigt om Sundhedsappen overholder enkelte af Forordningens artikler, men ikke de andre, da det i så fald alligevel vil medføre en bødestraf. Ligeså væsentligt er det, hvordan den form for sundhedsdata, som Sundhedsappen indsamler, kan karakteriseres. Dette skyldes, at det påvirker den hjemmel, som den dataansvarlige kan benytte ved indsamling af oplysningerne. Sanktionsrammen behandles yderligere i afhandlingens del 5-7.

3.1 Forordningens anvendelsesområde

Det materielle anvendelsesområde defineres i Forordningens artikel 2, stk.1. Forordningen finder således anvendelse, såfremt behandling af personoplysninger finder sted. Dette værende tilfældet uanset om behandlingen foregår automatisk, delvis automatisk eller ved manuel behandling. Sundhedsappen foretager en automatisk indsamling af personlige oplysninger, eftersom appen dagligt opdateres i real-time, hvilket betyder, at hvis personen bevæger sig, kan det umiddelbart derefter ses registreret på appen. Ved behandling af persondata skal enhver behandling opfattes som værende omfattet af begrebet "behandling" jf. Forordningens art.4, stk.2. Således er både Sundhedsappens automatiske indsamling, behandling, registrering og analysering af oplysningerne omfattet af begrebet *behandling*.

Apple skal ses som den dataansvarlige jf. Forordningens art.4, nr.7, da det er Apple, der som den juridiske person har dispositionsretten over oplysningerne og kan behandle disse. Databehandleren er den fysiske person, der behandler data på vegne af den dataansvarlige. I praksis vil dette typisk være en underleverandør, som har en kontrakt med den dataansvarlige. I forholdet mellem de to parter skal databehandleren være underlagt instruks fra den dataansvarlige jf. Forordningens art.4, nr.8. Det er derfor den dataansvarliges opgave at sikre, at behandlingen udføres efter reglerne i Forordningen, jf. Forordningens art.4 nr.7-8.

Ved persondata menes enhver information, hvormed der kan opnås en identifikation af en person jf. Forordningens art. 4, nr.1. Det være sig både direkte og indirekte, og bedømmelse foretages ud fra det

konkrete tilfælde. Alle fremgangsmetoder vil indgå i bedømmelsen af, hvorvidt det er muligt at identificere en person, og det er derfor ikke afgørende, om den dataansvarlige har benyttet den ene eller den anden fremgangsmetode. Da Sundhedsappen indsamler en række data, heriblandt navn, efternavn og fødselsdagsdato, vil den være omfattet af Forordningens anvendelsesområde, da det er muligt at identificere en person ud fra disse oplysninger. Her er det værd at bemærke, at Apple i anonymitetspolitikken har en anden opdeling end den Forordningen benytter med hensyn til, om oplysninger kan karakteriseres som værende personlige oplysninger. Forordningens anvendelsesområde tager udgangspunkt i, om der kan opnås identifikation af vedkommende. Dette gælder også for de personlige oplysninger i anonymitetspolitikken. Derimod benytter Apple følgende definition omkring de ikke-personlige oplysninger ”*oplysninger der ikke i sig selv kan forbindes med en enkelt person*”. Som nævnt i afsnittet omkring anonymitetspolitikken (del 2.3 afsnit 4) angives disse oplysninger som værende ”*beskæftigelse, sprog, postnummer og områdenummer, enhedens unikke identifikationsnummer, henvisende URL, lokalitet og den tidszone enheden er registreret i*”. Flere af disse informationer muliggør en identifikation, såfremt de anvendes i kombination med hinanden. Dette vil ikke være åbenlyst, og vil ikke altid kunne benyttes til identifikation, men det vil i mange tilfælde kunne lade sig gøre. Alt i alt bør der ikke foreligge nogen tvivl om, at de oplysninger der indsamles af Sundhedsappen, taler for at den er omfattet af Forordningens regler.

Ligeledes taler Forordningens art.4, nr.4 om profilering også for, at oplysningerne er omfattet af Forordningens anvendelsesområde, da oplysningerne potentielt kan benyttes til at profilere en person. Med dette menes, at en persons adfærd, helbred, pålidelighed og bevægelser kan forudsiges ud fra de indsamlede oplysninger. F.eks. kunne en person, der viser at tilbagelægge store afstande til fods, antageligt i forbindelse med motionsløb, være et interessant objekt til at annoncere for salg af løbesko. Det er således muligt at profilere en person ud fra de indsamlede oplysninger, og dette taler yderligere for at Forordningen finder anvendelse.

Apple har hovedkontor i Californien i USA, men iPhone sælges af Apple i EU med målrettet markedsføring mod unionsborgere. Der er samtidig tale om en aktivitet af permanent struktur, hvorfor Apple er etableret i unionen jf. Forordningens art.3 stk.1, samt TEUF art.49. Der er her ikke tale om en grænseoverskridende tjenesteyder, jf. TEUF art.57(1), da Apple samtidig er fysisk etableret med butikker i Danmark¹².

¹² Kure s.78

Forordningen finder derfor anvendelse da forudsætningerne i Forordningens art. 2-4, samt TEUF art.49 er opfyldt.

3.2 Oplysningernes juridiske karakter

På trods af at der findes en Sundhedsdatastyrelse, findes der ikke en officiel definition af Sundhedsdata i den danske ordbog. Sundhedsdata benyttes dagligt i det danske sundhedsvæsen, hvor der er tale om data fra patienter. Dette kan være alt fra oplysninger om patienters blodprøver til oplysninger om medicinforbrug. At definere Sundhedsdata som en samlebetegnelse for data, der kan beskrive den helbredsmæssige tilstand hos et eller flere individer, vil derfor ikke være forkert, men heller ikke præcist. Dette skyldes, at en beskrivelse af en persons helbredsmæssige tilstand formentlig indikerer, om personen er rask eller ej. Og det er ikke nødvendigvis hvad sundhedsdata beskriver. Den engelske definition af sundhedsdata er *data, der beskriver den helbredsmæssige tilstand, dødsårsager, livskvalitet eller muligheder for reproduktion hos den enkelte eller hos en gruppe af mennesker*¹³. Denne definition er bredere og dækker også de former for Sundhedsdata, som behandles af Sundhedsappen.

3.2.1 Karakter af de indsamlede personoplysninger jf. Forordningens art.9

Udgangspunktet i Forordningen er, at alle oplysninger, som ikke kan karakteriseres som følsomme, skal behandles som almindelige personoplysninger, jf. Forordningens art. 9, stk.1. Med dette lægger Forordningen derfor op til en ændring af, hvad er omfattet af begrebet *følsomme oplysninger*, da der brydes med begrebet om semi-følsomme oplysninger fra Persondataloven.

Sundhedsdata omtales ikke direkte i Forordningen, men nævnes derimod indirekte i oversigten over følsomme oplysninger, eksemplificeret ved 3 forskellige typer af data, jf. Forordningens art.9, stk.1. Disse er *Biometriske data, Genetiske data eller Helbredsmæssige oplysninger*. Definitionen på Biometrisk data findes i forordningens art 4, nr.14, men gengives her ikke ved eksempel. Dertil skal et fortolkningsbidrag fra Sundhedsdatastyrelsen inddrages, og her nævnes eksempler på disse som værende et ansigtsbillede eller fingeraftryksoplysninger¹⁴. Genetiske data defineres i art. 4, nr.13 og gengives ligeledes ikke med eksempler i Forordningen. Eksempler på disse er ifølge Sundhedsdatastyrelsen data fra biologiske prøver såsom DNA eller lignende¹⁵. Ingen af disse typer af Sundhedsdata passer på de oplysninger, der indsamles igennem Sundhedsappen.

¹³ https://en.wikipedia.org/wiki/Health_data

¹⁴ Bilag 2 – Sundhedsdatastyrelsen ordliste over brug af sundhedsdata

¹⁵ Bilag 2 – Sundhedsdatastyrelsen ordliste over brug af sundhedsdata

Helbredsoplysninger defineres i Forordningens art.4, nr.15 som: *Personoplysninger, der vedrører en fysisk persons fysiske eller mentale helbred herunder levering af sundhedsydelser, og som giver en information om vedkommendes helbredstilstand.* Denne definition passer delvist på de informationer, der indsamles af Sundhedsappen. Igen gives der ikke i Forordningen et konkret eksempel på, hvad der er omfattet af begrebet. For at disse informationer skal passe på definitionen *helbredsmæssige oplysninger* i Forordningen art. 9 stk.1, skal der være tale om data, der beskriver en persons sygdom, handicap, fysiologiske eller biomedicinske tilstand, sygdomsrisiko, eller helbredshistorik¹⁶. Retspraksis fra direktivet har afgjort, at information om at en person er syg, ikke udgør helbredsmæssige forhold, og der skal derfor mere til¹⁷. Anderledes forholdt det sig i dommen C-101/01 (Bodil Lindqvist), hvor det fastslås, at en oplysning om et forstuvet ben offentliggjort på en hjemmesid, var omfattet af begrebet følsomme oplysninger¹⁸. De indsamlede informationer kan vise udsving i den registreredes aktivitet, men ikke med sikkerhed fastslå, at der er tale om helbredsmæssige udfordringer eller risiko. Hertil er de indsamlede oplysninger ikke i nærheden af at fortælle det samme, som oplysningen i C-101/01 omkring det brækkede ben. Det passer derfor ikke på de indsamlede data, da der kan udledes en sådan information om den registrerede. De indsamlede oplysninger fra Sundhedsappen kan derfor ikke karakteriseres som følsomme oplysninger, da de ikke passer på definitionen i Forordningens art.4, nr.15, om helbredsmæssige oplysninger og skal derfor behandles som normale oplysninger, jf. Forordningens art.9, stk.1.

3.3 Forordningens regler om samtykke ved behandling af sundhedsdata

Sundhedsappens fremgangsmetode hvorpå den behandler personlige oplysninger, er at benytte et samtykke fra den registrerede. Som tidligere beskrevet gives dette samtykke både ved adgang til telefonens styresystem og når Sundhedsappen tages i brug for første gang. En aktiv handling fra den registrerede godkender hermed behandlingen. Det er det sidste samtykke, hvor der bedes om deling af Sundhedsdata med Apple, der er det relevante for denne del af opgaven, og benævnes i det følgende som samtykketeksten.

Det er forventet at det er skærpelsen af kravene til samtykke, der kommer til at forårsage de fleste af de administrative bøder, der vil blive udskrevet under Persondataforordningen¹⁹. Det at give et samtykke er formentlig det mest centrale aspekt af persondataretten. Såfremt det ikke var muligt at give samtykke, ville

¹⁶ Dall, Langemark og Langebæk s.45

¹⁷ Balci s.26

¹⁸ Balci s.26

¹⁹ Balci s.35

det utvivlsomt blive opfattet som en skærpelse af den enkelte borgers ret til at indgå aftaler. På den anden side er det digitale domæne et kompliceret sted at færdes. Med dette menes, at den registrerede ikke ved afgivelse af sine oplysninger med sikkerhed kan vide, hvordan hans data benyttes af den dataansvarlige. Samtykkereglerne fungerer derfor for at danne en ramme om det, den registreredes accept dækker over, samt hvad ikke er omfattet af tilkendegivelsen. Der er grænser for hvilke personer der kan afgive samtykke, da det kun kan afgives af habile personer. Dette er dog kun noget der er relevant for den dataansvarlige, såfremt der er grund til at tro, at personen er inhabil²⁰.

3.3.1 Hjemmelsgrundlag for behandlingen

Apple må kun foretage en behandling af personoplysninger, såfremt der er hjemmel til behandlingen i lov jf. Forordningens art.5. stk.1, litra a). Da samtykke er den anvendte hjemmel for Sundhedsappen, skal det nødvendige hjemmelsgrundlag til at behandle persondataoplysninger derfor findes i Forordningens art.6, stk.1. Der gives i denne artikel lov til at behandle personoplysninger, såfremt den registrerede giver samtykke til dette. Følsomme oplysninger ville kræve en udvidet hjemmel, og skulle dette være tilfældet vil den dataansvarlige skulle finde hjemmel blandt undtagelserne i art.9, stk.2. Dette er dog ikke nødvendigt, jf. afsnit 3.2.

3.3.2 Samtykkereglerne

I Forordningens art.7. findes de betingelser, den dataansvarlige skal overholde i forbindelse med samtykke, for at dette er afgivet korrekt. Her oplistes fire krav, stk.1-4, for at et samtykke er gyldigt. Stk.4 vedrører en kontraktrelation mellem de to parter og er derfor ikke relevant i denne sammenhæng. Den dataansvarlige har i forbindelse med indhentning af samtykke bevisbyrden for, at samtykket er givet korrekt, jf. art.7, stk.1. I denne sammenhæng bør der ikke benyttes mundtlige samtykker, da man kan ende i en klassisk problemstilling om påstand mod påstand. Med disse regler bliver direktivets regler udvidet, eftersom der er kommet flere krav med Forordningens ikrafttræden.

Det er den dataansvarliges opgave at sikre, at samtykket er holdt tilstrækkelig adskilt jf. Forordningens art. 7, stk.2. I den digitale verden kan dette generelt være et problem. Det er den dataansvarliges løbende opgave, da denne har bevisbyrden for at sikre, at disse opfylder betingelserne gyldighedsbetingelserne i art.7. Ved adgang til Sundhedsappen gives der et direkte samtykke til behandlingen fra den registrerede. Samtykket er kort og vedrører ikke andre forhold end at *forbedre Sundhed og Fitness-funktionerne*.

²⁰ Blume(1) s.65

Et samtykke kan tilbagekaldes, og den dataansvarlige bør i forbindelse med hjemmelsgrundlag overveje, om hjemmel kan findes andre steder end ved samtykke. Gamle samtykker er som udgangspunkt stadig gyldige på den betingelse, at de opfylder betingelserne i art.7, men kan tilbagekaldes af den registrerede til enhver tid jf. art.7, stk.3. Den registrerede skal have oplyst, at han kan tilbagekalde sit samtykke, ligeledes som at det skal være ligeså nemt at trække sit samtykke tilbage som at give det. Sundhedsappen oplyser den registrerede om dette i samtykketeksten. Ved at benytte Sundhedsappen er det dog ikke ligetil at finde ud af, hvor samtykket kan trækkes tilbage. For at gøre dette skal brugeren gå ind i telefonens *indstillinger* under *anonymitet* dernæst klikke på *analyse*, hvorefter dette kan slås fra.



Det vil være tilstrækkelig nemt for en bruger, såfremt der kan tilbagekaldes på samme internetside, som hvor samtykket er givet²¹. Da der er tale om en App, er det derfor spørgsmålet, om dette er tilstrækkeligt nemt for brugeren. Dette må være tilfældet, eftersom der stadig er tale om samme produkt, og at alle samtykker og delinger til andre enheder skal gives og tilbagekaldes netop ved at gå ind under *anonymitet* under *indstillinger*. Den registrerede kan dog vælge at tilbagekalde sit samtykke på en hvilken som helst måde, og kan derfor blot skrive til Apple, at han ønsker en deling af sine oplysninger stoppet øjeblikkeligt, hvorefter Apple skal imødekomme dette. Den allerede indsamlede data gennemgås under de generelle behandlingsprincipper 3.6.

Definitionen på et gyldigt samtykke findes i forordningens art.4, nr.11. Denne artikel stiller yderligere krav til indholdet af aftalen mellem brugeren og serviceudbyderen. Overholdes denne artikel ikke, vil samtykket ikke være gyldigt. Et samtykke defineres her som: *Enhver frivillig, specifik, informeret, utvetydig*

²¹ Dall, Langemark, Langebæk s.81

viljetilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling.

For at det digitale samtykke i Sundhedsappen skal være lovligt afgivet, skal det vurderes ud fra definitionen af samtykke i forordningens art.4, nr.11, med krav om at dette skal være *frivilligt, specifikt, informeret og utvetydigt*. Det nye i forhold til Persondataloven er her, at samtykket også skal være *utvetydigt*.

Betydningen af at noget er *Frivilligt* er naturligvis, at der ikke må foreligge tvang, når den registrerede accepterer. I betragtning 42 til Forordningen omtales *frivilligt*, som værende den situation hvor den registrerede reelt har et frit valg²². Her skal forholdet mellem de to parter diskuteres. I tilfælde af, at der eksisterer et *skævt* forhold mellem den registrerede og den dataansvarlige kunne dette føre til, at den registrerede ikke afgiver sine data *frivilligt*, som også omtales i betragtning 43. Dette kunne f.eks. være et ansættelsesforhold, hvor en ansat afgiver oplysninger til sin arbejdsplads evt. via en digital løsning omkring vagtbytte, om end dette formentlig ville ske fordi den registrerede ønsker det. Skulle den registrerede her modvilligt afgive sine data i frygt for at blive fyret, vil det derimod ikke være afgivet frivilligt. I

Sundhedsappens tilfælde er der ikke tale om et *skævt* forhold mellem den registrerede og den dataansvarlige, da den registrerede selv kan vælge at bruge andre udbydere end Apple. Skævt forhold skal forstås som f.eks en arbejdsgiver eller en offentlig myndighed, og det er altså ikke nok, at brugeren har en præference for Apple, for at forholdet kan karakteriseres som *skævt*. Brugeren kan også vælge ikke at dele sine oplysninger, men stadigvæk have adgang til Sundhedsappen, hvorfor der ikke er tale om indsamling af oplysninger, hvor brugeren betaler med at afgive sine data. Dette er derfor elementer der taler for at Sundhedsappen overholder kravet om *frivillighed* i betragtning 42-43, samt art.4, nr.11.

En ordlydsfortolkning af betragtning 42, med ordet *reelt*, kunne henlede tanken på den situation, hvor den registrerede afgiver sin accept med henblik på at ville have adgang til en bestemt service eller spil. Her vil en deling af oplysninger typisk ikke være nødvendig for at serviceudbyderen kan levere, men naturligvis alt afhængig af spillets karakter. *De registrerede vil have den vare de betaler for med deres data, og langt de fleste tænker ikke længe over, hvad deres data benyttes til, og finder handlen rimelig* jf. Peter Blume. Peter Blume mener derfor, at kravet om frivillighed er opfyldt, når den registrerede betaler med sin data²³.

