Agilitet i implementering af persondataforordningen

En juridisk og erhvervsøkonomisk analyse af databeskyttelse gennem design under en agil tilgang

af FREDERIKKE SCHLITTERLAU og JULIE ENØ JENSEN

Den 25. maj 2018 trådte en ny forordning om beskyttelse af personoplysninger i kraft, som har til formål at styrke de foranstaltninger, som sørger for korrekt håndtering af de registreredes personoplysninger. Nærværende afhandling har til formål at analysere persondataforordningens artikel 25 stk. 1 omhandlende databeskyttelse gennem design. Ydermere vil afhandlingen undersøge, hvilke krav databeskyttelse gennem design stiller til organisatorisk agilitet.

De organisatoriske tilgange er afgørende, når persondataforordningen implementeres i organisationens processer. Selve implementeringen skal ske som en del af en iterativ proces, for at det sikres, at formålet med forordningen oppebæres på den mest effektive måde. Gennem en iterativ proces bevares de elementer, som understøtter en effektiv implementering, og de elementer, som står i vejen for en effektiv implementering, frasorteres. Det er vigtigt, at forordningen anvendes i organisationerne med en tanke om hele tiden at kontrollere og effektivisere databeskyttelsen.

Nærværende afhandling præciserer, at databeskyttelse gennem design med alt sandsynlighed er betinget af at opretholde fleksibiliteten for at få en succesfuld implementering. Dette skabes gennem teorien bag organisatorisk agilitet. Baseret på denne teori kan det konkluderes, at implementeringen af databeskyttelse gennem design skal foregå ud fra de 8 udvalgte faktorer i analysen. De 8 faktorer danner grundlag for udformningen af denne afhandlings framework. Frameworket er denne afhandlings retningslinje for hver enkelt organisation og skal bruges som værktøj til at overholde databeskyttelse gennem design. Det kan konkluderes, at implementeringen af databeskyttelse gennem design skal gå igennem alle organisationens niveauer, hvorved denne afhandlings framework er det mest optimale værktøj hertil. Vores anbefaling til nuværende og fremtidig databeskyttelse i organisationer er at tage udgangspunkt i frameworket for at opfylde kravene, som databeskyttelse gennem design stiller til organisatorisk agilitet. Det er i høj grad nødvendigt for organisationerne at vedligeholde agilitet som en del af en iterativproces for at kunne stille den fornødne sikkerhed til den teknologiske udvikling.

Abstract

On the 25th of May 2018, a new data protection regulation, with the purpose of strengthening the institutions that ensure correct handling of personal data, became effective. The purpose of this dissertation is to analyse the data protection regulation's article 25 subsection 1, which is concerned with the privacy by design principle. Furthermore, the requirements for organisational agility that privacy by design entails will be investigated.

The organisational approaches are crucial, when the data protection regulation is implemented in an organisation's processes. The actual implementation must occur as a part of an iterative process, in order to ensure that the purpose of the regulation is realised in the most effective way. Through

an iterative process, the elements supporting an effective implementation are kept, while the elements working against an effective implementation are eliminated. It is central that the regulation is employed with a constant focus on controlling and making the data protection more effective.

This dissertation points out that privacy by design, with all probability, is contingent of an organisation preserving its agility, in order to achieve a successful implementation. The preservation is ensured by employing the theory on organisational agility. Grounded in this theory, it can be concluded that the implementation of privacy by design must occur based on the eight institutions chosen for the analysis. The eight institutions constitute the foundation that shapes the framework of this dissertation. The framework is considered this dissertation's guideline for every organisation and will be used as a tool to adhere to privacy by design. It can be concluded that the implementation of privacy by design must go through all organisational levels, and that the framework presented in this dissertation is the most optimal tool for achieving it. Our recommendation, for present and future data protection in organisations, is to follow the framework, in order to meet the requirements for organisational agility that privacy by design entails. It is highly important for organisations to maintain their agility as a part of an iterative process, in order to ensure the necessary security for the technological development.

Indholdsfortegnelse

Del I – Indledning

Det digitale marked ændrer sig i takt med, at teknologien er i konstant vækst. Persondata bevæger sig på tværs af landegrænser på et splitsekund uden problemer. Problemet ligger i, hvordan man kan kontrollere og håndtere flowet og behandlingen af persondata på en sikker og forsvarlig måde. Men hvorfor er dette et problem? Problemet handler ikke om, at databrug er uønsket, men om at kunne sikre en passende beskyttelse af det enkelte individs persondata og derved genoprette en tillid til de aktører, der anvender data. Den hidtidige udvikling kombineret med svingende regelefterlevelse har ført til, at EU Kommissionen har udformet en ny regulering i form af den nye persondataforordning (herefter forordningen). Denne er baseret på, at informations- og kommunikationsteknologien nu er grundlaget for alle moderne og innovative økonomiske systemer, hvilket har været med til, at der er blevet fremført en strategi for det indre marked i Europa.

> *"Et digitalt indre marked er et marked, hvor den frie bevægelighed for varer, personer, tjenesteydelser og kapital er sikret, og hvor privatpersoner og virksomheder gnidningsløst kan få adgang til og udføre onlineaktiviteter under fair konkurrencevilkår og med et højt niveau af forbruger- og databeskyttelse, uanset deres nationalitet eller opholdssted. Et digitalt indre marked vil sikre, at Europa fastholder sin førerposition i verden inden for den digitale økonomi, og hjælpe europæiske virksomheder til at vokse på verdensplan."* (COM(2015) 192 final, s. 3).

Men hvordan får man organisationerne til at opfylde strategien for det indre marked omkring den frie bevægelighed for personer samtidig med, at de konstant skal opfylde forordningens krav i artikel 25 om databeskyttelse gennem design, hvor man skal opnå passende tekniske og organisatoriske sikkerhedsforanstaltninger? Alle organisationer bestræber sig på at følge den fortsatte digitale vækst samtidig med, at den daglige drift stadig skal fungere, hvor der kan forekomme ressourcemangel. Yderligere skal man både have teknologier og medarbejdere, der skal kunne håndtere alt dette.

Det er forskelligt fra organisation til organisation, hvilke tekniske og organisatoriske foranstaltninger som ud fra et retligt perspektiv kan betegnes som passende. Som udgangspunkt skal hver organisation først finde frem til hvilke design, der er passende for dem og hvilke der i kommissionens øjemed må anses for at være passende. Efter denne udførelse fra organisationens ledelse og den persondataansvarlige skal dette efterfølgende implementeres i organisationen. Men at ændre

medarbejdernes og organisationens vaner og daglige rutiner synes være en udfordrende opgave. Så hvordan bliver kommissionens krav om databeskyttelse gennem design succesfuldt implementeret i organisationen? Det må anses for at være vigtigt ikke kun at kunne fremføre hvilke tiltag, der skal indføres i organisationen, men også faktisk få dem gennemført succesfuldt.

Sammenspillet mellem kravet til databeskyttelse gennem design og implementeringen heraf må ud fra en organisation anses som værende målet for at effektivisere organisationen. I det øjemed er denne afhandling en anbefaling for organisationerne til at benytte sig af organisatorisk agilitet for at opnå dette. Tankegangen bag tager udgangspunkt i fleksibilitet og forandringsledelse for dermed at skabe det bedste resultat i udformningen og implementeringen af databeskyttelse gennem design.