²² Dall, Langemark og langebæk s. 250

²³ Blume(1) s.66

Forordningens krav om at samtykket skal være *specifikt og informeret* kan ses i en sammenhæng²⁴. At samtykket skal være *specifikt*, samt *informeret*, betyder at formålet skal oplyses til den registrerede på en måde, så han forstår det, og derfor ved hvad han giver samtykke til. I Sundhedsappens tilfælde ved samtykketeksten informeres brugeren om, at han kan vælge at godkende deling/behandling af oplysninger, samt at han kan læse omkring betingelserne for sin accept. Et typisk forekommende scenarie ved dette er, at den registrerede vælger **ikke** at kigge dette igennem, men blot klikker på *accepter*. En perspektivering til aftaleretten kunne være situationen hvor en aftalepart accepterer et tilbud uden at have set indholdet af aftalen. Typisk er årsagen til dette at disse betingelser tager lang tid at læse, kan være svære at forstå eller at brugeren mangler tålmodighed. På trods af dette er der stadigvæk tale om en aktiv og direkte handling fra den registrerede, såfremt denne accepterer anmodningen om samtykke. Spørgsmålet vil her være om en behandling efter indholdet i servicebetingelserne (Anonymitetspolitikken) er gyldigt, såfremt det varierer fra det direkte samtykke i samtykketeksten. At den registrerede skal informeres indebærer naturligvis også, at det ikke må skjules for den registrerede eller være svært at forstå, hvad der gives accept til. Helt præcist i forhold til Sundhedsappen kommer det derfor an på, hvor langt en behandling efter anonymitetspolitikken vil række, såfremt denne behandling varierer væsentligt fra det direkte oplyste formål om at *forbedre sundheds og fitness funktionerne*. Det må her være det klare udgangspunkt, at hvis den registrerede skal give accept til flere forskellige behandlinger eller flere forskellige formål, skal disse fremgå af den tekst, hvor der gives accept, også kaldet samtykketeksten²⁵. Betydningen af dette er, at en behandling af personoplysninger efter et formål anonymitetspolitikken vil være ugyldig, såfremt dette formål varierer fra en behandling efter indholdet i samtykketeksten. Formål som markedsføring og optimering af andre tjenester vil være eksempler på formål, der går ud over det nævnte formål i samtykketeksten. En behandling efter anonymitetspolitikken og de formål der oplystes, er derfor behandlinger som den dataansvarlige skal hente yderligere samtykke til og er ikke omfattet af formålet i samtykketeksten, med mindre det kan direkte sammenkobles til formålet om at forbedre fitness funktionerne.

Ligeledes indeholder Forordningens art.4, nr.11 krav om, at det skal være *utvetydigt*. Dette betyder, at der ikke må forekomme tvivl om, hvad det er, den registrerede accepterer ved sit samtykke til. Princippet minder derfor meget om det generelle princip i Forordningens art.5, stk.1, litra b) om *udtrykkelighed*. Mundtlige samtykker vil være gældende, hvorimod en passiv accept aldrig vil være det. Der skal være tale om en aktiv handling fra den registrerede, og forud udfyldte felter i afkrydsningsskemaer vil ikke være

²⁴ Dall, Langemark, Langebæk s.57

²⁵ Dall, Langemark, Langebæk s.57

gyldige. I Sundhedsappen forsøges dette krav overholdt med en klar erklæring til brugeren om, at formålet med indsamlingen er at *forbedre sundheds og fitness funktionerne*, hvilket ikke bør give anledning til tvivl hos den registrerede.

3.4 Gennemsigtighedsprincippet

Princippet om gennemsigtighed har som formål at øge gennemsigtigheden, når de registrerede benytter de forskellige services i det digitale domæne. Som beskrevet i indledningen er den manglende gennemsigtighed den måske største årsag til den faldende tillid. Mangel på gennemsigtighed forårsager at brugeren blot accepterer anmodninger om deling af personoplysninger, da det forekommer uoverskueligt at sætte sig ind i, hvad en accept reelt indebærer. Den registrerede må naturligvis også selv bære en del af ansvaret for sine egne handlinger. Det vil derfor ikke være forkert at opfatte disse regler som værende til for at sætte denne grænse.

3.4.1 Gennemsigtighedsprincippet jf. art.12

I Forordningens artikel 12, stk.1 beskrives en gennemsigtig kommunikation til brugeren som værende *"kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og i et klart og enkelt sprog"*.

Reglen om gennemsigtighed medfører, at brugeren ikke skal udsættes for oplysninger som kan virke uoverskuelige eller ikke-forståelige på grund af deres formulering. De skal samtidig leveres i et kortfattet format fra den dataansvarlige. Fremgangsmetoden for hvordan den dataansvarlige overholder gennemsigtighedsprincippet er op til den dataansvarlige selv. Skulle den dataansvarlige anvende lange juridiske tekster, hvor den registrerede opgiver at sætte sig ind i dem og blot klikker på accepterer, vil det være i strid med gennemsigtighedsprincippet. Det skal ikke være muligt for den dataansvarlige at gemme de mest belastende elementer fra brugerens opmærksomhed. Forordningen tilpasser sig således den generelle forbrugeretlige regel, om at de mest byrdefulde vilkår skal fremstå tydeligt for forbrugeren.

I forbindelse med adgang til Sundhedsappen er formuleringen i samtykketeksten, som kun henviser til brugerens Sundhedsdata indsamles, ikke særlig præcis. Brugeren afgiver data omkring *navn, efternavn, fødselsdag, køn, højde, vægt*. Det kunne sagtens uddybes, så brugeren var sikker på, hvilke af de indsamlede oplysninger i Sundhedsappen er dem som deles. Man må formode, at det er data omkring den fysiske aktivitet og søvn, men det vides ikke med sikkerhed. Den registreredes vægt og højde kunne også være iblandt disse, men det vides ikke med den formulering der benyttes. Apples definition af sundhedsdata bør derfor tydeliggøres, eftersom de indtastede data ikke nødvendigvis alle er oplysninger man vil kalde sundhedsdata.

I anonymitetspolitikken nævnes en del formål, som rækker langt ud over det formål, der beskrives i samtykketeksten. Her nævnes forskellige formål for behandlingen i forbindelse med en række af de personlige oplysninger, der indsamles, som ydermere angives under samlebetegnelsen *tjenester*. Samlebetegnelsen *tjenester* kunne sagtens inkludere Sundhedsappen. Skulle den registrerede først læse samtykketeksten, men derefter ville have dette uddybet i anonymitetspolitikken, vil han først skulle tage sig tid at forstå indholdet. Dette ville ikke være tilstrækkeligt, såfremt den registrerede vil finde ud af, hvilke oplysninger der konkret hentydes til. Dette skyldes naturligvis, at der er tale om en generel anonymitetspolitik. Hertil kunne den dataansvarlige udarbejde en separat og forkortet udgave, som udelukkende vedrørte Sundhedsappen. Her bør det oplyses, hvilke informationer der udgør sundhedsdata, og hvad de indsamlede oplysninger anvendes til.

3.5 Oplysningspligten jf. Forordningens art.13

Oplysningspligten er hjemlet i Forordningens art. 13. Art. 14 i Forordningen omhandler ligeledes oplysningspligten overfor den registrerede, men vedrører situationen, hvor oplysningerne hentes fra andre end den registrerede. Art.14 er derfor ikke relevant, for det faktum der anvendes omkring Sundhedsappen. Art. 13 i Forordningen er relevant, eftersom denne artikel omhandler de krav der stilles til formidlingen mellem den dataansvarlige og den registrerede, ved at der hentes samtykke direkte fra den registrerede. Ligesom tidligere er det ønskeligt at imødekomme førnævnte situation, hvor den registrerede ikke kigger betingelser igennem men blot klikker på *accepter*.

Genstand for denne analyse er ligeledes den information, der formidles til de registrerede fra Apple igennem Sundhedsappen. Med de nye regler vil den registrerede nemmere kunne forstå sine rettigheder, eftersom han informeres om dem i samtykketeksten, end hvis han skal kigge en lang politik igennem. Her kan der argumenteres for, at man i virkeligheden giver den registrerede en bedre beskyttelse mod hans egen manglende tålmodighed.

Oplysningspligten består af tre kumulative krav for overholdelse, med stk.4, som hjemmel til undtagelse fra at overholde kravene i art 13, stk.1-3. Nr.1-2 kommer med seks krav der er angivet i bogstaver litra a-f i de to bestemmelser.

Oplysningspligten gør, at det skal fremgå, hvem der er den dataansvarlige, jf. stk.1, litra a). Kontaktoplysningerne på denne skal ligeledes fremgå af oplysningerne jf. litra b). Det fremgår ikke af

samtykketeksten i Sundhedsappen, hvem der er dataansvarlig eller hvordan denne kan kontaktes. Det er derimod ikke oplysninger den registrerede vil have problemer med at fremskaffe, da det oplyses at delingen af oplysningerne er med Apple, samt at Apple's kontaktoplysninger er indkodet som standard i iPhone. Der er derfor tale om oplysninger, som brugeren allerede er bekendt med, eller med relativt lethed kan fremskaffe, hvilket gør at stk.4 omkring oplysninger den registrerede allerede er bekendt med, ikke skal fremgå i teksten.

Formålet med behandlingen oplyses til gengæld af Apple, ved at brugeren i samtykketeksten skal tage stilling til deling, hvilket er i overensstemmelse med litra c) i bestemmelsen. Derimod kræver art.13, stk.1, litra c) at der udover formålet med delingen også oplyses hjemmel til behandlingen, hvilket ikke indgår i samtykketeksten til Sundhedsappen. Det vil her skulle fremgå, at der er hjemmel til samtykke jf. Forordningens art.6, stk.1 litra a). Oplysninger om hjemmel for behandlingen fremgår heller ikke i anonymitetspolitikken.

Litra d) i stk.1 stiller krav om, at den registrerede skal vide hvilken kategori af oplysninger der indsamles. Det fremgår ikke af samtykketeksten, hvilken kategori af personoplysninger der indsamles. Det fremgår dog i anonymitetspolitikken, hvor Sundhedsappen ikke nævnes ved navn, men blot ved samlebetegnelsen tjenester, hvorfra de forskellige kategorier er oplistet. Dette er dog en anonymitetspolitik gældende for alle Apples tjenester, og dette er derfor ikke tilstrækkeligt oplyst. Skulle dette være tilstrækkeligt, skulle det være angivet i samtykketeksten.

Litra e) i stk.1 kræver, at den dataansvarlige oplyser den registrerede om, hvorvidt modtageren kan opdeles i kategorier, dvs. også datterselskaber, samarbejdspartnere og lign. Dette fremgår ikke af samtykketeksten i Sundhedsappen, hvor Apple således nævnes som den eneste modtager. Dette er dog, igen noget, som Apple oplyser at de gør i anonymitetspolitikken, hvor det oplyses at både samarbejdspartnere og datterselskaber, "*muligvis*", også modtager de forskellige typer af oplysninger. Dette må ligesom litra d) fortolkes på samme måde, som kravet til samtykke. Man kan ikke give samtykke til noget, man ikke er bekendt med, og det er derfor ikke tilstrækkeligt at der gives informationer i en generel anonymitetspolitik omkring dette.

Skulle oplysningerne videregives til en datacentral eller lign. med beliggenhed udenfor Det Europæiske Økonomiske Samarbejde (EØS), også kaldet tredjelande, vil den registrerede skulle oplyses herom jf. artikel 13, stk.1, litra f). Det kræver, at den registrerede giver sit udtrykkelige samtykke, og samtidig skal han

informeres om risikoen, som hans accept indebærer i forbindelse med, at han accepterer dette. Det nævnes ikke i forbindelse med samtykketeksten til Sundhedsappen, at dette er tilfældet. I anonymitetspolitikken under Internationale brugere beskrives det alligevel, at det kan forekomme at oplysningerne udveksles²⁶. På Apples hjemmeside oplyses det, at oplysningerne fra Sundhedsappen lagres lokalt på telefonen og sendes til iCloud. Såfremt de faktiske omstændigheder ved denne sikkerhedskopiering til iCloud gør, at oplysningerne er placeret i USA, skal det fremgå af samtykketeksten. Dette er ikke tilfældet på nuværende tidspunkt.

I artikel 13, stk.2 henvises der til principper om rimelighed og gennemsigtighed, og der stilles med litra a-f yderligere krav til den dataansvarlige. Tidsrummet for behandlingen af oplysningerne skal her oplyses til den registrerede jf. art.13, stk.2, litra a). Såfremt det ikke er muligt at fastlægge et tidsrum for behandlingen, skal der fremgå, med hvilke kriterier for tidsrummet behandlingen foretages efter. Det oplyses ikke ved samtykketeksten, hvor lang tidshorisont oplysningerne behandles. I anonymitetspolitikken fremgår det dog, at personoplysninger kun opbevares så længe det er nødvendigt for at opfylde det formål, behandlingen er foregået med²⁷. Dette er dog, igen, kun oplyst ud fra samlebetegnelsen tjenester, og der tages ikke stilling til Sundhedsappen specifikt.

Stk.2, litra b) i oplysningspligten pålægger samtidig den dataansvarlige at informere de registrerede om deres rettigheder. Der skal informeres til den registrerede om, at denne kan kræve indsigt i de indsamlede oplysninger. Sundhedsappen skal informere de registrerede om at oplysningerne skal slettes, berigtiges, eller at behandlingen skal begrænses, såfremt den registrerede anmoder om dette. Dette nævnes ikke direkte, men Sundhedsappen forholder sig alligevel delvis til dette i samtykketeksten. Det nævnes her, at en deling med Apple kan afbrydes, såfremt den registrerede ønsker det. Der nævnes her intet direkte om sletning, men i anonymitetspolitikken indgår oplysninger om, hvordan den registrerede kan bede om både sletning og berigtigelse samt hvordan den registrerede får indsigt i, hvilke oplysninger Apple har om den registrerede. Muligvis er dette relevant ved brug af Sundhedsappen, da den registrerede selv har overblik over de indsamlede oplysninger ved at kigge i Sundhedsappen. Det er noget brugeren kan bede om, men som ikke er oplyst i samtykketeksten.

Såfremt en behandling er givet på baggrund af samtykke jf. Forordningens art.6 stk.1, litra a), eller ved udtrykkeligt samtykke i jf. art.9, stk.2 litra a) omkring følsomme oplysninger, skal den registrerede

²⁶ Bilag 3 s.6

²⁷ Bilag 3 s.4

informeres om muligheden for at trække sit samtykke tilbage jf. art.13, stk.2, litra c). Da Sundhedsappen netop benytter samtykke som hjemmel, er det derfor omfattet af denne bestemmelse. Det nævnes i samtykketeksten, at en deling med Apple til enhver tid kan trækkes tilbage. Dette krav overholdes derfor af Apple.

I samtykketeksten nævnes ikke muligheden for at klage til en tilsynsmyndighed, som kræves jf. litra d). Dette nævnes dog i anonymitetspolitikken som værende den nærmeste retskreds, hvor den registrerede befinder sig. Dette er derfor også mangelfuldt ved formidlingen til den registrerede.

Medhørende til kravene i oplysningspligten er også situationen, hvor den dataansvarlige påbegynder en ny behandling. Med dette menes, at såfremt den nye behandling ikke foregår efter samme formål som oplyst til den registrerede ved afgivelse af det oprindelige samtykke, skal den registrerede oplyses om dette på ny jf. Forordningens art.13, stk.3. Skulle en behandling af Sundhedsappen udelukkende foregå efter det oplyste formål i samtykketeksten, vil det være unødvendigt at informere den registrerede. Gøres dette skal den registrerede oplyses om forholdet, som netop gennemgås i art.13, stk.1-2. Dette overholdes derfor som udgangspunkt af Apple.

3.6 Generelle behandlingsprincipper

Der opstilles i Forordningens art.5 en række grundlæggende principper, der altid skal overholdes ved behandling af personoplysninger. Dette gælder uanset, om der er tale om følsomme oplysninger eller de normale personoplysninger. Principperne fortæller ikke, hvorvidt en behandling må foretages. Den vedrører spørgsmålet om, hvordan en behandling skal foregå. Dette angives i Forordningens art.5, stk.1, opstillet i punktform med seks punkter tilknyttet fra litra a-f. Principperne skal altid overholdes, uanset om det er den dataansvarlige eller databehandleren, der foretager behandlingen. Det overordnede ansvar ligger dog primært hos den dataansvarlige²⁸.

Forordningens art.5, stk.1, Litra a) har karakter af en generalklausul. Denne artikel hjemler, at behandlingen skal være lovlig, rimelig og gennemsigtig. Disse krav er meget tilsvarende principperne om god databehandlingsskik fra Persondataloven, hvorfor der her ikke er tale om en væsentlig ændring i forhold til direktivet. En lovlig behandling, forudsætter at der kun må behandles personoplysninger, såfremt der er lovhjemmel til behandlingen enten i Forordningen eller anden lovgivning. Rimelighedsprincippet i litra a) er

²⁸ Dall, Langebæk, Langemark s.51

sat ind som en måde, hvorpå der kan laves en overordnet bedømmelse af forholdet, og give mulighed for at argumentere ud fra dette princip. Principperne skal derfor i praksis benyttes til at fortolke de øvrige bestemmelser.²⁹

Litra b) omhandler det pågældende formål for indsamlingen. Dette skal være udtrykkeligt angivet, behandles legitimt og ikke senere behandles efter et formål der er uforeneligt med det oprindelige. Det er den dataansvarliges opgave at klarlægge, med hvilket formål oplysningerne indsamles inden dette finder sted, og det opvejes mod hvilken hjemmel behandlingen foretages. En senere behandling behøver ikke være præcis med det oprindelige, men må heller ikke være i modstrid med det oprindelige formål³⁰. Når dette vurderes skal den dataansvarlige vurdere det nye formål, samt hvilken betydning det har for den registrerede. For at Sundhedsappen skal overholde kravet omkring udtrykelighed vil det medføre en formidling af formålet i veldefineret sprog til den registrerede. Der kræves ikke en præcisering ned i mindste detalje, men en helt overordnet beskrivelse såsom "til brug for kommercielle formål" vil være utilstrækkelig, og skal defineres mere præcist. Derimod vil et formål som "til brug for salg af køretøjer", være tilstrækkeligt³¹. Sundhedsappen angiver et formål om at *forbedre sundhed og fitness-funktionerne*, som brugeren bedes om samtykke til ved at bede ham om at dele oplysningerne med Apple. Dette formål er i sig selv præcist og angivet i et let forståeligt sprog, og det taler for at princippet overholdes.

Litra c) er princippet om dataminimering. Dette princip siger, at oplysningerne der indsamles skal være tilstrækkelige, relevante, og begrænses så det kun er de nødvendige oplysninger der indsamles for at opnå formålet med indsamlingen. Det er dermed ønsket i litra c) at stoppe for en "tilfældig" indsamling uden formål blot for at have den liggende til senere brug. For at overholde princippet, vil den dataansvarlige for Sundhedsappen skulle foretage en vurdering af nødvendigheden af de indsamlede oplysninger i forhold til formålet med indsamlingen. Sundhedsappen indsamler følgende data: Søvn i antal timer, fysisk aktivitet i form af distance tilbagelagt, samt tælling af skridt fra den registrerede. Derudover indsamles de mere generelle data om brugeren såsom: Fornavn, efternavn, fødselsdag, køn, vægt, samt højde³². De indsamlede data skal derfor stemme overens med formålet om at *forbedre sundheds og fitness-funktionerne*. I forhold til den fysiske aktivitet kunne man sætte spørgsmålstegn ved, at man indsamler oplysninger om køn, vægt og højde samt fødselsdag, men da Sundhedsappen udregner et estimeret antal af kalorier der forbrændes, er disse data relevante i denne sammenhæng. Om det er nødvendig, at

²⁹ Burcu s.20

³⁰ Dall, Langebæk, Langemark s.53

³¹ Dall, Langebæk, Langemark s.53

³² Bilag 1 – Apple test case billede 20 + 22

indsamle oplysninger om navn kunne diskuteres. Potentielt kunne denne app blot fungere ved, at man logger ip-adressen lokalt på telefonen uden at indsamle flere oplysninger fra den registrerede end de, der er nødvendige for at give et estimat over den fysiske aktivitet. Det må i denne sammenhæng indgå i bedømmelsen, at Sundhedsappen's produkt vil blive forbedret, såfremt de formår at give en individuel og personlig oplevelse ved at benytte App'en. Dette aspekt taler for nødvendigheden af, at alle de indsamlede oplysninger er nødvendige for at appen kan optimere selve brugeroplevelsen, og behandlingen må anses som minimeret til det nødvendige.

Omkring behandling til andet formål, end det formål der gives til den registrerede ved samtykketeksten, gives der i art.6 stk.4 mulighed for, at den dataansvarlige, såfremt der er en sammenhæng med det oprindelige formål, at anvende oplysningerne uden indhentning af nyt samtykke. Dette er en regel, hvis omfang ikke kendes på nuværende tidspunkt. Der oplistes nogle betingelser omkring forholdet, men på nuværende tidspunkt kan der ikke udledes information om, om dette giver anledning til, at de dataansvarlige får en stor mulighed for dets anvendelse. Det alt overskyggende udgangspunkt må indtil videre være, at en behandling ikke må være modstridende med det formål, der beskrives ved det oprindelige samtykke.

Litra d) omhandler korrekthed og ajourføring (omtales også datakvalitet). Dette medfører, at de indsamlede personoplysninger skal være korrekte, og den dataansvarlige pålægges at tage ethvert rimelig skridt for at sikre, at dette overholdes. Hvad der menes med ethvert rimeligt skridt må bedømmes i forhold til, hvor langt den dataansvarlige skal gå for at opdatere oplysninger, samt hvor indgribende det vil være for den registrerede, såfremt disse oplysninger ikke er korrekte³³. Da de indsamlede oplysninger i Sundhedsappen blot måler den fysiske aktivitet, vil det som udgangspunkt ikke være relevant at overveje at ajourføre disse. Fejlagtige oplysninger vil forringe produktets kvalitet, men vil ikke umiddelbart være til skade for den registrerede. Denne risiko for at fejlagtige oplysninger kan skade den registrerede, vil naturligvis være højere jo flere forskellige typer oplysninger om den registrerede, den dataansvarlige er i besiddelse af. Skulle der her tilføjes oplysninger på grund af, at den registrerede benytter en wearable, såsom Apple iWatch, og den registrerede afgiver oplysninger såsom pulsmålinger, blodtryk og lign., vil dette naturligvis øge den registreredes risiko for at fejlagtige oplysninger potentielt kunne være til skade for vedkommende. Et forhøjet og livsfarligt blodtryk, som er fejlregistreret ville fejlagtigt kunne fortælle, at den registrerede led af akutte helbredsmæssige problemer. Det ressourcemæssige hensyn bag ordlyden

³³ Dall, Langebæk, Langemark s.54

ethvert rimeligt skridt kunne tale for, at oplysninger som disse, ikke skal ajourføres af den dataansvarlige. Hertil er risikoen ikke stor for, at de fortæller noget afslørende eller krænkende om den registrerede.

Litra e) omhandler den tid, de pågældende data opbevares. Den dataansvarlige må ikke opbevare oplysninger, der ikke længere er relevante. Af retspraksis fra PDL var denne grænse sat til at være maks. 5 år³⁴. Oplysninger skal, efter de ikke længere er relevante, slettes eller anonymiseres, så de ikke kan spores til den registrerede længere. I Sundhedsappen kunne det sagtens være indenfor formålet med brugen af appen, at sammenligne ens "performance" over tid, hvilket taler imod en sletning af oplysningerne ud fra formålet med indsamlingen. Omvendt kunne meget gamle sundhedsdata måske heller ikke have nogen stor værdi for den registreredes indsigt i egen sundhed. Det vil være den dataansvarliges opgave at vurdere denne nødvendighed, hvilket skal foretages efter proportionalitetsprincippet. Jo længere tid disse data opbevares, des større vil sandsynligheden være for at være i strid med litra e). En fastlagt sletterutine kunne være en måde, hvorpå en den dataansvarlige overholder dette princip. Alternativt kunne der indsættes en tydelig påmindelse, evt. en gang årligt, hvor den registrerede gøres opmærksom på, at sætte denne tidsperiode. Det nævnes selv af Apple i anonymitetspolitikken, at den dataansvarlige (Apple) selv sørger for at slette gammel og ikke relevant data fra deres tjenester. I anonymitetspolitikken nævnes Sundhedsappen ikke direkte. I stedet nævnes samlebetegnelsen *tjenester*, hvor Sundhedsappen må være iblandt. Hvor lang denne periode i realiteten er, kan ikke læses fra anonymitetspolitikken, der blot angiver et passende tidspunkt i forhold til formålet.

³⁴ Balci s.22

4. Konsekvensanalyse og datasikkerhed

Formålet med datasikkerhed er, at kun autoriserede personer eller den registrerede selv gives adgang til, at kunne læse den registreredes data. Forordningen har som mål at den dataansvarlige har interesse i dette, og sanktionerer såfremt datasikkerhed ikke opnås eller prioriteres. Et angreb på datasikkerheden kan komme udefra, men også indefra, og den dataansvarlige skal indstille sin databehandling efter, hvilke risici det vil kunne medføre for den registrerede. Gør han ikke det kan det medføre, at personoplysningerne overtages og anvendes til uautoriserede formål, opstilles forkert og dermed vises i forkerte sammenhænge, eller i bedste fald blot bliver tilintetgjort. Årsager til at personoplysninger angribes kan være mange. Nogle gør det for at vise, at det kan lade sig gøre, som var det en sport. Nogle gør det for penge eller hævn. De personlige oplysninger kan også fejlbehandles, og sikkerhedsbrud kan skyldes simple, interne fejl i administrationen.

Problemets størrelse i en juridisk kontekst afhænger ikke af, i hvor høj grad den registrerede selv anser det som værende et problem, at lige præcis hans oplysninger indsamles. Det kan der være mange forskellige meninger om, og det vil helt sikkert ikke være lønsomt for et firma som Apple, at spørge alle sine brugere om dette. Derfor må der foretages afvejninger, og risikoen må bedømmes aktivt, af de dataansvarlige samt passivt af lovgiver igennem regulering, for at sikre behandlingens risiko minimeres.

Forskellige behandlinger kræver forskellig opmærksomhed og foranstaltninger. Her kan sundhedsdata generelt skabe et problem for den registrerede såfremt de frigives og er disponible for vilkårlige. I forbindelse med tegning af en forsikring, kan der f.eks. være adskillige grunde til, at den registrerede ikke er interesseret i at sundhedsdata, er tilgængelige for enhver. Her vil en højere risiko set fra forsikringsselskabets side kunne medføre, at den registrerede skal betale en højere præmie. F.eks. ville en kræft patient, der ønsker at tegne en livsforsikring, formentlig ikke få lov til dette, eller skulle betale en høj præmie. Det ville ikke være utænkeligt, at nogle forsikringsselskaber ville benytte deres analytikere til, at få indsigt i hvilke mønstre i den anvendte data, der kunne antyde, en forhøjet risiko for, at en forsikringssum ville komme til udbetaling. Det samme kan siges om den registreredes jobmuligheder, som også kan blive forværrede, såfremt sundhedsdata blev offentliggjort. Hvis man ofte er disponeret for sygdom, kan en potentiel arbejdsgiver fravælge en potentiel medarbejder i en ansættelsessituation hvis det konkluderes, at en ansættelse ville medføre større udgift pga. flere sygedage. Det er heller ikke sikkert, at man i privat øjemed har lyst til, at ens omverden skal kende til de helbredsmæssige skavanker, man dør med. Som eksempel på dette kan nævnes at der for nylig var en historie i medierne, om en dating App for

homoseksuelle, der havde som standard, at brugerne delte informationer om, hvorvidt de var smittet med HIV³⁵. Når brugere afgiver oplysninger som dette, gøres det formentlig i bedste mening. Brugere benytter sådanne Apps i en fart, og tænker ikke nødvendigvis længere frem end de næste par klik på skærmen. Det er den dataansvarliges job, at forudse de eventuelle konsekvenser for brugeren. I situationen med oplysninger om HIV-smitte, bør den dataansvarlige tage foranstaltninger der afhjælper den risiko den registrerede løber ved at afgive disse informationer. Løsningen i lige præcis situationen med informationer om HIV-smittede, ville være at ændre den til ikke at indeholde oplysninger af denne karakter, da der er tale om følsomme oplysninger, som ikke kan indsamles uden hjemmel i lov, jf. også afhandlingens del 3.

4.1 Konsekvensanalyse af Sundhedsappen

Sundhedsappen indsamler følgende data fra den registrerede:

- Fornavn
- Efternavn
- Fødselsdagsdato
- Køn
- Højde
- Vægt

Derefter indsamles løbende oplysninger baseret på den registreredes brug. Disse er følgende:

Søvn i antal timer/min.

Fysisk aktivitet i antal skridt og distance opgivet i km³⁶.

Appen foretager en analyse af, i hvilke tidsrum den registrerede er aktiv. Dette gælder for alle behandlinger af Sundhedsappen. Den registrerede kan således se, alle registreringer, der foretages for tilbagelagt distance, den registreredes søvn, og pulsmålinger såfremt iWatch er tilknyttet. Tilknyttes flere oplysninger, stiger risikoen. Sundhedsappen tillader netop en sammenkobling med iWatch, og har desuden en funktion hvor blodtryk kan indtastes manuelt.

³⁵ <http://nyheder.tv2.dk/udland/2018-04-03-homo-datingapp-far-hug-for-at-dele-brugeres-hiv-oplysninger>

³⁶ Bilag 1 - Apple test case nr. 20, 22



Et element der afspejler den potentielle risiko, er hvor mange mennesker der kan se dem. Apple gemmer den registreredes oplysninger lokalt på telefonen, og sender dem i en krypteret udgave til iCloud, som er telefonens back-up system³⁷.

4.1.1 Risiko på indsamlingstidspunktet

På indsamlingstidspunktet er det begrænset, hvor megen skade det vil medføre, at oplysninger om en persons fysiske aktivitet i løbet af dagen samt søvnrytme offentliggøres. Offentliggørelse inddrages her, som sammenligningsgrundlag for, hvad det værste der kan forekomme med hemmelige oplysninger kunne være. I det hele taget er oplysningerne ikke af en krænkende art, og mennesker er ofte tilbøjelige til at dele disse, måske på nær oplysningen om personens vægt. Skulle oplysningerne, på indsamlingstidspunktet, sammenlignes med andres personers oplysninger, forelægger der ikke mistanke om, at den registrerede ville fremstå krænkende. Anderledes forholder det sig omkring oplysningen om blodtryk. Såfremt den registrerede er ved dårligt helbred, ville denne oplysning, potentielt, kunne være afslørende om den enkelte, og derfor være krænkende såfremt den offentliggøres. Dette ville kræve, at personen faktisk var syg før det var tilfældet, og skulle i langt de fleste tilfælde ikke afsløre noget om den registrerede.

4.1.2 Risiko over tid

De indsamlede oplysninger kunne potentielt over en tidsperiode, f.eks. 1-2 år vise udsving i den aktivitet, den registrerede har. En lav aktivitet og døgnrytme, som måles mod det normale for den registrerede ville være et udsving. Udsving som potentielt kunne få den registrerede til at fremstå mindre gunstigt, f.eks. hvis de tolkes af den der analyserer dem, som en sygeperiode eller svagt helbred. Den dataansvarlige bør i en

³⁷ <https://support.apple.com/da-dk/HT203037>

konsekvensanalyse, inddrage dette aspekt, og altid tænke i "worst case scenario". Dette gælder specielt såfremt der er tale om, at den tilkoblede wearable iWatch ligeledes er tilknyttet Sundhedsappen. Der vil i dette tilfælde indsamles oplysninger om den registreredes pulsmålinger, som ligeledes kan inddrages i en analyse. Apple er i særdeleshed et Big Data firma. Såfremt ikke blot den registreredes egne oplysninger offentliggøres, men en stor gruppe af mennesker får deres data offentliggjort, vil dette potentielt kunne føre til en krænkelse af de registrerede. Her bør det høre med til vurderingen, at såfremt oplysningerne sammenlignes med hinanden, og vises holdt op mod hinanden på nettet, kunne de mest dovne, eller syge individers data vises frem for offentligheden. Man kunne sagtens forestille sig, at dette bestemt ikke ville være i den registreredes interesse. Der er tale om de værst tænkelige omstændigheder, og formentlig ikke særlig sandsynligt, især fordi der er ikke bør kunne findes et økonomisk motiv for, at dette skulle ske. Det er dog den dataansvarliges job, at tænke i disse baner, og kunne fremvise dokumentation for, at det er situationer som disse, han indretter sit compliance-arbejde mod ikke at forekomme. Måden at imødekomme dette aspekt på vil for den dataansvarlige være at sørge for, at oplysningerne ikke gemmes i for lang tid af gangen. En fast sletterutine efter noget tid, vil være en foranstaltning der gør, at dette forhindres, som også omtalt i del 3.

4.1.3 Elementer der taler imod risiko

Offentliggørelse af de indsamlede oplysninger er ikke noget, man som udgangspunkt ville finde krænkende. Dertil ville de skulle præsenteres på en afslørende måde, før dette skulle være tilfældet. Med dette menes, at en person skulle hacke sig til oplysningerne, analysere dem, og fremstille grafer/ illustrationer hvor de dovne og syge blev fremstillet på en negativ måde. Hertil er det svært, at finde et motiv, som skulle gøre evt. hackere eller andre interesserede i at gøre dette. Der bør ikke kunne findes et økonomisk motiv for, at en hacker ville ihærdige sig, til først at komme i besiddelse af oplysningerne, og dernæst krænke de registrerede. Skulle et motiv kunne findes, skulle det være, at oplysningerne kunne benyttes som afpresningsmiddel overfor Apple, da det ikke er i deres interesse at de frigives. Sekundært kunne oplysningerne benyttes, som afpresningsmiddel overfor den registrerede, men dette er mindre sandsynligt. Dette ville dog kræve, at den der tilkæmper sig disse oplysninger, allerede inden angrebet, er klar over at lige præcis disse oplysninger om den pågældende, vil vise noget krænkende. De fleste registrerede har, formentlig, ikke tydelige tegn på sygdom, der kan aflæses ud fra disse oplysninger, og det er derfor meget usandsynligt, at et angreb foretages for at afpresse de registrerede.

4.2 Den juridiske ramme omkring beskyttelse af oplysningerne

Forordningen er neutral i forhold til teknologi, hvorfor den ikke kommer med udspecificerede krav til, hvordan den dataansvarlige skal opsætte sit netværk og lign. Dette kan skyldes, at teknologi er i uafbrudt udvikling, hvorfor det ville blive kræve konstant opdatering af Forordningen, blot for at imødekomme den teknologiske udvikling. Afgørende er at der er sikkerhed, og ikke hvordan denne sikkerhed opnås jf. art.42, stk.3, samt også art. 32. Der skal foretages en risikovurdering af enhver behandling, og beskyttelsen skal indrettes derefter. Det passende beskyttelsesniveau kan ikke opnås ved at følge en tjekliste, og de dataansvarlige må foretage en objektiv vurdering af forholdene. En objektiv vurdering skal forhindre de dataansvarlige i at foretage en vurdering der ikke viser risiko, og derfor ikke beskytter de registreredes oplysninger. Dette vil ikke være i de dataansvarliges interesse, da manglende compliance af sikkerhedskrav også straffes³⁸.

En vurdering af risiko har generelt to overordnede niveauer. Med dette menes at der enten er tale om høj risiko, eller lav/ingen risiko. Ved høj risiko, skal proceduren jf. art.35 følges. Er dette ikke tilfældet, vil det være den almindelige procedure jf. art.32 der altid skal følges, såfremt man som dataansvarlig behandler persondata³⁹. Ud over dette findes der andre principper i Forordningen, som også skal følges såsom Privacy By Design/Default principperne og nødvendigheden af ansættelse af ekspertise i form af Data Protection Officer.

4.2.1 Privacy by design/default

Forordningen indfører som noget helt nyt Privacy By Design og Privacy By default principperne. Disse principper er hjemlet i betragtning 78, samt art.25. De to principper minder om hinanden, og er svære at adskille. Privacy By Design indebærer, at virksomheden skal sikre at alle deres systemer og processer, der anvendes til behandling af persondata, har den fornødne sikkerhed. Fornøden sikkerhed betyder, at såfremt noget er dyrebart skal det beskyttes bedre. Sikkerhedsniveauet skal derfor være sat i forhold til den registreredes risiko. Det skal være "designet" til at klare persondatabeskyttelse. Privacy By Default indebærer, at udgangspunktet for databehandling i organisationen er at beskytte personoplysninger. En måde at overholde disse principper på ville være, at den dataansvarlige udviklede et system, hvor den der behandler den indtastede data, alene har mulighed indtaste de nødvendige oplysninger. Dernæst skulle systemet være udviklet, så oplysningerne slettes ligeså snart de ikke er nødvendige. De to principper

³⁸ Dall, Langebæk og Langemark s. 98

³⁹ Dall, Langebæk og Langemark s. 97

gælder desuden ikke kun virksomhedens IT-systemer, men hele organisationens databehandling⁴⁰. Derfor skal virksomhedens interne procedurer og kommunikationsprocesser ligeledes indrettes efter at overholde principperne.