1.1 Problemformulering

Den centrale problemstilling er:
Hvilke krav stiller databeskyttelse gennem design til organisatorisk agilitet?

Hertil er der følgende underspørgsmål:

- *Hvad forstås ved databeskyttelse gennem design i persondataforordningens artikel 25 stk. 1?*
- *I hvilken grad vil organisatorisk agilitet være anvendelig i implementeringen af databeskyttelse gennem design i persondataforordningens artikel 25 stk. 1.*

Formålet med nærværende afhandling er, at analysere det juridiske indhold af artikel 25, stk. 1 – *databeskyttelse gennem design.* Afhandlingen vil afdække den juridiske rækkevidde af artikel 25, stk. 1, under inddragelsen af artiklens ordlyd og relevant retspraksis. Det er et mål at redegøre for, hvilke tiltag der kræves af organisationerne i implementeringsprocessen. I relation til dette vurderes det, hvorvidt en teori omkring organisatorisk agilitet kan anvendes til at skabe det bedste resultat hos hele organisationen.

1.2 Afgrænsning

Implementeringen af forordningen har rigtig mange aspekter. Der er i nærværende afhandling valgt at tage udgangspunkt i den dataansvarliges ansvar inden for opfyldelsen af forordningens artikel 25, stk. 1 omkring passende tekniske og organisatoriske sikkerhedsforanstaltninger og en juridisk analyse heraf. Dog vil der i de fremførte interviews også henvises til den generelle implementering og håndtering af forordningen, som kan bidrage til understøttende empirisk materiale i afhandlingen. Al ansvar, der yderligere foreligger hos databehandleren, jf. forordningens artikel 28, bliver ikke belyst i denne afhandling, da fokus, som nævnt tidligere, kun er på den dataansvarlige. I forhold til det empiriske materiale afgrænses der kun til det, der i nærværende afhandling måtte anses for at være relevant og understøtte problemstillingen.

Afhandlingens problemstilling ønsker at undersøge organisationens håndtering af implementeringen af forordningens artikel 25, stk. 1, efter man har fundet frem til hvilke tiltag, der måtte anses at være passende sikkerhedsniveau. Dette bliver i denne afhandling analyseret ud fra en teori om organisatorisk agilitet. Indholdet afgrænses dermed til kun at omhandle denne tilgang og ikke andre agilitetsteorier. Det er en vurdering af, at man skal operere på det organisatoriske plan for en succesfuld implementering og ikke ned i softwareudviklingsteorierne eller agilitet i arbejdsprocesserne.

1.3 Metode

I denne afhandling bliver der brugt den retsdogmatiske metode, hvor der først vil blive identificeret de relevante juridiske problemstillinger ved databeskyttelse gennem design. Herefter bliver de juridiske problemstillinger løst gennem en fortolkning, systematisering og udfyldning af relevante retskilder, for i sidste ende at finde frem til, hvad der må betegnes at være gældende ret inden for området (Blume, 2009). Metoden vil i denne afhandling belyse både de nuværende og de fremtidige effekter for alle de dataansvarlige og deres medarbejdere i deres implementering af databeskyttelse gennem design. Denne metode er med til at skabe den røde tråd gennem den juridiske tilgang.

I forhold til den erhvervsøkonomiske tilgang i denne afhandling vil der blive taget udgangspunkt i organisatorisk agilitet som metode til at belyse en organisations måde og tilgang til at implementere databeskyttelse gennem design på bedst mulig vis og med størst mulighed for succes.

1.3.1 Kilder

Afhandlingen vil beskæftige sig med de europæiske databeskyttelsesregler til at belyse problemstillingen og der vil blive inddraget andre nationale retsregler i det omfang, der anses for at være relevant.

Afhandlingen vil ligeledes inddrage national retspraksis, som måtte synes relevant. Der findes dog ikke nogen national retspraksis inden for forordningen endnu og det kan derfor her tilføjes, at problemstillingen i denne afhandling omhandler en regulering der gælder fra 25. maj 2018 og derfor er nogle af de relevante retskilder og retspraksis baseret på regulering gældende fra før den 25. maj 2018. Dog må det antages, at alt det medbragte retspraksis må anses for at være et minimumskrav til databeskyttelse gennem design, da disse afgørelser allerede er vurderet af det danske datatilsyn.

En anden form for kildeinddragelse er i forhold til den lighed, der er mellem retssystemerne indenfor de nordiske lande og deres nationale regler indenfor databeskyttelse og endvidere deres håndtering af forordningen. Derfor kan retstilstanden i de andre nordiske lande i en vis grad tillægges betydning for retstilstanden i Danmark. Det er blandt andet Norge, som er langt i forhold til deres håndtering af databeskyttelse gennem design og derfor meget relevant for belysningen af problemstillingen. Afhandlingen vil anvende forordningen og yderligere anvende bøger, artikler og andre relevante sekundære kilder til at belyse problemstillingen. I nærværende afhandling vil kildehenvisningen være anført ud fra Harvard-metoden, hvor der refereres til forfattere og årstal på kilden.

1.3.1.1 Indsamling og inddragelse af empiriske data

For at forstå den praktiske kobling mellem det juridiske og det erhvervsøkonomiske perspektiv i nærværende afhandling, vil der blive inddraget tre interviews med praktikere inden for området. Det første interview er indgået med en dataansvarlig i virksomhed Y, det andet interview er indgået med en dataansvarlig i virksomhed X og slutteligt er der indgået et ekspertinterview med en advokat, som er specialist i databeskyttelse. Det er derved i al sin enkelhed det praktiske bevis for, at det juridiske og erhvervsøkonomiske, i relation til hvilke krav databeskyttelse gennem design stiller til organisatorisk agilitet, er uadskilleligt. Derfor er det nødvendigt at opnå en dybere forståelse for den praktiske håndtering, for at teorien kan komme effektivt til virke.

I alle tre interviews har den interviewede fået muligheden for at være anonym, og i alle tre tilfælde er dette blevet aktuelt. Det har hverken haft nogen negativ effekt på resultatet af interviewene eller gjort data sværere at arbejde med. Tværtimod har anonymiteten haft den betydning, at den interviewede har været ærlig og givet udtryk for de mest reelle og virkelighedsnære situationer. Hvilket har styrket kvaliteten af afhandlingen og hele baggrunden heraf.

Strukturen og manuskriptet i de tre interviews tager udgangspunkt i følgende 4 punkter (Myers, M. D. et Al., 2006)

- Preparing the opening – introducing yourself
- Preparing the introduction – explaining the purpose of the interview
- Preparing the key questions
- Preparing the close

Det er gjort for at skabe et godt og dynamisk flow i interviewet og for at få så meget nyttig viden ud af det som muligt. Derfor blev der lagt stor vægt på introduktionen, da dette ansås for at være vigtigt i forhold til at få den interviewede til selv at få et indblik i vores problemstilling og ud fra dette kunne svare herefter. Der var dog ingen problemer i at få de interviewede til at svare meget dybdegående på alle spørgsmål.

Derfor er det i denne afhandling den kvalitative indsamlingsmetode, hvor der er sket en indsamling af empiriske data, der er gjort brug af. Den kvalitative metode er valgt, da den er velegnet til at indsamle bløde og dybdegående data med forklaringer (Eriksson og Kovalainen 2012). Ved udførelsen af en kvalitativ metode mødes interviewer og respondent oftest fysisk og fører en samtale om emnet. Derfor bliver man også nødt til i denne metode at være mere struktureret, hvorved intervieweren stiller spørgsmål og respondenten svarer (Eriksson og Kovalainen 2012). Derfor er den tidligere beskrevet metode fra Myers, M. D. et Al., 2006 valgt. Den kvalitative undersøgelsesmetode er anvendelig i denne afhandling, da de primære data er indsamlet for at få en forståelse af det valgte emne og den valgte problemstilling i praksis. På baggrund af dette giver det en mulighed for at få mere uddybende forklaringer om emnet og problemstillingen i praksis.

I forhold til interviewformen er der valgt at anvende en semistruktureret interviewtype, hvor der benyttes åbne spørgsmål. Der er dermed ikke en bestemt plan eller mulighed for at rykke samtalen over i andre relevante og interessante emner, som opstår under interviewet (Eriksson og Kovalainen 2012). Denne type interview er valgt ud fra, at der er et ønske om at få belyst problemstillingen og emnet ud fra, hvad den enkelte respondent finder særligt relevant i forhold til afhandlingens problemstilling og hvad der så i praksis gør sig gældende for dem.

Formålet med denne afhandling er ikke at foretage en statistisk generalisering. Det er dermed ikke nødvendigt at foretage en systematisk udvælgelse af respondenter (Eriksson og Kovalainen 2012) og derfor er der blevet anvendt en kvalitativ undersøgelsesmetode. Overordnet er der taget udgangspunkt i tre interviews på cirka en times varighed hver. De personer, der er valgt som respondenter, er nøje udvalgt i forhold til deres særlige faglige ekspertise inden for området. En advokat som er rådgivningsekspert inden for persondataret, er blevet interviewet, for at få en holdning fra en praktiker som arbejder indenfor forskellige brancher og med mange forskellige mennesker. Derudover er to juridiske databeskyttelsesansvarlige i to store danske virksomheder blevet interviewet. Juristerne er valgt på baggrund af deres faglige speciale og mulighed for at belyse deres praktiske tilgang af afhandlingens problemstilling. Interviewene er efterfølgende blevet transskriberet. Alle interviewene er blevet fuldt transskriberet, med undtagelse af tale, der ikke er relevant for emnet. Formålet med interviewene er at få en overordnet forståelse af alle respondenternes viden og erfaring med emnet, da dette dermed bruges til en løsning for problemstillingen og dermed giver et bedre resultat for denne afhandling.

1.3.1.2 Kildekritik
Der gøres i denne afhandling brug af en række forskellige kilder. Disse kilders pålidelighed kan være tvivlsomme på grund af subjektive holdninger fra fx interviewene, da deres forudsætning ikke er at løse problemstillingen, men belyse deres egne problematikker i organisationerne og deres svar kan dermed være farvet af deres egne holdninger. Ydermere kan der i de andre brugte kilder være en minimal tilknytning til afhandlingens problemstilling og emne.

Dog understøttes de kritiske kilder af relevante og valide kilder, som findes indenfor afhandlingens emne, som på den baggrund gør dem anvendelige for at belyse problemstillingen fra flere vinkler. Ydermere er interviewene kun et udtryk for én persons synspunkt i begge af de to virksomheder og ikke fra flere ledere eller medarbejdere. Interviewene er dermed blevet anvendt med forbehold for respondentens personlige erfaringer og holdninger og er dermed ikke et samlet udtryk for alle i den pågældende organisation.

1.4 Struktur
Med afsæt i den indledende del af denne afhandling er det først og fremmest relevant at finde frem til, hvad der ligger i forordningens artikel 25, stk. 1 og hvordan denne skal fortolkes af organisationerne. Dette bliver fremført i del 3 i denne afhandling. Herunder hvilke tiltag man i denne afhandling har antaget at være passende tekniske og organisatoriske sikkerhedsforanstaltninger i den nye lovgivning ud fra allerede gældende teori og tidligere afgørelser.

Efterfølgende er det derefter relevant at opnå implementeringen på bedst mulig vis ved hjælp af organisatorisk agilitet og dermed skabe det bedst mulige resultat for organisationerne fra starten. Dette bliver fremført i del 4. Som grundlag for resultatet af denne afhandling er det derfor yderligere relevant at inddrage viden fra den praktiske håndtering af implementeringen af databeskyttelse gennem design og ud fra dette finde frem til udfordringerne og eventuelle løsninger fra de tre interviews. Alt dette ender ud i en model til organisationerne med denne afhandlings anbefaling til, hvilke redskaber organisationerne skal bruge for at opnå organisatorisk agilitet, som fører videre til en succesfuld håndtering af forordningens artikel 25, stk. 1. Dette vil fremgå i diskussionen, som danner grundlag for den fremtidige effekt af både forordningen og modellen for organisatorisk agilitet (figur 5).

Del II – Teoretiske ramme
2.1 Persondatabeskyttelse
2.1.1 Baggrunden
Den teknologiske udvikling har spillet en stor betydning for brugen af persondata og der vil være en konstant bevægelse inden for dette område (Blume, 2017). Den teknologiske udvikling presser sig på fra alle kanter både inden og udenfor EU. De store cloududbydere og generelt alle IT-virksomheder, fra blandt andet USA, har været med til at skabe en mistillid til det enkelte individ og deres beskyttelse af persondata. Dette blev især belyst i sagen om Maximillian Schrems (herefter Schrems), som i 2015 vandt en sag mod Facebook i forhold til overførsel af personoplysninger fra Europa til USA (EU-kommissionen, 2015, sag-362/14). Sagen om Schrems' kamp mod Facebook udsprang ved opdagelsen af USA's overvågning af private personer, som whistlebloweren Edward Snowden lækkede i 2013 (Greenwald, G. og Poitras, L., 2013). Forordningen skal derfor danne grundlag for at genoprette tilliden mellem borgerne og bevægeligheden af data, og erstatter dermed det retlige grundlag fra det tidligere persondatadirektiv 95/46/EF (herefter direktivet). Direktivet

har været gældende ret siden 1995, og til trods for at det ikke nævner den teknologiske udvikling, har fortolkningen af direktivet reguleret persondatabeskyttelse i 20 år. Denne beskyttelse er dog ikke længere tilstrækkelig, hvorfor udviklingen af forordningen er blevet iværksat. Den teknologiske udvikling er i en konstant proces, som aldrig stopper, og borgernes anvendelse af digitale løsninger er ligeledes støt stigende. Af disse årsager er det fundamentalt for borgernes sikkerhed, at forordningen varetager sikkerhedstiltag samt beskyttelse af personoplysninger på internettet jf. forordningens præambel 5-7.

Udformningen af forordningen skal skabe og håndhæve tilliden hos borgerne ved blandt andet at sikre håndhævelse af reglerne samtidig med, at den følger med den teknologiske udvikling og skaber en større sikkerhed for behandling af persondata på tværs af landegrænserne og dermed en mere fri datastrøm og større brug af cloud-computing i Europa. Dette er en del af kommissionens strategi for det indre digitale marked, som har til formål at håndtere alle de største hindringer for udviklingen af grænseoverskridende online handel og andre grænseoverskridende digitale aktiviteter samt sikre, at EU-medlemsstater er i front med den teknologiske udvikling (Kommissionen, 2015). Forordningen beskriver dette i dens præambel 5-7, hvor den nævner vigtigheden af borgernes tillid, udviklingen af det indre digitale marked og forordningens formål med håndhævelsen af sikkerheden omkring borgernes persondata, som adskiller sig fra direktivet. Denne udvikling viste også hurtigt, at muligheden for systematisering og digitalisering af oplysninger om mennesker medførte, at oplysninger ikke lå fysisk mere, men at de nu er søgbare på tværs af alle landegrænser qua den stigende brug af cloud enheder (Thzaskowski, J. et. Al., 2017). Overordnet set er der et ønske fra kommissionen om, at der skulle ske en harmonisering af reglerne indenfor EU. Sikkerheden af harmoniseringen er især underbygget af, at der er tale om en forordning, der er gældende som den står og ikke skal tilpasses national ret (Mortensen, 2018).