4.2.2 Data Protection Officer

Virksomheden kan vælge, at udnævne en Data Protection Officer (DPO), som skal være virksomhedens rådgiver i forhold til databeskyttelse. Dennes opgaver er at rådgive virksomheden og uddanne medarbejderne, så reglerne overholdes. Dette kan være enten en intern medarbejder eller en person virksomheden hyrer udefra. Det skal være en person der er godt rustet til opgaven, og art. 39 oplister således en række opgaver som DPO'en, som minimum skal varetage i organisationen. Han må gerne have andre opgaver i virksomheden, men de andre opgaver må ikke have modstridende interesse med databeskyttelse. Virksomheden skal meddele datatilsynet hvem der er DPO, samt dennes kontaktoplysninger. Det er DPO'en, der er virksomhedens kontakt til datatilsynet, og skal samarbejde med dem når det er nødvendigt⁴¹.

En virksomhed er tvunget til at have en DPO, såfremt den regelmæssigt har aktivitet med behandling af enten følsomme oplysninger eller oplysninger, der udgør en regelmæssig overvågning af den registrerede i stort omfang. Som med mange andre områder af Forordningen er bestemmelserne omkring DPO gjort brede. Det er derfor ikke nærmere bestemt, hvad der udgør eks. *I stort omfang*. Der vil formentlig blive kigget på virksomhedens hovedaktivitet i denne bedømmelse⁴².

4.2.3 Sundhedsappens passende sikkerhedsniveau som følge af risikovurdering

Der er flere elementer der taler for, at Sundhedsappens behandling ikke nødvendiggør en anvendelse af høje foranstaltninger. Det der taler for at oplysninger, som behandles af Sundhedsappen skal være omfattet af art.32 er, at de ikke i sig selv udgør nogen stor fare for den registrerede. De har ikke nogen speciel værdi, og bør derfor ikke være i fare for hackerangreb eller lign. En offentliggørelse ville kun i meget begrænset omfang krænke den registrerede, da oplysningerne først ville skulle analyseres for overhovedet at komme i nærheden af at kunne bruges/misbruges. Dette taler for en anvendelse af art.32, og dette niveau af beskyttelse. I art.32 stk.1 nævnes, at den dataansvarlige kan benytte sig af at kryptere oplysningerne, så de skal afkodes for at kunne tilgås. Her vil det kun være de personer med krypteringsnøglen, der kan få adgang til oplysningerne. Pseudonymisering af oplysningerne nævnes

⁴⁰ Dall, Langebæk og Langemark s. 111

⁴¹ Dall, Langebæk og Langemark s. 125

⁴² Dall, Langebæk og Langemark s. 124

ligeledes som en mulighed. Dette betyder, at oplysningerne opdeles på en måde, så det ikke umiddelbart kan lade sig gøre at identificere den registrerede, heller ikke selvom de samles igen. Er en oplysning pseudonymiseret skal den ikke betragtes som en anonym oplysning, men blot svært tilgængelig. En anonymisering af oplysninger vil naturligvis gøre, at oplysningerne ikke længere er omfattet af Forordningen, da Forordningen omfatter identificerbare oplysninger. Der er flere tiltag i art. 32, der, såfremt de anvendes, kan øge sikkerheden. Disse er at den dataansvarliges IT-system skal være stabilt, at der kan genoprettes adgang efter en hændelse, samt at der findes en procedure til at teste foranstaltningerne. Disse tiltag vil tale for, at den dataansvarlige har overholdt sine forpligtelser i tilfælde af sikkerhedsbrud, men der vil naturligvis altid være en afvejning af omstændighederne i den konkrete situation.

Der er også omstændigheder, der taler for en høj beskyttelse af de behandlede oplysninger i Sundhedsappen. Med dette menes, at der benyttes Cloud-computing, og at der findes mange registrerede. Samtidig indsamler Apple en masse oplysninger i deres produktportefølge, ud over Sundhedsappen. Derfor vil Apple, i en samlet bedømmelse, formentlig aldrig komme udenom, at skulle anvende art.35. Art.35 omhandler netop den situation, hvor den dataansvarlige skal foretage en konsekvensanalyse, der tager højde for teknologi, og muligheder for at analysere den indsamlede data ved et sikkerhedsbrud. Det er her begrebet DPIA kommer ind. En DPIA skal fastsætte de foranstaltninger, den dataansvarlige skal foretage for at imødekomme den trussel en behandling medfører. En udvidet sikkerhedsplan kunne man kalde den. Det er analysen af behandlingens risiko, der skal finde de svageste led i virksomhedens sikkerhedskæde. Dette være sig både fysisk, teknisk, organisatorisk og på andre områder, såfremt det er nødvendigt. I en DPIA skal der indgå en skriftlig og systematisk beskrivelse af, hvorfor man anser det nødvendigt at behandle lige præcis den data der indsamles, især hvis den er følsom.

4.2.4 Anden relevant lovhjemmel

En offentliggørelse af oplysninger, af de registrerede selv, ville forårsage at muligheden for at anvende oplysningerne øges for de dataansvarlige. Omkring emnet offentliggørelse, udtalte Folketingets Ombudsmand "*når man har en så åben profil på Facebook, svarer det til at man hænger oplysningerne op et offentligt sted*"⁴³. Oplysningerne i Sundhedsappen skal derfor ikke opfattes som offentliggjorte, da de ikke er en del af en åben profil. Det er derfor kun den registrerede selv, samt de personer denne vælger at vise dem til, der har adgang til oplysningerne. Det kunne umiddelbart ændre sig, såfremt den registrerede

⁴³ http://www.ombudsmanden.dk/find/udtalelser/beretningssager/alle_bsager/2011-15-1/2011_15-1_pdf-version/

valgte, at trække oplysningerne over i en anden App, men her ville det kræve et nyt samtykke, når denne App skulle benyttes.

Det valgte niveau af datasikkerhed kan også være et spørgsmål om penge. Den dataansvarlige kan af hensyn til omkostninger, vælge et lavere niveau såfremt det bliver uproportionelt dyrt. Det vil være en afvejning af de aktuelle forhold i situationen, hvor tungt dette hensyn må veje. Det vil dog som det klare udgangspunkt ikke være legitimt, at inddrage økonomiske hensyn, men Forordningen lægger alligevel op til at det kan blive det under de rette forudsætninger⁴⁴. Med dette menes der at investeringen er uforholdsmæssig dyr, i forhold til det den skal beskytte og den begrænsede ekstra beskyttelse investeringen påfører.

4.3 Opsummering af Sundhedsappens niveau af sikkerhed

Apples beskyttelse af de indsamlede oplysninger, gør at de lagres lokalt på telefonen, og sendes til iCloud i krypteret udgave. Det er derfor ekstremt usandsynligt, at disse oplysninger, ud fra den risiko de afspejler og ud fra deres begrænsede økonomiske værdi, de ville kunne have for nogen, at de kunne blive offer for hacker-angreb og derigennem afpresning. En hacker ville ikke kunne benytte oplysningerne med mindre han kan klare krypteringen, og hvis han kunne, er det ikke sandsynligt, at oplysningerne har nogen værdi for ham. Dette ville kun være tilfældet, hvis han fik adgang til alle de registreredes oplysninger. Her ville en hacker potentielt kunne true Apple med offentliggørelse. I forhold til de registrerede individuelt, er det ikke aktuelt, at de pågældende oplysninger skulle kunne krænke den enkelte. Heller ikke i en situation, hvor en medarbejder ved en fejl udsender eller offentliggør sådanne oplysninger. Apple har med foranstaltninger omkring, at oplysninger gemmes lokalt på telefonen og sendes til iCloud i en krypteret udgave, allerede inden Forordningens ikrafttræden etableret et højt beskyttelsesniveau for de registrerede. Forordningens krav til datasikkerhed jf. art.32, som er det niveau den pågældende behandling isoleret skal sigte på at opfylde, overholdes derfor af Apple. Da oplysningerne ikke, isoleret, udgør stor fare, vil det være art.32 der er det niveau af sikkerhed, Apple skal overholde.

⁴⁴ Blume(2) s.120

4.4 Juridisk konklusion

Det er bestemt i Forordningen, og kan udledes fra direktivets retspraksis, at de indsamlede oplysninger fra Sundhedsappen, ikke kan karakteriseres som følsomme. Hertil skal der forekomme en udvidelse af begrebet *helbredsmæssige oplysninger*, før dette vil være tilfældet. Eneste potentielle afvigelse fra dette er, at Sundhedsappen indsamler oplysninger om blodtryk, som i tilfælde af, at personen er syg og det kan aflæses, vil være en følsom oplysning. Indtil videre er der dog ikke noget der tyder på, at dette bliver tilfældet, ud over den nævnte afgørelse C-101/01 - Bodil Lindqvist, hvor en kollega nævnte sin kollegas brækkede ben på en hjemmeside. En oplysning om blodtryk vil ikke klart kunne fortælle, at en person er syg. Hertil vil det kræve, at personen der aflæser oplysningen er i stand til, at fortolke oplysningerne på denne måde, samt at oplysningerne rent faktisk stammer fra en syg. Heller ikke udsving i pulsmålinger, distance tilbagelagt osv., burde være oplysninger der hører til indenfor definitionen af helbredsmæssige oplysninger.

Om Apple overholder samtykkereglerne i Forordningen, vil komme an på om de krav der stilles til hvordan den registrerede informeres, som fremgår af samtykketeksten. Vedrørende art.7, stk.1-4 burde her ikke være nogen grund til, at tro dette vil volde Apple vanskeligheder. I art.4, nr.11 hvor samtykket specificeres til at være en *Frivillig, specifik, informeret og utvetydig tilkendegivelse af vilje*, findes der heller ikke nogen grund til, at Apple skal ændre deres nuværende fremgangsmetode, da denne allerede nu overholder kravene i Forordningen.

Vedrørende overholdelse af princippet om gennemsigtighed, finde der nogle små kritikpunkter, som formentlig aldrig ville føre til en dom, om at Apple ikke overholder princippet. Det mest relevante, er at analysere hvad Apple faktisk benytter de behandlede oplysninger til. Anonymitetspolitikken giver anledning til, at den oplysningerne benyttes til formål der rækker langt ud over hvad er nævnes i samtykketeksten. Dette bliver først relevant, i det moment, at Apple anvender oplysningerne til formål der rækker ud over det i samtykketeksten. Apple har kun lov til, at behandle de indsamlede oplysninger ud fra formålet om at forbedre fitness funktionerne, som samtykketeksten giver dem lov til. Foregår en behandling ud over dette formål er den ikke gyldig. Det der taler for at Apple behandler oplysningerne til formål ud over dette, er at det står i deres anonymitetspolitik. Det der taler imod at de behandler disse oplysninger til andre formål, er at anonymitetspolitikken er generel for alle deres tjenester. Samtykketeksten er ikke generel men derimod specifik, da den kun vedrør Sundhedsappen. En omstændighed der ligeledes taler imod, at Apple anvender oplysningerne til andre formål end det i samtykketeksten, er at Apple ønsker at samarbejde med andre firmaer om, at de kan udvikle deres egne Apps, som kan modtage oplysninger fra Sundhedsappen. Deres

økonomiske formål, er derfor ikke at anvende oplysningerne selv, men derimod at andre kan modtage oplysningerne. Udveksles oplysningerne, vil det juridiske forhold omkring samtykke osv., være et formål mellem denne App-udvikler og ikke Apple.

Anderledes forholder det sig omkring Oplysningspligten jf. Forordningens art.13. Oplysningspligten har adskillige mangler, før det vil være i overensstemmelse med Forordningen. Der mangler at oplyses hjemmel for behandling, om modtageren kan opdeles i kategorier(hvilket om nogle af datterselskaberne modtager oplysninger), om oplysningerne kan tilgås af nogen udenfor EØS samarbejdet, om hvilket tidsrum oplysningerne gemmes, at den registrerede kan bede om at oplysningerne rettes og begrænset, samt hvilken myndighed der afgør retlige tvister. Alt dette mangler for at oplysningspligten i art.13 er overholdt.

En konsekvensanalyse af de behandlede oplysninger, ville ikke føre til, at Apple med Sundhedsappen, skulle have et højere niveau end det der kræves jf. art.32. De specifikke oplysninger udgør ikke en ligefrem fare, og der skal mange sammentræf til i form af uheld og hackerangreb, før at disse oplysninger ville kunne komme til, at krænke den registrerede. I forhold til den beskyttelse der ydes for at beskytte oplysningerne, er det usandsynligt, at dette vil kunne forekomme. Dette vil kun være tilfældet, såfremt Apples øvrige produktportefølge ikke indgår i bedømmelsen.

5. Forordningens sanktionsramme

I det følgende præsenteres de relevante dele af Forordningens sanktioner for denne afhandling. Mulighederne for, at pålægge sanktioner skal primært findes i muligheden for at pålægge administrative bøder, men også andre tiltag gennemgås. De andre tiltag er de korrigerende beføjelser, anden straf, samt erstatningsansvar. Netop de administrative bøder anses, som årsag til den store medieomtale omkring Forordningens ikrafttrædelse. Det er primært disse der ligger til grund for virksomhedens beslutningsgrundlag omkring non-compliance. Derfor skrives denne del, med særligt fokus på netop dette område.

5.1. Administrative bøder jf. Forordningens art.83

De administrative bøder skal, som sanktionerne i det hele taget, repræsentere et rimeligt niveau i forhold til overtrædelsen. De skal have en afskrækkende effekt, og være effektive i forhold til, at nå deres mål. Det er forventet at de største bøder ikke kommer til at falde indenfor den første rum tid, og der vil muligvis gå mange år før vi ser rammen for udskrivelse af de administrative bøder, blive anvendt til fulde.

Muligheden for at sanktionere med administrative bøder skal findes i Forordningens art.83:

Administrativ Bøde op til EURO 10 mio./eller bøde op til 2 % af forrige års omsætning⁴⁵:

Forseelse der vedrører:

- Samtykke fra værge ift. børn
- Privacy by design/default principperne
- Repræsentanter
- Krav til databehandlere, samt databehandleraftaler
- Samarbejde med tilsynsmyndigheden
- Persondatasikkerhed, anmeldelse af sikkerhedsbrug og regler vedrørende DPIA
- Certificeringsordninger
- Kontrol eller certificeringsorganers forpligtelser

⁴⁵ Dall, Langemark og Langebæk - s.138

Administrativ bøde op til 20 mio./eller bøde op til 4 % af forrige års omsætning⁴⁶:

Forseelse der vedrører:

- De grundlæggende behandlingsprincipper
- Samtykkereglerne
- Rettighederne for de registrerede
- Overførsel af data til tredjelande
- De nationale særbehandlingsregler
- Manglende efterlevelse af påbud fra Datatilsynet

Der arbejdes med et forholdsvis simpelt system, eftersom de administrative bøder lægger i størrelsesorden 2 %/ 10 Mio. Euro, eller 4 %/20 Mio. Euro, af virksomhedens forrige årsomsætning. Det er her værd at bemærke, at manglende opfyldelse af samtykkereglerne, potentielt kan udløse en bøde på 4 % af virksomhedens forrige årsomsætning, og er derfor blandt de forseelser der straffes hårdest indenfor bøderammen. I bedømmelsen om straffens størrelse skal der tages stilling til hvilken af de muligheder der er mest passende i forhold til forseelsen⁴⁷. Samtidig er det værd, at bemærke at art.83, stk.5-6, hjemler at såfremt der anvendes en procentdel af virksomhedens sidste årsomsætning som bodegrundlag, er det på grund af at dette beløb er højest af de to muligheder. Med muligheden for at straffe i en beløbsstørrelse, har man desuden formået at imødekomme problemstillingen hvor en nystartet virksomhed uden nævneværdig omsætning i det forrige år, ikke kan pålægges en passende sanktionsmulighed.

Et meget væsentligt aspekt af de administrative bøder, er at man har valgt at udskrive bøder efter samme fremgangsmetode, som indenfor konkurrenceretten⁴⁸. I praksis betyder dette, at hele virksomhedens organisation kommer til at indgå i bødestørrelsen, dvs. der er tale om den globale concerns omsætning i det forrige år. Der er derfor lagt op til muligheden for at pålægge administrative bøder i astronomisk størrelse, såfremt nogle af de store virksomheder ikke prioriterer overholdelse af Forordningens regler.

I Forordningens art.83, stk.3 omtales også muligheden for, at udskrive kumulative administrative bøder. Kumulative administrative bøder ville være, at en virksomhed straffes med forskellige bøder, og bødernes værdi, kan lægges oveni hinanden. Dette ville potentielt kunne den samlede bødestørrelse, en virksomhed skulle betale på årsbasis, for ikke at overholde regelsættet, gøres endnu højere. Såfremt en dataansvarlig,

⁴⁶ Dall, Langemark og Langebæk s.138

⁴⁷ Dall, Langemark og Langebæk s.138

⁴⁸ Dall, Langemark og Langebæk s.138

enten uagtsomt eller endda forsætligt, overtræder flere af Forordningens regler, udskrives, som udgangspunkt, ikke administrative bøder for de forskellige forhold. Udgangspunktet er derfor, at der straffes for den mest alvorlige forseelse, med den højest mulige bøde, for alle virksomhedens overtrædelser. Dette gælder endda såfremt overtrædelsen er forsætlig. Rækkeviden af dette gælder dog ikke uforbeholdent. I art.83, stk.3 nævnes der et forbehold for, at der kan udskrives kumulative bøder. Dette kan lade sig gøre såfremt der ikke er tale om de samme, eller forbundne behandlingsaktiviteter. Dermed må det være muligt, under forudsætning af, at behandlingsaktiviteterne er adskilt, at udskrive bøder for forskellige forhold, som dermed lægges oveni hinanden. Dette aspekt er især interessant såfremt virksomheden er en koncern. Dermed er muligheden holdt åben, for at pålægge kumulative bøder til de store selskaber, såfremt deres adskilte behandlingsaktiviteter hver især ikke overholder Forordningens regler.

5.2 Korrigerende beføjelser art.58, stk.2

De korrigerende beføjelser er blandt de muligheder Datatilsynet har for, at få de dataansvarlige til at ændre adfærd. De kan med denne type af beføjelser, forsøge at stoppe en ellers ulovlig behandling, uden at gå så langt, som at benytte administrative bøder. Der kan udskrives advarsler mod ellers planlagt behandling, fordi denne med stor sandsynlighed ikke vil stemme overens med Forordningens regler. De kan ligeledes udtale sig kritisk om en allerede foregået behandling, såfremt denne behandling ikke stemmer overens med Forordningen⁴⁹.