Forordningen definerer betegnelsen af personoplysninger som værende enhver form for information, som kan henføres til en identificeret eller identificerbar fysisk person (herefter den registrerede), jf. forordningens artikel 4, stk. 1. Indikatoren af personoplysninger kan fx være navn, adresse, e-mail og andre almindelige oplysninger om personen. Derudover findes der følsomme personoplysninger såsom helbredsoplysninger, fagforeninger, seksuel præference, mf. jf. forordningens artikel 9, stk. 1. Ydermere regulerer forordningen automatisk og ikke-automatisk behandling af ovenstående personoplysninger, samt når behandlingen af europæiske personoplysninger udføres af en dataansvarlig eller af en databehandler, som befinder sig både inden og uden for Europas grænser, jf. forordningen, artikel 2 - 3.

Anvendelsen af artikel 25 er meget central i forordningen, da den er indsat i forordningen med henblik på at kunne sikre reguleringens tilpasning til den teknologiske og samfundsmæssige udvikling med det sigte at skabe databeskyttelse gennem design. Her menes, at man som dataansvarlig skal inkorporere databeskyttelse i IT-systemerne og i de organisationer, der anvender løsningerne. Formålet med artikel 25 er at skabe en regulering, hvor den dataansvarlige gennemfører passende tekniske og organisatoriske foranstaltninger som standardindstillinger for at sikre personoplysningerne, jf. forordningen, artikel 25, stk. 2. Den juridiske del af nærværende afhandling beskæftiger sig med at finde frem til det nærmere indhold af denne bestemmelse. Derfor er det yderst relevant at analysere hvilke tekniske og organisatoriske tiltag, der er tilstrækkelig under en betydning af ordet *passende*. Når man skal fastlægge det passende niveau for sikkerheden, skal der anlægges en holistisk betragtning, så man når hele vejen rundt med en passende sikkerhed (Dall, N. P., et al., 2016). Der er en tendens til, at man kun fokuserer på de tekniske foranstaltninger inden for sikkerhed, men det er yderst vigtigt at de organisatoriske, herunder de fysiske sikkerhedstiltag, tages i betragtning og håndteres i alle organisationer.

2.1.2 Databeskyttelsesdirektiv vs. Databeskyttelsesforordningen

Direktivet har været gældende ret i de sidste 20 år og erstattes af forordningen den 25. maj 2018. I forbindelse med at forordningen bliver gældende ret, er det interessant at understrege de forskelle, der er mellem direktivet samt dennes implementering i persondataloven og forordningen, der formentlig bliver suppleret af databeskyttelsesloven. Herunder fokuseres på kravene omkring databeskyttelse gennem design.

Som udgangspunkt fremgår der ikke nogen bestemmelser i direktivet, der er direkte med forordningens artikel 25, om databeskyttelse gennem design. Direktivet indeholder ikke bestemmelser, som eksplicit kræver databeskyttelse gennem design, dog er bestemmelsen afdækket i direktivet, hvor den opfordrer de dataansvarlige til at gennemføre databeskyttelse gennem design. Det kan også fremhæves, at der er en tilsvarende bestemmelse i persondataloven, som er implementeret på baggrund af direktivet, som opfordrer til ovenstående, jf. direktivets artikel 17 og persondatalovens §41, stk. 3.

I kommissionen er der sammensat en gruppe, som skal sikre og vejlede om databeskyttelse, kaldet artikel 29-gruppen, som består af repræsentanter fra hver EU-medlemsstat. Gruppen vil fortsat eksistere efter 25. maj 2018, omend den omdannes til Databeskyttelsesrådet, og får tildelt en række yderligere beføjelser. I en udtalelse fra artikel 29-gruppen står om forholdet mellem de tidligere og fremtidige regler, at direktivets artikel 17 indeholder en tilsvarende tankegang som forordningens artikel 25. Dette er også lagt til grund i den danske betænkning om forordningen, hvor der blandt andet står:

> *"…at databeskyttelsesdirekivet indeholder flere bestemmelser, som opfordrer de dataansvarlige til at gennemføre teknologibeskyttelsesregler i forbindelse med både design og drift af informations- og kommunikations teknologier. Artikel 29-gruppen nævner bl.a. direktivets artikel 17, hvor der fastsættes en forpligtelse for den dataansvarlige til at gennemføre passende tekniske og organisatoriske foranstaltninger."* (Betænkning nr. 1565, side 410.)

Ovenstående citat henviser således også for dansk rets vedkommende til direktivets artikel 17, som forpligter medlemsstaterne til at fastsætte bestemmelser om, at den registreringsansvarlige skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger. Betydningen må være, at direktivets artikel 17, stk.1, må fortolkes som værende en bestemmelse, der beskytter personoplysninger mod tilintetgørelse og tab af data, mod delingen af data og udefrakommendes adgang til data i organisationen, især hvis dette forekommer over internettet (direktivet 95/46/EF, artikel 17, stk. 1). For dansk rets vedkommende kan henvises til, at der af persondatalovens §41, stk. 3 fremgår, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske foranstaltninger, som er implementeret fra direktivets artikel 17.

Dermed fremgår det af ovenstående bestemmelser, at der i et vist omfang ønskes databeskyttelse gennem design indfortolket i direktivet og persondataloven, omend der i den tidligere regulering kun opfordres til, at den dataansvarlige skal iværksætte et databeskyttelsesdesign, hvorimod forordningen kræver en gennemførelse heraf. Det vil sige, at forordningens artikel 25 ikke i sig selv etablerer nye krav til den dataansvarlige, idet dette allerede følger af direktivet og databeskyttelsesloven. Den reelle forskel er håndhævelsen af efterlevelsen af kravet om databeskyttelse gennem design (Betænkning nr. 1565). Fremover vil det blive sanktioneret, såfremt den dataansvarlige ikke sikrer både tekniske og organisatoriske sikkerhedsforanstaltninger ved implementeringen af IT-systemer men også under brugen af IT-systemet.

2.2 Den organisatoriske agilitet

2.2.1 Hvad er agilitet?

Ordet ”agilitet” refererer til evnen til at være fleksibel og hurtigt at kunne tilpasse sig ændrede betingelser. Ordet er af latinsk oprindelse, og stammer fra ordet ”agilis” som betyder at bevæge, handle, gøre, udrette, administrere og at opnå (DSL, 2018). Essensen af at være agil bygger på evnen til at kunne bevæge sig hurtigt og let samt at kunne skifte retning og tage et skarpt sving (Vocabulary.com Dictionary, 2018). De nuværende konkurrenceforhold er præget af højintensiv rivalisering i et dynamisk og usikkert miljø. Evnen til at reagere hurtigt og effektivt på disse ændringer er en nødvendighed, der adskiller vellykkede organisationer fra dem, der fejler (Harraf, A., 2015). Især når der sker ændringer i form af implementering af forordningen, som nærværende afhandling beskæftiger sig med, er der et stort behov for, at en organisation behersker den agile håndtering.