De korrigerende beføjelser giver desuden Datatilsynet ret til, at udskrive påbud i forskellige situationer. De kan udskrive påbud, mod en behandling og bede om at behandlingen korrigeres så den stemmer overens med Forordningen. De kan kræve, at de registrerede informeres om forhold der vedrører deres behandling af persondata. Der findes desuden muligheden for at kræve en bestemt behandling stoppet, samt at bede om sletning af indsamlet data, eller at en behandling begrænses af de dataansvarlige. De korrigerende beføjelser må anses som den sidste mulighed for de dataansvarlige, inden der udskrives administrative bøder⁵⁰.

⁴⁹ Dall, Langemark og Langebæk s.136

⁵⁰ Dall, Langemark og Langebæk s.136

5.3 Frihedsberøvelse eller anden straf jf. art.84

En regulær frihedsberøvelse indgår ikke i Forordningens lovtekst. Bedømt ud fra ordlyden i art.84, må det alligevel antages, at dette er en mulighed. Dette skyldtes, at der nævnes muligheden for at fastsætte andre sanktioner⁵¹. Det bliver interessant at følge hvilken grad af forseelser, der udløser anvendelse af art.84. En straf af denne karakter vil kun komme på tale, så længe det ikke er muligt at finde lovhjemmel til at udskrive administrativ bøde⁵². Skulle et så alvorligt brud på persondatasikkerheden forekomme, at en fængselsstraf ville være den passende straf, vil dette skulle varetages af de nationale domstole. Funktionen af art.84 er derfor stadig uvis, og om en frihedstraf for brud på Persondataforordningen, i det hele taget kommer til at indgå i sanktionsrammen. Muligheden er dog med art.84 holdt åben, som mulighed for de værste overtrædelser.

En anden mulighed af denne artikel, kunne også være at man ville pålægge straf i anden form, som ikke nødvendigvis er en direkte økonomisk sanktion. Af muligheder kan nævnes frakendelse af ret til, at drive virksomhed i periode, eller samfundstjeneste. Funktionen med artiklen kunne, også være at forhindre den situation hvor et selskab lukker efter, at have brudt reglerne, for derefter at lade selskabet hæfte for bøden.

5.4 Erstatningsansvar jf. art.82⁵³

Reglerne for erstatning minder om de danske erstatningsregler. Forordningen giver mulighed for, at placere et erstatningsretligt ansvar på virksomheden. Den der har lidt tab kan kræve erstatning fra den dataansvarlige eller behandlere. Den dataansvarlige eller evt. behandler skal bevise sin uskyld, og der gælder derfor omvendt bevisbyrde. Det interessante ved deres kommende virke, er om vi kommer til at se brud på reglerne der medfører søgsmål fra en større gruppe af mennesker, dvs. gruppesøgsmål.

⁵¹ Forordningen art.84, samt Blume(1) s.135

⁵² Blume (1) s. 135

⁵³ Dall, Langemark og Langebæk s.139-140

6. Økonomisk non-compliance af Forordningens samtykkeregler

I en af de første timer til faget Ret og Kontraktret, 1.semester cand.merc.jur efteråret 2016, blev det økonomiske syn omtalt. Årsagen var en diskussion omkring virksomhedens forpligtelser til sin omverden, i forbindelse med kontraktbrud⁵⁴. Grundlæggende går et økonomisk syn ud på, at virksomheden prioriterer sine forpligtelser overfor omverdenen i forhold til, hvad der bedst kan betale sig økonomisk. Virksomheder som overvejer non-compliance i forhold til loven, må antages at have en høj præference for profitoptimering, Men virksomhedens rationale kan også være andet og mere end profitoptimering. Det vil afhænge af den individuelle aktør.

Denne del af afhandlingen omhandler de valgmuligheder virksomheder har omkring overholdelse af regler. Der tages her udgangspunkt i den samme forseelse, set fra Apple som en stor virksomhed og set fra en hypotetisk mindre virksomhed. Grundlæggende er der væsentlige forskelle på det økonomisk optimale valg for de to virksomheder. Dette gælder internt i organisationerne, hvor kompetencen er forskellig og mere spredt end i de små virksomheder, men også eksterne påvirkninger i form af bødestørrelse og bevågenhed spiller en rolle i forhold til vurderingens resultat. I begge tilfælde gælder den grundlæggende antagelse, at der ikke foretages nogen overvejelser omkring non-compliance, såfremt der er stor chance for opdagelse og beskedent udbytte. En vigtig pointe er, at der ikke svares på spørgsmålet, om Apple eller den hypotetiske mindre virksomhed bør vælge at bryde regler, men udelukkende om det er økonomisk **optimalt**, såfremt dette valg foretages.

En endelig beslutning om at overtræde en given regel vil kræve et indgående kendskab til de forskellige værdier i modellen, der anvendes til at analysere beslutningen. De forskellige værdier består af g (gain), p (chancen for opdagelse i procent), f (bødestørrelse) og $t \times \lambda$ (nytteværdi $\times$ antal). For at finde det mest korrekte resultat ud fra omstændighederne, er det nødvendigt at opdele nogle af værdierne og foretage deludregninger separat. Der redegøres for dette, samt for hvilken påvirkning dette har på resultatet.

Om skadegørende handling

Der tages udgangspunkt i Apple samt en hypotetisk mindre virksomhed med en årlig omsætning på 5 mio. kr. Begge virksomheder anvender sundhedsdata, og forseelsen tager udgangspunkt i behandling af denne type af oplysninger. Den valgte forseelse er overtrædelse af Forordningens regler om samtykke kombineret

⁵⁴ Ret og Kontraktret 17.oktober (Tema: Moral og efficiens)

med et brud på princippet om gennemsigtighed. Den hypotetiske overtrædelse er følgende. Virksomheden undlader bevidst at oplyse de registrerede om, at de indsamlede oplysninger videregives til højest bydende eksterne købere af data. Skadegørende handling vil i eksemplet betyde, at handlingen er skadelig for befolkningens tiltro til det digitale domæne. En direkte personlig skade for de registrerede og efterfølgende erstatningskrav er ikke omfattet af den skadegørende handling.

Alle udregninger, både positive og negative, foretages på baggrund af en årlig besparelse/indtægt. Dette skyldes, at de administrative bøder udregnes på årsbasis. Der er derfor tale om årlig omsætning/omkostning, chance for at blive opdaget pr. år, årlig besparelse i compliance pr. år etc.

6.1 Apples økonomiske forhold til compliance med samtykkereglerne

Det må antages at Apple, som en af verdens største virksomheder, har store fordele i form af specialiseret kompetence indenfor mange forskellige områder. Denne kompetence gør, at virksomheden har færre transaktionsomkostninger end mindre virksomheder, da de selv har ekspertise og viden, som de ikke behøver hyre udefrakommende konsulenter til at løse. Det negative ved at være en virksomhed i denne størrelsesorden er den store bevågenhed, samt bødens størrelse, der vil tage udgangspunkt i den globale omsætning.

Det forudsættes, at Apple kun kan overtræde reglerne med en isoleret handling. Årsagen til denne antagelse er, at Apple kan få mange separate bøder, såfremt de overtræder Forordningen ved forskellige adskilte behandlinger jf. art. 83, stk. 3. Apple kan derfor ikke undlade at investere i compliance, eftersom de kan risikere at straffes for kumulative forseelser. De har kun muligheden for, isoleret, at opnå indtægt på enkeltstående forseelser og samtidig kun opnå besparelse direkte lokaliseret til denne behandling.

6.1.1 Apples skadegørende handling (gain)

I den valgte model ligger udgifter til compliance implicit i værdien af den skadegørende handling, eftersom modellen ikke har et separat element der indregner compliance. Derfor adskilles udgifter til compliance og gøres til genstand for en separat udregning. Årsagen til denne fremgangsmetode er, at der er tale om en besparelse på ellers afholdte udgifter, og besparelsen skal derfor ses som en positiv påvirkning.

Den forventede værdi af skadegørende handling kan derfor udtrykkes:

Gain(g):

Omsætning ved at foretage skadegørende handling + Besparelse i ellers afholdte udgifter til compliance
– **Omsætning ved at lade være med at foretage skadegørende handling**

Generelt kan det være svært at vurdere potentielle handlingers indflydelse på omsætningen præcist, og vil kræve transaktionsomkostninger, enten i form af konsulenthonorar eller lign. Omkostningerne til compliance kan samtidig være høje og placeret blandt mange forskellige medarbejdere på tværs af afdelinger. Transaktionsomkostninger kan være svært målbare, grundet placering i små udsving i produktivitet, på et stort antal medarbejdere. Her vil det være ønskeligt, at kunne foretage sammenligninger med tidligere perioder, hvor der ikke forelå den samme forpligtelse. Det antages, at Apple i kraft af deres størrelse har særdeles gode muligheder for og kompetencer til at foretage denne udregning med minimale transaktionsomkostninger.

De korrigerende beføjelser i Forordningen gør, at der er lagt op til, at virksomheder der opdages i at have overtrådt Forordningen ikke omgående straffes med store bøder. Det vil derfor være i virksomhedens interesse at undersøge, hvor grænsen ligger. Virksomheden forudsættes derfor at udregne den investering i datasikkerhed der er økonomisk optimal, uden at der uddes bøde.

Den optimale udgift til compliance:

Udgift til compliance, der påvirker den forventede værdi, indtil det punkt hvor den forventede værdi af at investere yderligere i compliance bliver negativ. Det skal derfor opfattes som den investering, der nedbringer risikoen til det niveau, hvor det ikke kan betale sig at foretage yderligere investeringer i datasikkerhed. Dette fjerner ikke hele risikoen, da der ellers vil være tale om at virksomheden overholder loven.

6.1.1.1 Værdi af skadegørende handling

Det antages, at Apples skadegørende handling har værdien **100 mio. kr.** Ingen transaktionsomkostninger påregnes, da Apple ikke er afhængige af konsulenter for at udregne den præcise værdi.

6.1.1.2 Værdi af besparelse til compliance

Det antages, at Apple kan spare en halv medarbejder med månedsløn på 30.000 kr = 30.000 kr x 12/2
= **180.000 kr./pr.år**, ved kun at investere i den optimale udgift til compliance. Apples udgift til compliance er dermed halveret og udgør **180.000 kr./pr.år**.

6.1.2 Den procentvise chance for at blive opdaget(p)

Chancen for opdagelse er forskellig fra handling til handling. Grundlæggende influeres chancen for at den skadegørende handling opdages af to væsentlige faktorer: Handlingens karakter samt den eksponering handlingen har.

Et væsentligt element om anvendelse af sanktionsrammen er, at reglerne modtages af rettighedssubjekterne. I litteraturen kritiseres Forordningens tekst kraftigt af Peter Blume. Kritikken bygger på, at Forordningens tekst ikke formår at informere dets budskab til dem, der skal forstå den. Et svært forståeligt regelsæt henvendt mod en befolkningsgruppe med svages forudsætninger for at forstå dets indhold taler for, at chancen for opdagelse formindskes⁵⁵. Samtidig indeholder forholdet mellem den registrerede og den dataansvarlige i mange tilfælde ikke noget økonomisk mellemværende. Dette må også antages at formindske den registreredes incitament til at gøre opmærksom på, at hans rettigheder er overtrådt. Der er dog andre faktorer der taler for høj anvendelse af sanktionsrammen. Dette er, at det ikke er påkrævet, at alle de registrerede skal forstå, at reglerne er brudt, men derimod kun en enkelt eller nogle få. Muligheden for juridisk bistand er desuden gjort let tilgængelig, eftersom Datatilsynet bistår de registrerede med vejledning.

Det antages, at Apple har stor viden om chancen for opdagelse, da de grundet erfaring og kompetence, kan udregne dette præcist. Ingen transaktionsomkostninger påregnes.

Chancen for opdagelse på en given handling udregnes på årsbasis. Som stor virksomhed har Apple mange forskellige databehandlinger. For at mindske chancen for opdagelse kan virksomheden på årsbasis, rotere mellem hvilke af sine behandlinger der holder loven. Dette kan den mindre virksomhed ikke gøre, med mindre den har flere behandlinger at vælge imellem.

6.1.2.1 Værdi af chance for opdagelse

Chancen for at Apples forseelse opdages og retsforfølges indenfor en periode på et år vurderes til **20 %**.

⁵⁵ Blume(1) s.130 chancen for opdagelse

6.1.3 Bødens størrelse(f) – direkte omkostninger

Det er ikke kun administrativ bøde der skal betales indenfor kategorien af direkte omkostninger.

Sagsomkostninger og erstatning kan også blive aktuelt alt afhængig af forseelsens karakter og Apples villighed til at betale.

Dermed bliver den endelige udregning af de direkte omkostninger:

Bøde + (gennemsnit erstatning x antal af skadelidte) + juridisk bistand

Den administrative bødestørrelse ligger som udgangspunkt fast på de 4 % af sidste års omsætning. Dette skyldes, at dette beløb er væsentlig højere end de 20 mio. Euro og er dermed det beløb, der skal gælde jf. Forordningens art.83. Apple omsatte i 2017, for 229,23 milliarder dollars⁵⁶, eller 1.375 billion omregnet til Danske Kroner. En administrativ bøde til Apple kan derfor potentielt blive i størrelsen omkring 55 mia. kr. Der er hermed tale om en potentielt verdensrekord for højeste bøde uddelt, kun sammenlignelig med Googles overtrædelse af konkurrencereglerne, der udløste bøde på omkring 30 mia. kr.⁵⁷.

Erstatning kan blive aktuelt, såfremt Apple har forårsaget et økonomisk og dokumenteret tab hos en af de registrerede. En sag om erstatning vil kræve, at Apple har foretaget en handling, hvor de registrerede har et direkte økonomisk forhold til den dataansvarlige. Dette vil medføre, at chancen for opdagelse stiger væsentligt. Det antages, at Apple aldrig overvejer handlinger hvor chancen for opdagelse er stor, og dette vil være tilfældet såfremt de registrerede har direkte økonomisk forhold til forseelsen. Erstatning er derfor ikke relevant at medregne, da den valgte forseelse ikke tager udgangspunkt i, en forseelse der kan medføre dette resultat.

Den juridiske bistand vil her være at opfatte som en transaktionsomkostning. Den vil variere fra sag til sag, men vil være højest i de tilfælde, hvor virksomheden ikke accepterer den forelagte bøde og derfor skal igennem en retssag. Der tages ikke hensyn til, at afholdelse denne omkostning kan medføre frifindelse. Derimod forudsættes det, at dette beløb er den gennemsnitlige udgift, Apple afholder pr. sag i forbindelse med lignende sager.

⁵⁶ <https://www.statista.com/statistics/265125/total-net-sales-of-apple-since-2004/>

⁵⁷ <https://www.aljazeera.com/news/2018/07/eu-hits-google-5bn-fine-breaking-competition-rules-180718091255980.html>

6.1.3.1 Værdi af administrativ bøde

Administrativ bøde på 4 % af virksomhedens globale omsætning = **55 mia kr.**

6.1.3.2 Værdi af juridisk bistand

Det antages, at Apple vil køre sagen, samt at de på forhånd kan kalkulere med denne omkostning præcist, evt. gennem fast aftale med advokat. Der kalkuleres med en udgift på **500.000 kr.**

6.1.4 Anden straf – indirekte omkostninger ($t \times \lambda$)

I det følgende gennemgås muligheden for anden straf end administrativ bøde. Ifølge Peter Blume kan dette bestå i den teoretiske mulighed for fængselsstraf, men bedømt ud fra ordlyden i art.84, kan andre muligheder som frakendelse af ret til at drive virksomhed, og samfundstjeneste ligeledes være en mulighed. Kun fængselsstraf gennemgås som teoretisk mulighed. En basis for udregning af værdien af dette kan findes i udtrykket:

Samlet værdi af anden straf kan derfor udtrykkes: Tabt nytteværdi af fængselsstraf pr.måned x straffens længde i måneder

Frihedsberøvelse vil blive vurderet meget forskelligt af aktøren, alt afhængig om denne er risiko neutral, eller risiko avers. Den risiko-neutrale ville vurdere den tabte nytteværdi, proportionelt med den tid, han skal spendere i fængsel. Des længere straf jo højere vægtes den tabte nytteværdi proportionelt. Er afsoningen f.eks. 10 måneder, vil han vurdere alle 10 måneder individuelt til at have den samme tabte nytteværdi. Den risiko-averse ville af forskellige årsager ikke vurdere fængselsopholdet proportionelt med længden af afsoningen. Denne ville uproportionelt vurdere de sidste måneder af en lang fængselsstraf, højere end de første, eller omvendt. Dette kunne være tilfældet hvor en person sagtens kan spendere en måned i fængsel, men under ingen omstændigheder vil acceptere et år.

I forhold til den overtrædelse Apple foretager af Forordningens regler, som lægges til grund for denne analyse, må en straf i form af frihedsberøvelse kun anses som en teoretisk mulighed, og dette uddybes ikke yderligere i afhandlingen.

6.1.5 Dårlig omtale

Dårlig omtale passer ikke direkte ind i non-compliance modellen, men vil generelt være at opfatte som en indirekte omkostning⁵⁸. En værdi af dårlig omtale må være næsten umulig at værdifastsætte præcist. På

⁵⁸ <https://securekey.com/blog/bad-reputation-the-indirect-costs-of-data-breaches/>

trods af dette antages det, at Apple på forhånd kan udregne et estimeret omfang af værdien af den negative omtale.

Dårlig omtale omtales i Østergaard & Motzfeldt⁵⁹, hvor den beskrives som værende kortvarig og uden stor betydning i forbindelse med overtrædelser af PDL. Dette vil formentlig i mange tilfælde være korrekt, endda også ved overtrædelser af GDPR. Samtidig må det være givet, at store velkendte virksomheder på størrelse med Apple, vil live mødt med massiv medieomtale ved offentliggørelse af, at virksomheden, bevidst har undladt at overholde regelsættet.

6.1.5.1 Værdi af dårlig omtale

Det antages, at værdien af at negativ omtale for Apple, som følge af et bevidst brud på Forordningen opdaget og dokumenteres, udgør **10 mio. kr.**

6.1.6 Udregning af Apples økonomiske forhold til non-compliance af samtykkereglerne

Non-compliance modellen, hvor det findes økonomisk optimalt, såfremt $g > p(f + (t \times \lambda))$, anvendes som udgangspunkt for at udregne om det er økonomisk optimalt ikke at overholde regler. Da det ikke findes relevant at inddrage indirekte omkostninger i form af anden straf, udgår sætningen $(t \times \lambda)$, men der indsættes tabt værdi som følge af negativ omtale. Derfor bliver udregningen følgende:

Forventet værdi af skadegørende handling:

+ Den opnåede værdi skadegørende handling(gain) + besparelse i udgifter til compliance
– Chance for opdagelse og retsforfølgelse målt i procent(p) x (bødens størrelse(f) + omkostninger forbundet med negativ omtale) + omkostninger ved at investere i den optimale udgift til compliance

Dermed kan den forventede værdi af Apples manglede overholdelse af samtykkereglerne udregnes:

Forventet værdi af Apples non-compliance af samtykkereglerne

100 mio. kr + 180.000 kr. > 0,2 x (55 mia. kr. + 500.000 kr. + 10 mio. kr.) + 180.000 kr.

100 mio kr. > 0,2 x (55.010.500.000,00 x 0,2)

⁵⁹ Østergaard & Motzfeldt s.6

= 100.000.000 mio. kr. > 11.010.100.000 kr.

Den forventede værdi er negativ eftersom 100 mio. kr. naturligvis er væsentlig lavere end 11 mia. kr. Dette er naturligvis forudsat at chancen for opdagelse er på 20 %. Det skulle derfor være højst usandsynligt, at Apple nogensinde vil træffe en bevidst beslutning om ikke at overholde Forordningens regler vedrørende samtykke ud fra et rationalt om, at dette er det økonomisk optimale valg. For at dette skulle være økonomisk optimalt, vil det kræve, at chancen for opdagelse og retsforfølgelse reduceres til ca. 0,4%, hvor den risikoneutrale aktør ville være indifferent overfor valg om compliance, da de to værdier er lige høje. Omvendt skulle Apple derimod have en mulighed for at indtjene denne værdi i forhold til den skadegørende handlings værdi, ville det ud fra de givne forudsætninger kræve, at værdien er 110 gange så høj, som den der anvendes i eksemplet. Dette ville være en overtrædelse hvor værdien i g = 11 mia. kr, før at den risikoneutrale aktør ville være indifferent overfor valget om compliance.

6.2 Mindre virksomheders økonomiske forhold til compliance af samtykkereglerne

Hvor en virksomhed på størrelse med Apple, antageligt, med lethed kan betale en bøde i astronomisk størrelse, forholder det sig anderledes med de mindre virksomheder. Her kan en bøde være direkte årsag til at virksomheden må lukke. Virksomheden kan på baggrund af truslen om administrativ bøde være tvunget til at lade budgettet indeholde udgifter til overholdelse af regelsættet.

Det antages i dette eksempel, at såfremt virksomheden overvejer non-compliance af Forordningens regler, skal den kende til den potentielle værdi, overtrædelsen vil indbringe. Ellers vil den som udgangspunkt ikke gøre det. I praksis kan dette være forkert, eftersom en mindre virksomhed uden stort overskud potentielt kan være tvunget til non-compliance. Dette vil være tilfældet, såfremt virksomheden ikke har råd til at efterleve de krav Forordningen stiller om datasikkerhed, og den viden den skal besidde om Persondataforordningen generelt.

De grundlæggende mekanismer i non-compliance modellen er ens uanset virksomhedens størrelse. Denne del gennemgår kun de mest relevante forskelle, som skal findes i virksomhedens interne og eksterne forhold. Da der er tale om den samme overtrædelse, udgår de samme elementer som i forrige afsnit (6.1).

6.2.1 Skadegørende handling(gain) foretaget af mindre virksomhed

En mindre virksomhed har ikke samme forudsætninger som store, for at vurdere en skadegørende handlingens værdi. Skulle den have dette, ville det være fordi den kan sammenligne med tidligere periode, uden forpligtelse til at overholde Forordningen. Det antages i eksemplet, at der foreligger transaktionsomkostninger i form af konsulenthonorar, for at fremskaffe denne viden.

Virksomheden forudsættes, let at kunne lokalisere udgifter til compliance. Dette foretages af en enkelt medarbejder, evt. som en del af dennes stilling. Dennes løn kan dermed spares.

Virksomheden benytter princippet omkring den optimale udgift til compliance, og investerer mindst muligt for at nedbringe chancen for opdagelse til minimum. Besparelse i udgifter til compliance vil i virksomheden foregå ved, at en medarbejder omprioriterer sine arbejdsopgaver. Det er her muligt for virksomheden, præcist at fastslå hvor meget besparelsen udgør.

Den samlede indtægt på den skadegørende handling kan udtrykkes:

Gain(g):

Omsætning ved ikke at foretage skadegørende handling + Besparelse i udgifter til compliance

– Omsætning ved at lade være med at foretage skadegørende handling

6.2.1.1 Værdi af skadegørende handling

Skadegørende handlingens værdi fastsættes til 500.000 kr. Honorar til konsulent på 10 timer x 1.800 kr/t = **18.000 kr.** påregnes i transaktionsomkostninger.

6.2.1.2 Værdi af besparelse til compliance

Princippet omkring den optimale udgift til compliance anvendes, hvorfor udgift til compliance herefter anslås til at være **150.000 kr.** Det antages, at virksomheden frigiver ressourcer til værdi af **150.000 kr.** ved ikke længere at prioritere overholdelse af reglerne.

6.2.2 Chancen for at blive opdaget i procent (p)

Virksomheden antages at anvende den optimale udgift til compliance, er næsten usynlig i medierne, og antallet af registrerede er under 50.000. Det antages, at virksomheden ikke selv ved, hvor høj den reelle procentsats er, og der vil foreligge transaktionsomkostninger i forbindelse med at udregne den præcise sats evt. i form af honorar til konsulent.

6.2.2.1 Værdi af chancen for at blive opdaget

Det antages at chancen for opdagelse og retsforfølgelse udgør **5 %**. Honorar til konsulent på 10 timer x 1.800 kr/t = **18.000 kr.** påregnes i transaktionsomkostninger.

6.2.3 Bødens størrelse(f)

Bødeniveauet ligger, modsat tilfældet med Apple, ikke fast. Det er ikke muligt at fastslå den konkrete bødestørrelse, eftersom der skal straffes med bøde op til 20 mio. Euro, og de 4 % af virksomhedens sidste årsomsætning anvendes her som udgangspunkt.

6.2.3.1 Værdi af administrativ bøde – direkte omkostninger

Under forudsætning af at virksomhedens sidste årsomsætning var 5 mio. kr., vil den administrative bøde være: $0,04 \times 5 \text{ mio. kr.} = \mathbf{200.000 \text{ kr.}}$

6.2.4 Dårlig omtale af mindre virksomheder

Modsat Apple er den hypotetiske virksomhed ikke synlig i medierne. En potentiel økonomisk skade som følge af dårlig omtale forudsættes derfor at være kortvarig og uden betydning. Virksomheden forudsættes ikke at kunne udregne den præcise værdi, men benytter ikke udefrakommende ekspertise for at udregne dette. Værdien af dårlig omtale udgår fra beregningen.

6.2.5 Udregning af mindre virksomheds økonomiske compliance af samtykkereglerne

Da der benyttes samme fremgangsmetode som i forrige eksempel med Apple, blot fratrasket værdi af dårlig omtale, bliver udregningen således.

Forventet værdi af skadegørende handling:

+ Den opnåede værdi skadegørende handling(gain) + besparelse i udgifter til compliance
– Chance for opdagelse og retsforfølgelse målt i procent(p) x (bødens størrelse(f) + omkostninger ved at investere i den optimale udgift til compliance.

$500.000 \text{ kr.} + 150.000 \text{ kr.} > (0,05 \times 200.000 \text{ kr.}) + 150.000 \text{ kr.} + 18.000 \text{ kr.} + 18.000 \text{ kr.}$

$500.000 \text{ kr.} > 46.000 \text{ kr.}$

Den forventede værdi er her positiv under antagelse af at den procentvise chance for opdagelse er 5 procent/år. Det forholder sig derfor væsentligt anderledes end i forrige eksempel med Apple. Det vil

således være økonomisk optimalt ikke at overholde Forordningens regler under de valgte antagelser. Bemærkelsesværdigt er, at 36.000 kr. af de forventede omkostninger udgør konsulentonorar. Der er hermed tale om en udgift virksomheden kan spare året efter, såfremt den fortsætter med ikke at overholde reglerne.

Den forventede værdi af den administrative bøde udgør 10.000 kr. Såfremt denne sats sættes til 100 %, og virksomheden åbenlyst vælger ikke at overholde reglerne, vil det stadig være økonomisk optimalt under de valgte forudsætninger. Det største spørgsmålstegn må stilles ved, om virksomheden har muligheden for at tjene 500.000 kr. ved ikke at lade en behandlingsform overholde reglerne.

6.3 Kritik af den praktiske anvendelse af modellen – Problem of valuation⁶⁰

En direkte anvendelighed af økonomiske modeller er ikke formålet, og heller ikke med den model der inddrages i denne del af afhandlingen. Formålet er derimod at diskutere den påvirkning af adfærd, som omstændighederne forårsager. I denne del af afhandlingen er formålet, at fokusere på de økonomiske rammer reglerne giver, og den adfærd virksomhederne efterlever som konsekvens deraf.

En direkte anvendelse af modellen har to generelle udfordringer. Den er baseret på antagelser af generelle forhold og vurderinger omkring størrelser af forskellige værdier. Des mere præcise de valgte antagelser forsøger at være, des større chance vil de have for være forkerte samt at formidle overbevisninger fra den der foretager analysen. For at imødekomme dette begrundes de valgte antagelser grundigt, men endnu vigtigere, sættes de i perspektiv. Med dette menes, at der inddrages konsekvenser af, at antagelserne er på et andet niveau. Dette kunne f.eks. være antagelsen om, at chancen for at Apple opdages er højere end ved mindre virksomheder, hvorfor der redegøres for et andet niveau end dette, samt hvilke konsekvenser et andet niveau vil have for resultatet.

Den anden generelle udfordring for en praktisk anvendelse af modellen er, at aktører foretager vurderinger baseret på subjektive holdninger. Dette gælder både for indtægter og udgifter. Vurderinger er især problematiske, når de ikke omhandler en standardiseret vare eller ydelse. En generel tendens er, at tabere overspiller deres tab, og vindere underspiller deres gevinst⁶¹, samt at vurderinger bærer præg af personlige

⁶⁰ Polinsky s.164-166

⁶¹ Polinsky s.164

forhold hos den enkelte. Forhold hos den enkelte, der kan påvirke vurderinger er den såkaldte "wealth factor", som forårsager, at den enkeltes personlige forhold, økonomi og præferencer influerer den værdi, den pågældende sætter på en given skade eller gevinst. Et eksempel anvendt af Polinsky kan opstilles til at beskrive relevansen af dette⁶². Eksemplet tager udgangspunkt i en person, der er følsom overfor lyd og bor til leje i en opgang, hvor naboen støjer. Hans personlige formue kunne være 50.000 kr. Skulle man spørge denne person, om hvor meget han ville betale for at undgå at naboen spiller høj musik, kunne et svar være 30.000 kr. og således en relativ stor del af den personlige formue. Skulle man derimod spørge samme person om, hvor meget han ville forlange for at lade musikken spille og dermed leve med støjen, ville svaret her oftest være mærkbart højere, f.eks. 100.000 kr. Der er altså tale om den samme genstand/ydelse og meget forskellige svar. Det samme gør sig gældende for potentielle gevinster. Problemet med vurderinger er især relevant, hvis aktøren har personlige følelser i forbindelse med vurderingen. I en praktisk anvendelse af non-compliance modellen kunne det være, at virksomheden har svært ved at begå sig ud fra de nuværende krav til compliance, da de er dyre for virksomheden at overholde og måske forårsager ændrede personlige leveforhold for den ansvarlige, som følge heraf. Løsningen i praksis vil være at få objektive vurderinger foretaget, evt. af konsulent. Objektivitet er derfor en vigtig faktor i forbindelse med praktiske vurderinger af de respektive værdier i modellen.

6.4 Økonomisk konklusion

Et yderst forkortet svar på spørgsmålet i problemformuleringen kan udtrykkes som, at den dataansvarlige vil vælge at foretage valget om non-compliance i tilfælde af, at indtægterne overstiger udgifterne. Naturligvis er dette alt andet end simpelt, eftersom værdierne ikke er åbenlyse. Et svar på spørgsmålet kræver en forståelse af de forhold, der påvirker værdierne i den model, der danner grundlag for analysen.

Om begge aktører

Først bør denne konklusion understrege, at Apple ikke blot er en stor virksomhed, men derimod en kæmpe stor virksomhed. De 4 % i administrativ bødesats er kun relevant i de tilfælde, hvor 4 % af virksomhedens omsætning udgør mindre end 20 mio. Euro. Det er de færreste virksomheder, der passer under denne kategori. Derfor skal de to virksomheder ikke sammenlignes med hinanden direkte. Dette ville ikke give mening. Årsagen til at netop disse to typer virksomheder indgår i afhandlingen er den påvirkning de har hver især på lovgiver. Såfremt Apple skulle vælge at bryde Forordningen og ikke prioriterer reglerne, kunne

⁶² Polinsky s.164-165

dette potentielt blive så alvorligt for lovgiver, at han måtte vælge at ændre reglerne for at være i stand til at skabe en frygt for sanktionerne. Dette ville den mindre virksomhed formentlig aldrig være i stand til. Skulle det blive opdaget, at han bryder loven, ville han blive straffet efter de rammer loven tillader, men det ville næppe føre til andet end det.

Der er flere elementer af modellen, der er svære at vurdere præcist. En antagelse i afhandlingen bygger på, at det godt kan lade sig gøre at vurdere de forskellige forhold, men at dette kommer med en pris i form af udgifter til rådgivning. Denne kan enten findes internt i organisationen eller udefra i form af konsulent.

Om Apple

Forudsat de valgte antagelser i beregningen er korrekte, kan det konkluderes, at Apple aldrig vil vælge non-compliance af Forordningens artikler vedrørende samtykke, da det vil kræve at en skadegørende handling er så værdifuld, at det kan svare sig i forhold til de enorme bødesatser. Hertil er det svært at forestille sig, at en enkelt behandlingsform kan skabe en så stor værdi, at dette kan lade sig gøre. Dette skyldes især reglerne omkring kumulative bøder, hvor der straffes efter virksomhedens globale omsætning, og de forskellige behandlinger kan straffes for sig. Derfor rammes store virksomheder meget hårdt.

Virksomhedens indtjening fra andre kilder end den behandlingen vedrører, inddrages på grund af reglen om den globale omsætning, som beregningsfaktor. Dette kan skabe en bødestørrelse helt ude af proportion, i forhold den potentielle mer-indtjening, som Apple ville kunne holde op mod udgiften. Det er derfor højst usikkert, at Apple nogensinde vil overveje non-compliance.

I forhold til de forskellige værdier i modellen, har Apple bedre forudsætninger for at udregne deres værdi end de mindre virksomheder. De kan benytte egne ressourcer eller hyre udefrakommende ekspertise. Vigtigst i forhold til dette er, at de også indtjener omkostningen, eftersom en overtrædelse af Forordningens regler med al sandsynlighed vil skabe en større meromsætning, end en mindre virksomhed. Dette skyldes at Apple formentlig har flere registrerede, der benytter deres produkter. På trods af de fordele Apple har i forhold til at udregne værdierne, bør bødesatserne alligevel være sat så højt af lovgiver, så valget om non-compliance, aldrig bliver aktuelt for dem.

Om mindre virksomheder

Som modellen antyder er der flere tal, som en dataansvarlig skal forholde sig til ved vurdering om non-compliance som det økonomisk optimale valg. Det forudsætter en klarhed om niveauet i alle værdierne. Findes der risiko i disse er det mindre sandsynligt, at den dataansvarlige vil vælge ikke at overholde loven.

De mindre virksomheder vil potentielt kunne finde det økonomisk optimalt ikke at prioritere compliance. Helt grundlæggende kan der findes flere årsager til, at en mindre virksomhed vælger ikke at overholde Forordningen. De kan vurdere det som værende højst usikkert, at det opdages eller blot ikke have råd til compliance. I det sidste tilfælde vil den omstændighed, at de opdages i at overtræde Forordningen formentlig, føre til samme resultat, som hvis de overholder loven og investerer penge, de ikke har til compliance.

Den væsentligste beslutning vedrørende non-compliance bygger på virksomhedens meromsætning, såfremt de bryder loven. Denne skal overstige den forventede værdi, de straffes med. Hertil må det antages, at en risikoneutral aktør vil være indifferent hvis den forventede meromsætning er den samme som den forventede værdi af den økonomiske straf. En risikoneutral aktør er dog en teoretisk person. Skulle den potentielle straf blive høj nok, vil selv den mest risikoneutrale aktør blive risikoavers.

Generelt er der ikke tale om værdier, hvor aktøren klart kan forudsige værdiens niveau. Der foreligger med andre ord en risiko omkring alle værdierne, og denne risiko vil den risikoaverse aktør have en merpræmie for at påtage sig. Som udgangspunkt bør den aktør, der overvejer non-compliance derfor først undersøge den værdi, som han lettest kan finde. Med dette menes den meromsætning, han kan tjene, såfremt han ikke overholder loven. Er denne værdi ikke høj nok, bør non-compliance ikke overvejes. Hvis den ikke overstiger den forventede værdi, kan det ikke betale sig. Skulle det omvendte scenarie være tilfældet, vil det herefter være den dataansvarliges opgave at undersøge henholdsvis chancen for opdagelse og den potentielle bødestørrelse. Er værdien af den meromsætning virksomheden kan tjene positiv, kan han gå videre med sine udregninger.

Modellen er ikke risikofri, forstået på den måde, at der altid er en risiko for, at værdierne kan være anderledes end aktøren forudsiger dem. Selv under antagelse, at risikoen kan nedbringes ved, at der betales for dette, er det nødvendigt at inkludere flere aspekter. Såfremt der betales for, at aktøren kan kende værdien af et af tallene i modellen, er det ikke sikkert, at kendskab til denne værdi vil medføre, at aktøren kan gå videre med sin plan omkring non-compliance. Med andre ord, der foreligger en risiko for, at de penge, der investeres, ikke kan tjenes ind på ikke at overholde loven.