> *”Without exception, all of my biggest mistakes occurred because I moved too slowly.”*
> John Chambers, Cisco CEO (Harraf, A., 2015).

Begrebet ”agilitet” anvendes i denne afhandling i et erhvervsøkonomisk perspektiv til at beskrive en organisations omstillingsparathed samt evnen til at håndtere uforudsete situationer i forsøget på at tilpasse alle dele af organisationen lige fra medarbejdernes arbejdsgange til næste træk på det strategiske niveau. Det gælder om at opbygge en organisationskultur, der understøtter hyppige ændringer og kæmper mod den iboende modstand mod forandringer, som eksempelvis kan opstå hos medarbejderne. Viden, empowerment og træning af medarbejderne er værktøjerne, hvilket viderebehandles i de erhvervsøkonomiske afsnit. Agilitet fra en organisations synsvinkel handler således om adræthed (Fløe, P., 2014).

Der findes flere forskellige former for agilitet. Overordnet set bevæger man sig inden for organisatorisk agilitet, som er udgangspunktet i denne afhandling, da man i implementeringen af databeskyttelse gennem design skal omfavne hele organisationen i alle led og ikke kun de forskellige informationssystemer og forretningsprocesser, som er de andre led i agilitet. Vælger man kun at undersøge en agil software udviklingsmetode eller agilitet i forretningsprocesserne, kommer man i sin implementering til at mangle håndteringen af medarbejderne og deres forandringsproces.

2.2.2 Historisk udvikling af agilitet

Agilitet er i det 21. århundrede ikke længere et valg for organisationerne. Organisationernes adræthed og kompetence til at reagere skiftende til det eksterne miljø er blevet en nødvendighed for at kunne bibeholde succes i organisationerne. Med hurtig udvikling på det globale marked og med konstant nye forandringer er det vigtigt, at organisationerne kan være fleksible og dermed kunne reagere hurtigt på de konstante forandringer der sker på markedet (Harraf et. Al., 2015).

Årsagen til, at organisationer skal have en agil tilgang, begrundes med den hurtigt skiftende teknologi, mindskelse af risici, det skiftende miljø og forventningerne fra kunderne. Alle disse drivkræfter er hele tiden i bevægelse. For at opnå succes i disse hurtigt skiftende drivkræfter er agilitet en af de vigtigste spillebrikker. Udviklingen har ydermere gjort, at agilitet kan blive et konkurrenceparameter for mange organisationer, og derfor må det anses for at være en tilgang, der er i vækst i de forskellige organisationer (Crocitto et. Al., 2003).

En agil tilgang kræver både en strategisk og en mental turn-around – især på ledelsesniveauet. Ud fra dette udgangspunkt findes der nogle grundprincipper inden for agilitet, som stammer fra udviklingen af metoden omkring den agile softwareudvikling, hvor man har taget udgangspunkt i disse og inkorporeret dem til alle andre processer i organisationerne, selvom det ikke har været en

IT-udvikling, man har villet opnå. Det stammer fra ønsket om at opnå en udbredelse af teamarbejde, teamets fælles mål og den "empowerment" af medarbejdere "på gulvet", der har givet rigtig mange softwarevirksomheder et løft. Grundprincipperne indenfor den mere organisatoriske agilitet frem for den agile softwareudviklingsmetode er (Fløe, P., 2014):

- at der skal ske en radikal ændring i managementstrategien og tilgangen hertil, samt en klar og fælles enighed om skabe den bedste værdi for kunden,
- at der skal ske en ændring i lederrollen fra, at man har ledelse på micro-management niveau til, at man får skabt mere selvorganiserede og selvledende teams,
- at koordinere opgaver på en helt anden måde og skabe en fælles accept og forståelse af, at de ændringer, justeringer og fejltagelser, der sker, ikke er en dårlig ting, men en nødvendighed for at holde trit med den ekstrem hurtige udvikling, der sker omkring en og de pludselige skift, der forekommer,
- at der sker en ændret tilgang til planlægning og opnåelse af en fælles forståelse for, at planlægning er essentiel,
- at der er et muligt behov for justeringer af nogle grundværdier, så organisationen hele tiden bakker op om principperne om de kontinuerlige forbedringer, læring og total transparens og
- at der kan være behov for en anden form for kommunikation, hvor der i en agil organisation skabes kommunikation horisontalt i stedet for vertikalt.

Ovenstående grundprincipper skal dermed danne grundlag for ledelsestilgangen til ens medarbejdere under implementeringen af databeskyttelse gennem design i organisationen.

Selvom der i denne afhandling er fokus på implementeringen af databeskyttelse gennem design og ikke et direkte produkt til kunderne, så må ovenstående antages også at være gældende her, da man som kunde måske ikke vil bruge eller handle med organisationen, hvis man ikke har styr på overholdelsen af forordningen. Påvirkningen af implementering af forordningen vil variere fra branche til branche, da det må antages at påvirke en produktionsvirksomhed i mindre grad, end det vil påvirke organisationer inden for service og det offentlige. Den agile tankegang fordres til at få medarbejderne til at ændre deres arbejdsgange og rutiner samtidig med, at det ikke må gå ud over det endelige produkt. I det følgende vil der blive gennemgået 12 drivkræfter, som på hver deres måde underbygger og støtter op om den agile aktivitet en i en organisation. De 12 drivkræfters relevans ved implementering af forordningen vil blive diskuteret senere i nærværende afhandling, hvor de mest relevante drivkræfter tilsammen danner et framework for organisatorisk agilitet (se del V).

2.2.3 Drivkræfter i organisatorisk agilitet

#	Drivkraft:	Definition:
1	Culture of Innovation (Harraf et. Al., 2015)	Forandringsparathed bruger eksterne drivkræfter til at fordre forandring. Det er evnen til at gøre nye ting og evnen til at gøre gamle ting på nye måder.
2	Empowerment (Harraf et. Al., 2015)	Forholdet mellem ledere og medarbejdere. Det vigtige i denne drivkraft er effekten af valget af decentralisering og centralisering i forhold til beslutninger.
3	Tolerance for Ambiguity (Harraf et. Al., 2015)	Agile organisationer skal fungere selv i lyset af en tvetydighed. Denne drivkraft repræsenterer en organisations overordnede tankegang, hvor en kultur overskrider organisationens niveauer og grænser.
4	Vision (Harraf et. Al., 2015)	Kortfattet redegørelse af hvordan organisationen hver dag arbejder for at opnå mål. Den definerer organisationens mest optimale fremtidige mål.
5	Strategic Direction (Harraf et. Al., 2015)	Karakteristika for succesfulde visioner, hvor der er et skarpt og tydeligt fokus, som giver en organisation en klar strategisk retning.
6	Change Management (Harraf et. Al., 2015)	Forandringsledelse har direkte tilknytning til en organisations vision, som styrer organisationens overgang fra sin nuværende placering til et ønsket fremtidigt mål.
7	Communication (Harraf et. Al., 2015)	Kommunikation i en organisation er altafgørende for at opnå fleksibilitet. Beslutningstagning, ledelsesfunktioner og overordnet ledelseseffektivitet er kun mulig gennem de forskellige kommunikationskanaler.
8	Operations Management (Harraf et. Al., 2015)	Udvidelse af nogle af de organisatoriske kapaciteter, er altid forbundet med øget fleksibilitet inden for en organisation. Forandring skabes kontinuerligt, hvor der ikke er fleksibilitet i sig selv.
9	Structual Fluidity (Harraf et. Al., 2015)	Organisationsstruktur er den ledende ramme, der primært driver en organisations præstationer og etablerer de forbindelser og kommunikationskanaler, der har stor indflydelse på organisationens vision og skabelsen af fleksibilitet.
10	Development of organizational learning (Harraf et. Al., 2015) (Nijssen, M., 2012)	En kompetence for agile organisationer er hurtig organisatorisk indhentning af viden. At have en fornemmelse for markedet til at kunne respondere hurtigt, korrekt og effektivt. Håndtering af viden vurderes som vigtige aktiver i en organisations aktivstruktur. En læringsorganisation søger løbende at effektivisere samtidig med, at de samlede organisatoriske processer forbedres.
11	Scalable workforce (Nijssen, M., 2012)	Med en skalerbar arbejdsstyrke ser man på, hvor de menneskelige ressourcer konfigureres og transformeres.
12	Highly adaptable organizational infrastructure (Nijssen, M., 2012)	Den organisatoriske infrastruktur er nøglen til koordinering og integrering af aktiviteter og implementering af ressourcer. Det skaber en stærk og agil infrastruktur som en kompetence til organisationer.