7. Den økonomisk optimale sanktionsramme

De dataansvarlige må formodes at have en målsætning profitoptimering, imens lovgiver agerer ud fra, at han repræsenterer befolkningen. Forordningen er i høj grad blevet til for at genskabe tilliden til det digitale

domæne. En udelukkende økonomisk tilgang omkring Forordningen, som et værktøj til at promovere økonomien, ville formentlig ikke genskabe denne tillid. En 100 % økonomisk tilgang, som den Kaldor-Hicks optimale tilgang, vil betyde at alle overtrædelser der indtjener sig selv, tillades, og de overtrædelser der ikke er økonomisk optimale, forbydes. Dette vil betyde, at tilstanden før Forordningens ikrafttræden fortsættes, og vil med meget stor sandsynlighed ikke føre til en genskabt tillid.

Til trods for dette er det ikke sikkert, at en delvis økonomisk tilgang, der tilgodeser økonomien, ikke er anvendelig i praksis. En delvis økonomisk anvendelse vil betyde, at lovgiver tager stilling til hvilke overtrædelser der skader i hvilken grad og værdifastsætter dem. Dette er nødvendigt for en økonomisk tilgang, da der ellers ikke kan foretages udregninger om, hvilke overtrædelser der er optimale. En delvis økonomisk tilgang vil også betyde, at de allerværste tilfælde, hvor så meget som en enkelt registreret berøres meget kraftigt, holdes udenfor og tillades under ingen omstændigheder. I praksis kunne dette være, at behandlinger der vedrører følsomme oplysninger eller hvor risikoen er høj, stadigvæk ikke vil tillades. Hvilke behandlinger der skal indgå i denne kategori besluttet af lovgiver, og er elementer der i det hele taget holdes ude af afhandlingen.

Det er tydeligt at ved udarbejdelse af Forordningen, at der er taget stilling til, hvad der anses som skadelig adfærd. Det er også tydeligt, at den administrative bødestraf pålægges med formål om at adfærdsregulere de dataansvarlige. De skal overholde loven, ellers straffes de. Dette gøres uden at bestræbe sig på at finde værdien i de forseelser, den omhandler. Dette kunne man godt finde bemærkelsesværdigt, da man ønsker at pålægge straf ud fra et princip om rimelighed. Rimelighed kunne man godt argumentere for som værende et valg om at pålægge en økonomisk straf der er den samme, som den skade der forårsages. Gøres dette er problemet, at man risikerer at pålægge en økonomisk straf der er den samme som værdien for den skadegørende handling. Dette vil føre til, at den risikoneutrale aktør vil være indifferent overfor om loven holdes. Derfor vil der i den delvis økonomiske tilgang samtidig skulle pålægges en yderligere straf, i tilfælde som den risiko-neutrale aktør, og en mindre straf såfremt den risiko-averse aktør begår forseelsen, for ikke at skræmme den aktør væk, hvis forseelse ville være økonomisk gavnlig.

For at kunne pålægge den korrekte økonomiske straf, vil det kræve, at man finder den økonomiske handlingens værdi. Dette er ikke let i praksis og bør være en vurdering der foretages af myndigheden. Derfor er det en del af den delvis økonomiske tilgang, at myndigheden ved administrativ praksis fastsætter værdien. Værdierne er svære at finde præcist for de dataansvarlige som også illustreret i del 6 omkring *problem of evaluation*. Formålet med den delvis økonomiske tilgang er, at de dataansvarlige ikke skal have

for mange tal at forholde sig til, om de er klar over om en handling er optimal. De skal blot ud fra at observere enkelte tal, helst så få som muligt, kunne tage stilling til, om en behandling er økonomisk optimal.

7.1 Økonomisk optimale anvendelse af sanktionsrammen for administrative bøder

Forordningens sanktioner er primært opbygget omkring den administrative bøderamme, som det foretrukne værktøj til at adfærdsregulere de dataansvarlige. I bogen *Introduction to law and economics*, opsættes en model med henblik på at fastlægge hvordan en lovgiver i en fiktiv by kan anvende bøderammen økonomisk optimalt, i forhold til, at borgerne dobbelt-parkerer⁶³. Målet er at de overtrædelser, der koster samfundet penge, skal aktørerne vælge ikke at foretage, og de forseelser der er gavnlige for samfundet, skal de foretage. Aktører er enten risikoneutrale eller risikoaverse, og alle overtrædelser koster samfundet lige meget. Hernæst er det op til lovgiver at fastsætte bøden og den indsats der anvendes for at håndhæve, påvirker den chance aktøren har for, at forseelsen opdages. Dette resulterer i, at aktørernes adfærd i teorien, reguleres efter hensigten om økonomisk optimalitet, ud fra de antagelser modellen inkluderer. Dette skyldes at de kan udregne den forventede værdi af gerningen. Aktørerne ved hvor meget de får i bøde. De ved grundlæggende hvor stor chancen er for opdagelse, og kan derfor udregne den forventede værdi. Herfra kan de tage stilling til, om den forventede værdi ved at bryde loven er højere eller lavere end den værdi, de vurderer at årsagen til at bryde loven er værd.

Skulle man opsætte et lignende, teoretisk scenarie ved håndhævelsen af Persondataforordningen, indenfor et geografisk område, kunne det se således ud:

Administrationsudgift	Succesrate	Administrativ bøde	Forventede værdi
30 mio. kr. (1.000 ansatte)	Fanger alle (1)	1.000 kr.	1.000 kr.
3 mio. kr. (100 Ansatte)	Fanger 10 % (0.1)	10.000 kr.	1.000 kr.
0.3 mio. kr. (1 Ansat)	Fanger 1 % (0.01)	100.000 kr.	1.000 kr.

Den forventede værdi er i alle tilfælde 1.000 kr. Her ville det være økonomisk optimalt for lovgiver at sætte bøden så højt som muligt, for ikke at anvende unødige ressourcer på at håndhæve loven. Den risikoneutrale ville således vælge at bryde loven, såfremt hans forventede værdi ved at gøre det ville

⁶³ Polinsky s. 79-90

overskride denne grænse på 1.000 kr., og han ville være indifferent, såfremt den forventede værdi var på netop de 1.000 kr.

Som tidligere nævnt, forholder det sig anderledes, såfremt aktøren er risikoavers. Han vil have en merpræmie for, at påtage sig en risiko for, at der pålægges ham en bøde. Dette vil føre til et valg om ikke at bryde loven selv i de tilfælde, hvor det ville være økonomisk optimalt, såfremt han brød loven. Dette ville derfor ikke være ønskeligt. Derfor vil der skulle tages højde for, at den administrative bøde sættes lavere, og de administrative udgifter, som påvirker chancen for at blive opdaget, sættes højere. Årsagen til dette skal findes i at der opstår risk bearing costs⁶⁴, på grund af bøden sættes lavere end den skade der forårsages. Det er derfor den bedste "trade-off" mellem disse parametre der afgør, hvordan den optimale forventede værdi skal sættes i det teoretiske scenarie fra Polinsky⁶⁵.

Forskellen mellem *Law Enforcement Using Fines* og håndhævelse af Forordningen

Grundlæggende er der store forskelle mellem det teoretiske eksempel i bogen, og hvordan Persondataforordningen håndhæves. Her fremhæves de vigtigste forskelle:

Værdien for alle forseelser i det teoretiske eksempel skader med samme værdi. Dette er ikke tilfældet for Forordningen, hvor alle forseelser skader med forskellig værdi.

Aktørerne kender grundlæggende til den forventede værdi. Dette er ikke tilfældet ved håndhævelsen af Forordningen, hvor de mange forskellige forseelser har forskellige forventede værdier.

7.2 Den administrative model

Som alt overskyggende udgangspunkt er private mennesker risikoaverse⁶⁶. Det samme kan siges om de dataansvarlige. En 100 % risikoneutral person, er en teoretisk person, og en model eller virkelighed hvor denne findes i hobetal, er ikke realistisk.

For at håndhæve Forordningen efter mål om at opnå økonomisk optimalitet, kræver det at især den risikoaverse gøres bedre i stand til, at træffe valget. Formålet med dette løsningsforslag er derfor at opsætte en mulighed for de dataansvarlige hvor de kun skal træffe et valg. Valget om at betale en administrationsudgift. Denne udgift kan derefter opvejes imod den ekstra indtjening de vil have, såfremt de ikke skal holde loven.

⁶⁴ Polinsky s.85

⁶⁵ Polinsky s. 90

⁶⁶ Motzfeldt/Østergaard s.14

Størrelsen på den administrative udgift vil naturligvis afhænge af, hvor tung en administrativ byrde der er tale om. Denne skal være sat af lovgiver og være en gennemsnitlig udgift, sådan at den dataansvarlige altid er klar over, hvor meget det koster. Dette kræver naturligvis, den grundlæggende forudsætning, at den dataansvarlige er i stand til, at vurdere på forhånd, om hans behandling er iblandt de forseelser, som kan godkendes. Dette antages den dataansvarlige at være i stand til at vurdere i størstedelen af tilfældene, men i sidste ende vil dette også afhænge af, hvor lang antallet af godkendte/ikke godkendte behandlinger bliver, samt ikke mindst om han er i stand til at forstå, om hans behandlingsform er iblandt dem.

Den administrative instans står derfor med den opgave at vurdere hvilke forseelser, der er økonomisk skadelige og at værdifastsætte disse værdier. Den ekstra indtjening er de dataansvarlige bedre til at vurdere, og de skal derfor fremlægge dokumentation for beløbet af den ekstra omsætning, de mener, at kunne skabe, såfremt de ikke overholder loven.

7.3 Den økonomisk optimale skadesdefinition

Det er nødvendigt for at udregne om en given behandling er økonomisk optimal, at fastlægge en værdi for de forskellige overtrædelser. En præcis vurdering er svær, og vil formentlig være ressourcekrævende. Problemet med at vurdere nøjagtig, betyder dog ikke, at lovgiver ikke kan afgøre vurderingsspørgsmålet. Dette findes der adskillige eksempler på heriblandt fra erstatningsret, hvor der fastsættes en grænse for, hvor meget skadelidte kan kræve i svie og smerte pr. dag⁶⁷. Det samme kan gøres ved at lade lovgiver vurdere de overtrædelser, Forordningen vedrører efter en bestemt praksis, hvor værdierne af skade besluttet ud fra nogle overordnede rammer. En metode for at opnå dette kunne være, at man inddeler de forskellige forseelser og virksomheder i niveauer. Derfra kan udregningen af den værdi, den pågældende forseelse forårsager i skade, sammenlignes med den pågældende gevinst.

Forordningen har selv defineret de elementer der antages at skade. Ud fra dette kan en opdeling foretages af hvilke forseelser der antages at skade mere end andre. I præambelen til Forordningen findes desuden en overordnet definition af hvad der forårsager skade.

7.3.1 Forordningens skadesdefinition

Forordningens skadesdefinition, er meget omfattende. Alle forhold og forseelser der ikke skal tillades beskrives i de mange artikler og betragtninger. Indtil videre er den mest præcise opdeling over hvilke

⁶⁷ <http://hviid-erstatningsadvokater.dk/personskade-takster-2017/>

forseelser der er mere skadelige end andre, den der kan udledes i art.83. Her foretages den meget generelle opdeling med de to niveauer, henholdsvis op til 10 mio. Euro eller 2 % af sidste års omsætning i bøde, eller op til 20 mio. Euro og 4 % af forrige års omsætning i bøde. Hvorledes der sanktioneres økonomisk, skal udledes i retspraksis. Dette er ikke på nuværende tidspunkt information der er tilgængelig.

I Forordningens motiver indgår en direkte beskrivelse af hvad motivet bag vedtagelsen af Forordningen er baseret på. Forordningen begrundes sin egen eksistens, samt kritiserer den manglende gennemslagskraft af direktivet, i præambelens betragtning 9. Her beskrives virkningerne af direktivet som værende ikke tilstrækkelige samt... *med til at skabe en udbredt offentlig opfattelse af, at der hersker betydelige risici for beskyttelsen af fysiske personer i forbindelse med online-aktivitet*⁶⁸. Skaden skal her også anses, som værende *den udbredte offentlige opfattelse*. Med andre ord, den folkelige tillid til det digitale domæne, er det mål der ønskes styrket. Der hentydes derfor til den dårlige omtale. Dårlig omtale er en faktor der varierer fra virksomhed til virksomhed. De største virksomheder, eller dem hvis brand er mest kendt, er de virksomheder med størst potentiale til, at skade tilliden i befolkningen.

Bedømt ud fra Forordningen, er følgende elementer tillagt betydning, i vurdering af hvad der udgør skade på det digitale domæne. Den enkelte overtrædelse, og den pågældende virksomheds evne til at sprede mistillid. Sidstnævnte omkring evne til at sprede mistillid, må som udgangspunkt bedømmes ud fra virksomhedens størrelse og omdømme.

7.3.2 Den delvis økonomiske skadesdefinition

En metode hvorpå værdien af skade kunne fastsættes i praksis, kunne være ved at opstille en model, med formål om at udregne dette. Dette ville betyde, at der foretages en administrativ vurdering, om hvilke forseelser der koster samfundet mest, og lader dette være bestemmende for vurderingen. Dette vil fungere ved, at der tages udgangspunkt i hvor meget det koster samfundet, i tilfælde af, at en enkelt registreret udsættes for forseelsen.

⁶⁸ Forordningens præambel betragtning nr.9

Samtidig skal der også tages stilling til, at der er tale om den folkelige tillid. Denne influeres af i hvor høj en grad, der forsages dårlig omtale om en given virksomhed, såfremt denne skulle forsage en skade. Dette inkorporeres i modellen ved, at lade virksomhedens individuelle evne til at sprede et negativt budskab, indgå som element i vurderingen. Denne faktor fastsættes ligeledes administrativt. Dermed kan der opsættes en model, for at udregne skade:

Model for skadesvurdering

Bedømt ud fra de elementer i Forordningen, hvor der tages stilling til, hvad der udgør skade, kan der opstilles følgende model. Modellen er baseret på en lineær funktion med udtrykket:

$$F(X) = AX + B$$

Der findes tre bestemmende faktorer, angivet som følgende:

Skadesfaktor = X, administrativt fastsat værdi af de forskellige skadegørende handlinger.

Eksponeringsfaktor = A, den specifikke virksomheds evne til at sprede dårlig tillid, såfremt den opdages.

Dette fastsættes, ligeledes, administrativt.

Antallet af registrerede berørt af handlingen = B

De forskellige faktorerens værdi opstilles i niveauer, f.eks. 10, eller 100 forskellige niveauer, for at gøre behandlingens skadeevne så præcis som mulig.

For at en given handling vil være økonomisk optimal, vil det kræve at den ekstra indtjening den pågældende dataansvarlig foretager, overskrider værdien af denne model omkring skade. De dataansvarlige vil være de bedste til, at vurdere den ekstra indtjening de kan opnå, såfremt en behandling tillades. Den dataansvarlige skal derfor selv ved den administrative behandling, vedlægge dokumentation for en ellers behandlings økonomiske potentiale.

7.4 Kritik af modellen

Grundlæggende er de forseelser der forsager skade i Forordningens tilfælde, svære at foretage en nøjagtig vurdering af. Problemstillingen afspejler de samme elementer fra den økonomiske del (del 6) omkring *problem of evaluation*. Mennesker vurderer subjektivt, baseret på den enkeltes økonomi og præferencer, og både lovgiver og dataansvarlige, kan vurdere forkert.

Der er samtidig tale om, at vurderingen baseres på virksomhedens evne til, at budskabet spredes, hvilket også er med til, at vurderingen bliver meget vanskelig. Forskellige forseelser spredes forskelligt, alt afhængig af andre ting, end virksomhedens størrelse og brand værdi. Virksomhedens aktivitet kunne være et eksempel på, hvordan befolkningen ville placere deres forventninger, til lige præcis denne type af firma og dets medarbejdere. Et eksempel på dette kunne være, at sammenligne en buschauffør, med en medarbejder i en børnehave. Det ville være forventet, at pædagogerne i børnehaven er meget god til, at passe på børnene, hvor man til en vis grad også vil forvente, at buschaufføren passer på sine passagerer. Det ville dog ikke være forventet at buschaufføren havde decideret specialviden om, at passe på børn da det ikke er indenfor dennes arbejde at have en sådan viden. Her ville man ikke tillægge medarbejderne samme forudsætning, om at de skal være gode til, at passe på børn. Der er med andre ord store forskelle i de forventninger fra omverden til aktøren, i forhold til hvad denne foretager sig. Disse forventninger kan formentlig ikke inkorporeres i en model, hvor man placere de forskellige overtrædelser i niveauer, og lader dem være bestemmende for en vurdering af skade. Hertil ville der komme mange forskellige reaktionsmønstre omkring de forskellige overtrædelser, alt afhængig af hvem der foretog dem. Hermed bliver det meget svært, at inkorporere eksponeringsfaktor i den vurdering af skadesforholdet. Resultatet af dette ville blive en indskrænkning af de behandlingsformer der vurderes, at kunne tillades administrativt.

Polinsky nævner selv i sin teori, er der findes flere forhold der ikke kan overføres til praktisk anvendelse. Selv den mest risikoneutrale aktør, vil i de tilfælde hvor han kan risikere hele sin formue, eller en meget stor del af denne, ikke være risikoneutral længere, men derimod risikoavers⁶⁹. Dette kaldes også *wealth effects*⁷⁰, som ligeledes omtales i *problem of valuation*. Den administrative udgift kan ende med, at skulle sættes højt, da der er tale om forhold der er svære, at vurdere. Ender udgiften med, at blive for høj, vil det skræmme aktører væk, der ikke ønsker at løbe risikoen for, at deres behandling ikke godkendes efter de har betalt administrationsudgiften. Lovgiver kan omvendt ikke lade administrationsudgiften tilbagebetales ved manglende godkendelse, da dette blot vil føre til, at alle aktører forsøger, at få selv de mest håbløse behandlinger godkendt, da det så er risikofrit, at få foretaget den administrative vurdering. Konsekvensen af dette er også, at listen med de forhold der ikke kan indgå i den administrative vurdering øges, for at holde den administrative udgift nede. Her er det spørgsmålet om dette også vil ende med, at inkludere behandlinger der er økonomiske gavnlige, hvilket er det modsatte af formålet med den administrative behandling.

⁶⁹ Polinsky s.90

⁷⁰ Polinsky s. 164

En administrativ fastsat udgift vil være en større gevinst for de store virksomheder end de mindre, såfremt udgiften er den samme. De større virksomheder kan bedre betale udgiften, og lettere indtjene den, eftersom deres behandlinger, formodentlig, indtjener mere end de små virksomheder. Dette kan imødekommes ved, at der pålægges en større udgift for de store virksomheder end ved de mindre. Dette skal dog være relativt i forhold til den potentielle indtjening, som kun virksomheden kender til. Skal lovgiver derfor kunne sætte et beløb der er relativt, i forhold til indtjeningen, kræver det, at det er dem der også foretager vurderingen om indtjeningen, eller at de ved betaling af administrationsudgiften er i besiddelse af denne viden. Dette vil være svært, og i bedste fald medføre, at den administrative udgift bliver højere.