Tabel 1. Kilde: Egen tilvirkning.

2.2.3.1 Culture of Innovation
Innovationskultur er grundlæggende inden for agilitet. En organisation med en velfungerende innovationskultur er ikke udfordret af forandring. En velfungerende innovationskultur indebærer, at en organisation løbende vurderer sine systemer, strukturer, procedurer og teams. Sammenlagt er dette knyttet til forandringsledelse, hvor innovation er en gnist, der stimulerer forandring. En innovationskultur er brugen af ændringer i det eksterne miljø for bedre at forme organisationens interne miljø.

> *"Det er evnen til at gøre nye ting og evnen til at gøre gamle ting på nye måder"* (Harraf et. Al., 2015).

Innovation, især i industrier med hurtig forandring, er af stor betydning. Mere specifikt er det en kultur af innovation, snarere end innovation selv, der er afgørende for organisationers succes og fleksibilitet.

Innovationskultur er karakteriseret ved en efterspørgsel af muligheder og generel opmærksomhed. Organisationen skal som helhed fremskønne et internt behov for at opdage nye muligheder for innovation, heriblandt være aktiv i at finde og handle på disse opdagelser. Endvidere skal organisationer være rede til at udnytte nye muligheder og skabe en konkurrencemæssig fordel og dermed have en åben tilgang for nye erfaringer og opretholde kreativitet. Innovationskulturen er tæt linket til det eksterne miljø og organisationens strategiske mål. Dette er en understregning af, at agilitet er et koncept i konstant bevægelse, som tilpasser sig forskellige miljøer, organisationer og virksomhedsbehov. Erfaring tyder på, at organisationer, der prioriterer innovation, har større chance for at opnå succes gennem de yderligere dirvkræfter i agilitetens framework (Harraf et. Al., 2015).

2.2.3.2 Empowerment
Empowerment er en drivkraft, der beskriver forholdet mellem ledelse og medarbejdere baseret på autoritet. Det handler om, hvordan organisationens ledere deles i forhold til medarbejderne på de forskellige niveauer i organisationen. Det mest grundlæggende i denne drivkraft er decentralisering i forbindelse med forholdet mellem ledere og medarbejdere. Herunder hvorvidt beslutningstagning er fordelt i organisationen.

Organisationer med decentrale strukturer har en tendens til at være mere fleksible og bedre i stand til at reagere på ændringer i det eksterne miljø. Når en medarbejder på et lavere niveau har fået tildelt en autoritet eller en medbestemmelse, sker der oftere og hurtigere en mere præcis reaktion på de forandringer, der måtte hænde fra både det interne og eksterne miljø. Dette medfører, at der i krisetider kan træffes en hurtigere beslutning på det øverste ledelsesniveau, som resulterer i en hurtigere udførelse. Decentralisering viser sig derfor ofte at være mere effektiv, da fordelen og effekten af beslutningstagning på det lavere niveau hos medarbejderne, og organisationens lydhørhed som helhed, medfører øget effektivitet og større ejerskab hos medarbejderne. En decentralisering og medbestemmelse i beslutningsprocessen, øger generelt organisationens overordnede fleksibilitet, end ved en centralisering (Harraf et. Al., 2015).

2.2.3.3 Tolerance for Ambiguity
Agile organisationer skal fungere selv i lyset af en tvetydighed. Denne drivkraft er tæt forbundet med drivkræften om innovationskultur, da den repræsenterer en organisations overordnede tankegang, hvor en kultur bevæger sig på tværs af organisationens niveauer og grænser. Langt de fleste markeder er præget af uforudsigelighed og der er dermed ikke én korrekt reaktion til det eksterne miljø, da der kan opstå skiftende behov for løsninger på forskellige tidspunkter. Derfor er fleksibilitet en afgørende drivkraft. En organisation skal være parat til at identificere ændringer og reagere på dette. Derfor er denne drivkraft vigtig, da det essentielle her er tolerancen for tvetydighed,

som kan forekomme i en organisation. Det kan være udfordrende at finde frem til brugbar data for en organisation, da de fleste markeder består af en overflod af information og viden. Det er ydermere et vigtigt element i denne drivkraft, at der er en forståelse for, at en konkurrents erfaringer kan være behjælpelige. Hvis en konkurrerende organisation står i samme situation, (fx ved implementering af forordningen som fremhæves i denne afhandling) hvor alle skal opfylde de samme lovkrav vedrørende databeskyttelse, kan det være svært at gennemskue, hvorledes den enkelte organisation skal reagere. Derfor kan vidensdeling være en stor hjælpe for de pågældende organisationer på markedet. Dette øger tvetydigheden i forhold til den globale konkurrence (Harraf et. Al., 2015).

2.2.3.4 Vision

En organisations vision er en kortfattet redegørelse for, hvorledes en organisation hver dag arbejder for at opnå deres mål. Det er den, der definerer en organisations optimale fremtidige mål. Dens primære funktioner er at inspirere organisationen. Inden for rammerne af fleksibilitet omfatter visionen ikke kun den skriftlige eller formidlede beskrivelse af organisations mål, men også midlerne og metoderne til at etablere samt gennemføre organisationens vision. Dette omfatter en professionel ledelse, der styrer og leder organisationen. En klar og tydelig vision er altafgørende for en organisations succes. Dette begrundes med, at det skal give lederne og medarbejderne et overordnet mål at arbejde henimod både kollektivt og konstant. Der er en klar forbindelse mellem denne drivkraft, innovationskultur (afsnit 2.2.3.1) og forandringsledelse (afsnit 2.2.3.6). I forhold til agilitet skal visionen være enkel, med klare formål og principper, da dette resulterer i en mere fordelagtig adfærd i hele organisationen frem for komplekse regler, som giver anledning til en adfærd, der modarbejder visionen (Harraf et. Al., 2015).

2.2.3.5 Strategic Direction

En organisations overordnede retning er etableret i visionen. Herunder er engagementet i ledelsens fokus på at nå det ønskede optimale mål med succes afgørende for organisationens succes. At have fokus gør i sidste ende ikke en organisation mere fleksibel, men det er handlingerne baseret på dette fokus, der bliver gjort for at opfylde visionen, som skaber succes. Ved ledelsens fokus omfatter det kommunikation og efterlevelse heraf på ledelsesniveauet, for at opnå visionen og dermed adskiller man sig som agil organisation fra andre. Organisationer, der fejler, har ofte ikke et fokus, hvilket gør dem ineffektive, uinspirerede eller ikke-eksisterende. Karakteristika for succesfulde visioner er, hvor man har et skarpt og tydeligt fokus, som giver en organisation en klar strategisk retning. Når der er en klarhed af retningen, hjælper det en organisation med at reagere på en fleksibel og effektiv måde, da man derved etablerer vejledende rammer for beslutninger, der reagerer på eksterne drivkræfter. Godt lederskab er det primære element for denne drivkraft og håndhævelsen af en organisations engagement i dets vision (Harraf et. Al., 2015).

2.2.3.6 Change Management

Forandringsledelse har en direkte tilknytning til en organisations vision, som styrer organisationens overgang fra sin nuværende placering til et ønsket fremtidigt mål. En fleksibel organisation er en, der med held kan klare forandring og være opmærksom på arten af ændringer, der forekommer i og omkring sig selv (Harraf et. Al., 2015). Det er en klar faktor, at ændring er uundgåelig. Forandring vil komme og vil påvirke organisationer væsentligt. Som alle de tidligere drivkræfter skaber forandringsledelse en fleksibilitet og unikhed for organisationer.

Organisatoriske beslutninger fører direkte til interne ændringer, når det er nødvendigt. Udover dette kan beslutninger udenfor en organisation også føre til pludselige forandringer. Ændringer i

det eksterne miljø kan komme fra forbrugernes beslutninger og præferencer, statslige beslutninger vedrørende politik eller regulering eller andre beslutninger. I nærværende afhandlings tilfælde er det forandringer inden for reguleringer i hele Europa, som påvirker hvert medlemsland, men også omliggende lande.

Forandringsledelse i agile organisationer består af tre dele, herunder opfattelse af ændringen, implementering af ændring og testændring. Opfattelsen af ændringen vedrører en organisations forudsætning for at afdække potentielle ændringer, både interne og eksterne. Det fremhæver også hurtigheden og nøjagtigheden af ændringsperspektivet. Gennemførelsen af ændringen er processen, hvor en beslutning fører til gennemførlige resultater. Agile organisationer får ændringer implementeret hurtigere, nemmere og mere præcist end en mindre fleksibel organisation. For at dette skal ske, skal ledere imidlertid være opmærksomme på beslutningsprocessen, herunder drivkræften om vision (afsnit 2.2.3.4), teambuilding og kommunikation (afsnit 2.2.3.7). For at skabe en mere agil organisation kræves det dermed i denne drivkraft omkring forandringsledelse, at organisationen er i stand til at afbalancere de forskellige komponenter i flere drivkræfter i overensstemmelse med deres organisations behov (Harraf et. Al., 2015).

2.2.3.7 Communication

Kommunikation i en organisation er altafgørende for at opnå fleksibilitet. Beslutningsprocesser, ledelsesfunktioner og overordnet ledelseseffektivitet er kun muligt gennem de forskellige kommunikationskanaler. Det vil sige, at når en leder får en idé eller træffer en beslutning, skal den formidles gennem en organisation for at kunne håndteres og indarbejdes af medarbejderne i organisationen. Intern kommunikation reagerer på de veje, hvorved information cirkuleres gennem en organisation. Der er tre primære retninger, hvor kommunikationskanaler findes. Disse er top-down, horizontal og bottom-up kommunikation. De mest succesfulde og tilsvarende mest agile organisationer er i stand til at kombinere disse kommunikationsmetoder effektivt, som skaber en åben kommunikation gennem en organisation.

Udover den formelle strategiske kommunikation til medarbejdere eller interessenter er organisationens uformelle sprog en forudsætning for vækst og strategisk agilitet, som skaber fleksibilitet. Uformel kommunikation inden for organisationen letter klarheden i organisationen og dens beslutninger. Teambuilding har en klar sammenhæng med denne drivkraft, da implementeringen af teams er typisk forbundet med decentralisering, da teams dermed bliver mere ansvarlige for beslutningstagning og succesen. En organisations tendens til at implementere eller udnytte teams har indflydelse på organisationens overordnede fleksibilitet. Indholdet af denne drivkraft er prioritering af holdaktivitet af specifikke opgaver. Udnyttelse af teams er en effektiv metode til bedre at engagere medarbejdere og reducere modstand mod forandring. Mens holdaktivitet kan øge mængden af tid, der kræves for at træffe en beslutning, har kvaliteten af beslutninger i teams en meget højere afgørende effekt. Disse bør derfor være et klart element i en organisations opbygning af agilitet (Harraf et. Al., 2015).

2.2.3.8 Operations Management

Generelt er meget af det en organisation forsøger at opfylde, direkte relateret til effektivitet og operationel ledelse inden for rammerne af organisatorisk agilitet. De organisationer, der konsekvent opfører sig aktivt, herunder engagerer sig i aktiviteter, er afgørende for at styre effektiviteten. For at udvide nogle af de organisatoriske kapaciteter, der altid er forbundet med øget fleksibilitet inden for en organisation, må man forstå, at der kontinuerligt skal skabes forandring, hvor der ikke er fleksibilitet i sig selv mere. Med det i mente kræves der en anvendelse af denne drivkraft til at

muliggøre organisatorisk agilitet, som må antages kun at være en lille udvidelse af det, der allerede er velkendt for driftsledere (Harraf et. Al., 2015).

2.2.3.9 Structural Fluidity

Dette koncept vedrører måder, hvorpå arbejdet påbegyndes, udføres og afsluttes. Organisationsstruktur er den ledende ramme, der primært driver en organisations præstationer og etablerer de forbindelser og kommunikationskanaler, der har stor indflydelse på organisationens vision og skabelsen af fleksibilitet. Organisationer har en tendens til at være flade uden at være kundefokuseret, procesorienteret og teambaseret. Disse karakteristika, selvom de er forskellige i det unikke anvendelsesområde til forskellige organisationer, er kernen af agilitet. Endvidere viser disse egenskaber strukturens funktion og forhold til andre forskellige attributter af agilitet. Fladere organisationer har for eksempel tendens til at fremme bottom-up og horisontal kommunikation, mens manglen på strukturelle grænser muliggør lydhørhed og samtidig øger en organisations tolerance for tvetydighed. Organisatorisk fluiditet fremhæver betydningen af fleksibilitet for at gøre det muligt for en organisation at være adræt (Harraf et. Al., 2015).

2.2.3.10 Development of organizational learning

En læringsorganisation søger løbende at effektivere, samtidig med at de samlede organisatoriske processer forbedres. Forskning definerer to læringsmetoder: single og double loop (Harraf et. Al. 2015). Ved single loop learning vil man gerne forbedre gennem foranstaltninger og metoder, der tidligere er blevet anvendt. Kontinuerlige forbedringer er i fokus. Man skal dog have i mente, at ved målene for single loop learning bliver der sjældent stillet spørgsmålstegn og organisationen fokuserer ubevidst på specifikke mål. I modsætning til ovenstående er der ved double loop learning fokus på medarbejdere på alle organisatoriske niveauer, hvor man løbende prøver at udfordre organisationens praksis. Den sidste nævnte metode i forhold til læring er mere almindeligt anvendt for agile organisationer, da behovet for løbende forbedring under denne læringsstil hverken bliver ødelagt eller begrænset af organisationens begrænsende tankegang.