7.5 Målsætning med Forordningen

Forordningens motiv omtales i præambelens betragtning 9. I denne begrundes Forordningen sin egen eksistens, samt kritiserer den manglende gennemslagskraft af direktivet. Her beskrives virkningerne af direktivet som værende ikke tilstrækkelige samt... *med til at skabe en udbredt offentlig opfattelse af, at der hersker betydelige risici for beskyttelsen af fysiske personer i forbindelse med online-aktivitet*⁷¹. Skaden skal her også anses, som værende *den udbredte offentlige opfattelse*, som med andre ord er den folkelige tillid. Det kan derfor udledes af præambelen betragtning 9, at direktivet ikke har skabt det incitament blandt de dataansvarlige, til at disse har prioriteret at overholde regelsættet. Incitament skal her forstås, som den økonomiske straf ikke var tilstrækkelig ved direktivet, og de dataansvarlige kunne uden økonomiske konsekvenser lade være med at prioritere, at overholde reglerne. Det er tydeligt, at der hentydes til håndhævelsen, eftersom lovteksten i Forordningen og direktivet, minder om hinanden. Resultatet af den manglende håndhævelse har ført til et fald i tilliden til det digitale domæne. Samtidig kan det også udledes, at en bedre beskyttelse, ligeledes, har været blandt motivet, som netop også vil være et resultat af at de dataansvarlige har større incitament til at efterleve regelsættet.

Det vil ikke være retvisende kun at anse bedre beskyttelse af personoplysninger, som det eneste motiv for vedtagelse af Forordningen. Kommissionen har selv beskrevet den mulige økonomiske gevinst, en totalharmonisering af regelsættet vil medføre, som en væsentlig faktor for vedtagelse af Forordningen. Det anslås at den potentielle øgede vækst med vedtagelse af Forordningen løber op mod 415 mia. Euro, og skabelse af hundredetusindvis af nye jobs⁷². I præambelen beskrives økonomien, som havende potentiale til

⁷¹ Forordningens præambel betragtning nr.9

⁷² https://ec.europa.eu/commission/sites/beta-political/files/dsm-factsheet_en.pdf

at styrkes, såfremt udvekslingen af personoplysninger stiger. Dette skal foregå gennem en øget udvekslingen af persondata, på baggrund af øget folkelig tillid. Dette udtrykkes i betragtning nr.7 i præamblen, hvor der redegøres for den teknologiske udvikling samfundet har haft. Her omtales denne udvikling som en stærk medvirkende faktor til øget vækst i samfundet. Denne skal bibeholdes, eller endda styrkes, ved at genskabe tilliden til de digitale tjenester.

Betragtning 7 og 9 i præamblen kan godt anskues, som hinandens modsætninger ved første øjekast. En øget anvendelse af persondata skaber økonomi, hvor en begrænsning af det selv samme, som er det Forordningen til en vis grad medfører, bør skabe det modsatte. Dette er ikke den korrekte fortolkning. Den rigtige fortolkning må, uden tvivl, være følgende: Forordningens ankomst, skal skabe en folkelig tillid til Det Digitale Domæne, ved at begrænse den skadevirkende aktivitet. Dette opnås ved at skabe en effektiv beskyttelsesramme. På baggrund af den høje beskyttelsesramme, opnås målet om at genskabe tilliden og derigennem den forbedrede økonomi. Det er igennem den høje beskyttelse, at brugen af de digitale tjenester, vil stige som resultat. Dette forhøjede brug af disse tjenester, skal derigennem skabe en økonomisk vækst. Der er tale om, at tillid skal fortjenes. Tillid er et symptom på det underlæggende element, datasikkerhed. Det er den sikkerhed borgerne føler de har når de færdes i det digitale domæne, der skal skabe den bedre økonomi. Sikkerheden skal med andre ord være høj, for at tilliden, og derefter økonomien skal stige, som resultat deraf.

7.6 Integreret konklusion

Grundlæggende findes der adskillige problemer for en anvendelse af den delvis økonomiske tilgang. Dette er allerede illustreret i afsnit 7.4, om hvordan vurderingsspørgsmålet kan påvirke anvendelsen. Mest relevant for forståelsen er det, at de forskellige udfordringer påvirker den administrative udgift, så denne bliver højere, samt antallet af ikke-lempelige forseelser øges. Dette kan resultere i at anvendelsen indskrænkes. Dette betyder ikke, at den nævnte vurdering ikke kan foretages, men at den kan blive høj. Alle ting vil formentlig kunne udregnes og endda forholdsvis præcist, men forholdende ville kræve særdeles kyndig rådgivning. På baggrund af denne usikkerhed, må en vurdering af modellen, være baseret på en antagelse. Denne antagelse er følgende:

De dataansvarlige præsenteres for en administrativ udgift. Denne kan de holde op mod, om de ønsker, at vurdere om hvorvidt det er økonomisk optimalt, at betale denne udgift, eller lade være.

I forhold til lovgivers motiver taler flere forhold imod anvendelsen af den delvis økonomiske tilgang. I høj grad vedrører problemer med at anvende modellen, at der er tale om tillid til det digitale domæne. Denne tillid skal vindes gennem en høj beskyttelsesramme, og ikke ved økonomisk spekulation. En økonomisk anvendelse vil formentlig ikke skabe en øget tillid, da tillid er et symptom på de forskellige behandlinger. Lovgiver, som repræsenterer de registrerede, vil ikke finde tiltag der går imod datasikkerhed, som værende forenelig med, at opnå en højere tillid. Dette umuliggør ikke en delvis økonomisk anvendelse, men vil kraftigt begrænse de forseelser, som lovgiver kan tillade at være lempelige. Lovgiver vil med andre ord, kun tillade de forseelser han er sikker på ikke skader tilliden.

Størrelsen på den administrative udgift vil, alt afhængig af de forskellige påvirkninger, kunne stige. Lovgiver vil med den foreslåede model, skulle forholde sig til, at skulle reagere i forhold til den optimale pay-off, imellem at lade de dataansvarlige betale hele udgiften til administration selv, eller at påtage sig noget af denne udgift, som også omtalt omkring Polinskys model i del 7.1 omkring *risk-bearing costs*. For lovgiver vil det være ønskeligt, at kunne vurdere udgiften nogenlunde præcist, så den kan håndhæves efter den bedste kombination af pay-offs. Fejl, som også omtales af Polinsky er en faktor der påvirker risikoen, er ønskelige at holde på et så lavt niveau, som muligt. For at det skal være ønskeligt for lovgiver, skal fejl ved vurderingen være lave, så omkostningerne ikke stiger. Dette vil føre til, at de risiko-averse ikke vil risikere, at bryde loven, hvilket vil føre til, at lovgiver må påtage sig de førnævnte risk-bearing costs.

De dataansvarlige vil ud fra deres ønske om profitoptimering, være anderledes mindre kritiske. Ud fra antagelsen om, at de dataansvarlige præsenteres for den administrative udgift, kan denne kan enten betale eller lade være. Bliver udgiften for høj, vil det formentlig skræmme de mest risikoaverse væk fra at benytte muligheden. Der findes derfor væsentlige begrænsninger for dets anvendelse. Med dette menes, at risiko ikke kan fjernes helt, uanset administrationsudgiftens størrelse. Den dataansvarlige kan ikke være sikker på, at en betaling af udgiften også vil medføre at behandlingen tillades. Udgiften skal her holdes op mod værdien af den ekstraindtjening han mener, at kunne opnå. Her er spørgsmålet hvor sikker han er på, at denne indtjening også er i det leje han håber. Risikoen vil her, proportionelt, være højere såfremt administrationsudgiften ligeledes, er høj. Her kan det i sidste ende betyde, at den dataansvarlige, som illustreret i del 6 omkring non-compliance, vil være nødsaget til at forholde sig til adskillige tal, på samme måde som i denne del af afhandlingen. Med dette menes, at han skal vurdere den ekstra indtjening og

chancen for at behandlingen tillades. Dette vil naturligvis være relativt i forhold til udgiftens størrelse, og skulle anses i samspil med lovgivers beslutning. Skulle lovgiver påtage sig en del af udgiften i form af risk-bearing costs, vil dette kunne medføre at de dataansvarlige skal betale en lavere udgift. Dette vil tiltrække de risikoaverse aktører, til at benytte sig af muligheden.

8. Konklusion

Apple overholder på de fleste områder de udvalgte regler der er genstand for analysen i den juridiske del af denne afhandling. Mindst relevant bliver analysen omkring overholdelse af gennemsigtighedsprincippet. Dette skyldes, at kravene som stilles i gennemsigtighedsprincippet omhandler krav, som de andre artikler i forvejen stiller. Vedrørende samtykkereglerne har Apple en høj standard allerede inden Forordningen er trådt i kraft. Apple skal således ikke foretage nogle ændringer i deres nuværende fremgangsmetode for at være en overensstemmelse med kravene i Forordningens art.4, samt art. 7. Anderledes forholder det sig omkring de krav, der stilles i Forordningens art.13, vedrørende oplysningspligten. Mange af de krav, som oplysningspligten vedrører, har Apple slet ikke inkorporeret i deres formidling til den registrerede. Dette er helt sikkert et område, hvor Apple inden Forordningens ikrafttrædelse skal have ændret deres fremgangsmetode for ikke at være i strid med Forordningens art.13.

Omkring den beskyttelse Apple skal yde i forhold til den risiko de indsamlede oplysninger udgør, må det være betryggende som Apple-bruger, at de oplysninger beskyttes så godt, som Apple selv angiver er tilfældet. Dette gør det højst usandsynligt, at oplysningerne kan tilgås af andre. I så fald ville oplysningernes kryptering gøre dem umulige at læse. Skulle dette alligevel ske, vil det ikke være oplysninger, der udgør en så høj risiko for den registrerede, at denne kunne føle sig krænket af at de kom i fremmede hænder. Derfor er det også tilstrækkeligt, at Apple følger de anvisninger for datasikkerhed i art.32, som er den generelle fremgangsmetode. Her skal der tages hensyn til, at afhandlingen ikke bedømmer Apple som helhed. Var dette tilfældet, skulle Apple formentlig anvende art.35 med den dertil hørende udvidede sikkerhedsplan (DPIA).

Afhandlingens økonomiske og integrerede del omhandler virksomheden som beslutningstager. I begge dele, er det vigtigste spørgsmål for den dataansvarlige, om hvorvidt han kan tjene mere på ikke at overholde Forordningens regler.

I den økonomiske del er spørgsmålet, hvorvidt han kan opnå vished omkring værdierne, såfremt han benytter non-compliance modellen. Det kan potentielt koste ham dyrt, såfremt han ikke er i stand til dette, og vælger at gøre det alligevel. Såfremt han er i stand til dette, kan han alligevel være uheldig, at blive opdaget. Her spiller den bødestørrelse, den dataansvarlige kan risikere at modtage også en afgørende rolle. Det er størrelsen af bøden, der kan anvendes som indikator for, i hvor høj en grad den dataansvarlige kan tillade sig at være risikoneutral. Såfremt bøden er i en så høj størrelse, at virksomheden må lukke som

konsekvens af forseelsen opdages, er det formentlig sikkert, at den førhen så risikoneutrale aktør også vil være risikoavers i den situation, hvor en stor del af hans formue er på spil.

I det hele taget er der flere ting, der er afgørende for, om den dataansvarlige nogensinde kommer til at træffe valget om non-compliance. Den rigtige fremgangsmetode må være, at den dataansvarlige først vurderer, hvor mange penge han mener at kunne opnå i mer-indtjening, såfremt han ikke holder loven. Dette beløb må antageligt være af en vis størrelse, før det overhovedet vil kunne betale sig for den dataansvarlige. Det må samtidig også være det beløb, som den dataansvarlige lettest har adgang til at vurdere. Er der her ikke tale om et mærkbart beløb, er det ikke sikkert at den dataansvarlige nogensinde vil finde det interessant at gå videre med de resterende udregninger i modellen. Dette er naturligvis afhængigt af, i hvor høj grad denne er risikoneutral, samt om bødens størrelse vil have afgørende betydning.

I den integrerede del af afhandlingen inddrages lovgivers motiver i forhold til ønsket om, at skabe en økonomisk optimal anvendelse af de administrative bøder. Bedømt ud fra motiverne er det tvivlsomt, om lovgivers hensigter med håndhævelsen af de administrative bøder er at lade økonomiske hensyn have en betydningsfuld rolle. Det ønskelige resultat med Forordningen er at opbygge tilliden til det digitale domæne. Her vil økonomiske motiver let kunne opfattes som en modsætning til at opbygge tillid. I bedste fald vil dette medføre, at økonomiske overvejelser inkluderes i begrænset omfang, og i værste fald vil de slet ikke inkluderes. Det første må være tilfældet for den nuværende udgave af Forordningen. Dette skyldes, at økonomiske betragtninger er inkluderet på flere områder, både omkring datasikkerhed hvor det accepteres at den dataansvarlige kan have et lavere niveau, såfremt det bliver uforholdsmæssigt dyrt, men også omkring målsætningen med Forordningen, hvor økonomi nævnes som en væsentlig målsætning med vedtagelse af det nye regelsæt.

Formålet med modellen i den integrerede del er at skabe et system hvor lovgiver kan gøre adgangen for de økonomisk optimale overtrædelser lettere for de dataansvarlige. Det er tankegangen om ikke at blokere for den type af forseelser, som er økonomisk optimale, og som de risikoaverse dataansvarlige vil foretage under det nuværende regelsæt, som ønskes promoveret. I stedet for at den dataansvarlige skal forholde sig til adskillige tal og det at bryde loven i det hele taget, er det meningen, at den dataansvarlige skal forholde sig til kun et tal. Dette vil være en stor udfordring, eftersom det er svært at udregne, hvor meget skade de forskellige forseelser forårsager. Dette kan medføre, at administrationsudgiften øges til et niveau, hvor de risikoaverse anser risikoen for at betale afgiften, og ikke få sin behandling godkendt, som værende for høj.

For at imødekomme denne risiko, kan lovgiver sænke udgiften og dermed påtage sig nogle af omkostningerne. Alternativt kan antallet af forseelser, som kan indgå i bedømmelsen, sættes ned.

Litteratur og henvisninger

Bøger

- Dall, Langebæk, Langemark. 2016. **Persondataforordningen - En håndbog for praktikere**. København. Ex Tuto A/S. 1.Udgave.
- Balci. 2018. **Kompendium i Persondataret og Persondataforordningen**. Frederiksberg. KompendieForlaget. 1. Udgave.
- Blume. 2017. **Persondataretlige grundfigurer - Strejftog i den nye persondataret**. København. Jurist og økonomforbundets Forlag. 1. Udgave. Citeret i afhandlingen: **Blume 1**.
- Blume. 2016. **Den nye persondataret. Forordning 2016/679 om persondatabeskyttelse, Med en omtale af direktiv 2016/680 (politipersondataret)**. København. Jurist – og Økonomforbundets Forlag. 1. Udgave. Citeret i afhandlingen: **Blume 2**.
- Nielsen. 2005. **Institutionel Teori - En tværfaglig introduktion**. Roskilde. Roskilde Universitetsforlag. 2. Udgave.
- Polinsky. **A Introduction to Law and Economics**. New York. Aspen Publishers. 3. Udgave.
- Kure. 2014. **EU-ret kompendium**. Karnov Group Denmark A/S. 5. Udgave.

Artikler

- Flyverbom. 2017. **Datafication, transparency and trust in the digital domain**. s.3.
- Polinsky, Shavell. 1999. The Economic Theory of Public Enforcement of Law. NBER Working Paper no.6993. s.4-6.
- Motzfeldt, Østergaard. 2016. Fortid, Nutid og fremtid. Juridisk Institut, Syddansk Universitet. s. 6, s.14.

Lektioner

- Ret og Kontraktret 17.oktober. 2016. (Tema: Moral og efficiens)

Regulering

- **Forordning 2016/679** - om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF. GDPR.
- **Persondataloven**. Baseret på Persondatadirektivet. Direktiv 95/46 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. PDL.

- **Aftaleloven.** Bekendtgørelse af lov om aftaler og andre retshandler på formuerettens område. AFTL.
- **Traktaten om den Europæiske Unions Funktionsområde.** TEUF.

Domme

C-101/01 – Bodil Lindquist

Internethenvisninger

- Jensen og Wittorf udg. 2017. **Indsigt: Salg af dine sundhedsdata er et spirende kæmpemarked: Her er fire vigtige pointer.** Link: <https://www.computerworld.dk/art/242022/indsigt-salg-af-dine-sundhedsdata-er-et-spirende-kaempemarked-her-er-fire-vigtige-pointer>
- Apples omsætning. Link: <https://www.apple.com/newsroom/2018/02/apple-reports-first-quarter-results/>
- Sundhedsappens formål. Link: <http://lydogbillede.dk/nyheter/apple-health/apple-tager-fat-om-hele-sundheden/>
- Formål med research kit og Sundhedsappen. Link: <https://www.apple.com/researchkit/>
- Definition af sundhedsdata: https://en.wikipedia.org/wiki/Health_data
- Appen der indsamler HIV-oplysninger. Link: <http://nyheder.tv2.dk/udland/2018-04-03-homo-datingapp-far-hug-for-at-dele-brugeres-hiv-oplysninger>
- Sundhedsappens sikkerhedsforanstaltninger. Link: <https://support.apple.com/da-dk/HT203037>
- FOM om offentliggørelse af registreredes oplysninger. Link: http://www.ombudsmanden.dk/find/udtalelser/beretningssager/alle_bsager/2011-15-1/2011_15-1_pdf-version/
- Apples omsætning if. Statistica.com. Link: <https://www.statista.com/statistics/265125/total-net-sales-of-apple-since-2004/>
- Googles rekordbøde. Link: <https://www.aljazeera.com/news/2018/07/eu-hits-google-5bn-fine-breaking-competition-rules-180718091255980.html>
- Dårlig omtale indirekte omkostning. Link: ¹ <https://securekey.com/blog/bad-reputation-the-indirect-costs-of-data-breaches/>
- Hviid Advokater. Erstatningsretlige satser. Link: <http://hviid-erstatningsadvokater.dk/personskade-takster-2017/>
- EU-Kommissionens økonomiske motiv. Link: https://ec.europa.eu/commission/sites/beta-political/files/dsm-factsheet_en.pdf