En kompetence for agile organisationer er hurtig organisatorisk indhentning af viden. (Nijssen, M. et. Al., 2012). At have en fornemmelse for markedet til at kunne respondere hurtigt, korrekt og effektiv håndtering af viden vurderes som vigtige aktiver i en organisations aktivstruktur. Dette gør sig også gældende, når der er tale om implementering af den nye forordning, som for en organisation kræver stor viden for netop dette område, for at skabe en agil håndtering heraf. Konstant at opnå og skabe organisatorisk viden er meget vigtigt i et agilt miljø. Uden dette ville en organisations videnskabelse hurtigt blive forældet. Essensen består i at være i stand til at underbygge evnen til konstant at skabe, tilpasse, distribuere og anvende viden (Dyer og Ericksen, 2006).

2.2.3.11 Scalable workforce

Med en skalerbar arbejdsstyrke, ser man på, hvor de menneskelige ressourcer konfigureres og transformeres, som kan føre til risiko for tab af viden. Så snart et menneskeligt element spiller ind, kan dette være med fare for ukorrekte arbejdsgange. Endnu vigtigere kan det føre til afbrydelse af social kapital (medarbejderens sociale netværk og unikke relationer), der er vigtige for at skabe ny viden. Dette er absolut en afgørende kompetence, når det kommer til at skabe databeskyttelse gennem design som en del af deres organisatoriske agilitet. Hvis ikke de ansatte i en organisation er beredt på en skalerbar hændelse som fx implementering af den nye forordning, er det med stor sandsynlighed en mangelfuld organisation, når det kommer til den agile tilgang. Når der skal ændres eller reguleres på arbejdsgange ved implementering af den nye forordning, er dette for en

organisation med en skalerbar arbejdsstyrke et kæmpe tillæg for den agile understøttelse (Dyer og Ericksen, 2006).

2.2.3.12 Highly adaptable organizational infrastructure
Den sidste agile drivkraft for en organisation er at opretholde en agil struktur, som bygger på en forudsætning for arbejdskraftens skalerbarhed om en meget tilpasningsbar organisatorisk infrastruktur. Den organisatoriske infrastruktur er nøglen til koordinering og integrering af aktiviteter og implementering af ressourcer. Dette skaber en stærk og agil organisatorisk infrastruktur som en kompetence til organisationer (Dyer og Ericksen, 2006).

Kompetencer for agile organisationer giver anledning til at rette opmærksomheden mod de mulige organisationspraksis i forbindelse med kompetencerne. Agilitet er blevet undersøgt på tværs af forskellige fagområder, såsom forretningsagilitet, it-agilitet, fleksibel produktion og fleksible forsyningskæder. At se organisatorisk agilitet ud fra et dynamisk kapacitetssynspunkt er et ret nyt felt, især når man fokuserer på HR-aspekterne af denne dynamiske kapacitet (Nijssen, M., 2012). Som guide til fremtidig praksis vil der i denne afhandling blive udviklet og diskuteret metoder til anvendelse af implementering af databeskyttelse gennem design som en del af organisatorisk agilitet (del III, del IV og V).

De relevante organisatoriske kompetencer nævnt ovenfor skal tilpasses organisationens mål og strategi. Disse mål og strategien er i konstant bevægelse i et dynamisk miljø. Dette gør sig især gældende ved implementering af den nye forordning, da der her ikke blot er tale om en enkeltstående aktivitet, men derimod en iterativ proces, som efter implementering både kræver opfølgning og kontrol. Derfor er det essentielt for en organisation at bestride ovestående kompetencer, førend det bliver en succesfuld implementering for organisationen som helhed (Nijssen, M., 2012).

Del III - Juridiske ramme – Databeskyttelse gennem design

3.1 Oprindelsen af databeskyttelse gennem design

3.1.1 De 7 principper om databeskyttelse gennem design

Dr. Ann Cavoukian er anerkendt som en af verdens førende eksperter inden for beskyttelse af personoplysninger. Hun er skaberen af konceptet ”Databeskyttelse gennem design - The 7 Foundational Principles”, som er en metode, der hjælper til proaktivt at beskytte personoplysninger gennem designspecifikationer for informationsteknologier, netværksinfrastruktur og forretningspraksis. De syv principper om databeskyttelse gennem design fungerer som en referenceramme og kan anvendes til udvikling af mere detaljerede kriterier for beskyttelse af persondata. De universelle principper i Fair Information Practices (FIP) bekræftes af de 7 principper om databeskyttelse gennem design, men går ud over dem for at søge den højeste globale standard. FIP er en generel betegnelse for et sæt standarder, der styrer indsamling og brug af personoplysninger og behandler spørgsmål om privatlivets fred og nøjagtighed (Cavoukian, A., 2011).

Værdien af data og behovet for at kontrollere ansvarlige og civiliseret brug af data er steget dramatisk. Den frembrusende innovation, globale konkurrence og stigende systemkompleksitet udfordrer beskyttelsen af persondata. Men vi kan ikke blot udelukke os fra ovenstående udfordringer for at beskytte vores data, da vi gerne vil nyde godt af fordelene ved innovationen - nye bekvemmeligheder og effektivitet. Gennem de seneste år har anvendelsen af personoplysninger gennemgået en rivende udvikling til vores nutidige informationssamfund. Derfor er det gennem forord-

ningen et krav, at data beskyttes med henblik på en effektiv implementering af databeskyttelsesprincipperne, for at samfundets udvikling ikke bliver til fare for personoplysningers sikkerhed (Cavoukian, A., 2010).

Der er en stigende forståelse for, at innovation, den globale konkurrence og den øgede systemkompleksitet skal tilgås ud fra et perspektiv om "design-tænkning" inden for sikkerhed af personoplysninger. Derfor udspringer den måde, hvorpå beskyttelsen af privatlivets fred skal håndteres fra samme design-tænkningsperspektiv. Dette betyder, at fortrolighed og andre tiltag skal indarbejdes i netværksdatasystemer og teknologier som standard. Dette gælder enhver standard, protokol og proces, der berører de registreredes liv. Fortrolighed skal ligeledes integreres i organisatoriske prioriteter, projektmål, designprocesser og planlægning. De syv principper af Dr. Ann Cavoukian søger derfor at muliggøre den fornødne sikkerhed ved at etablere en universel, processuel orienteret ramme for et design med den stærkeste beskyttelse af privatlivets fred, der er tilgængelig i vores samfund. Principperne vil blive beskrevet i det følgende (Cavoukian, A., 2010).

3.1.1.1 Princip nr. 1: Proactive not Reactive; Preventative not Remedial
Det første princip beror på, at proaktiviteten vælges frem for reaktiviteten. Uanset om det anvendes til informationsteknologier, organisationspraksis, fysisk design eller netværksinformationsøkosystemer, begynder Databeskyttelse gennem design med en eksplicit anerkendelse af værdien og fordele ved proaktivt at vedtage stærke tiltag til beskyttelse af privatlivet tidligt og konsekvent. Denne tilgang er karakteriseret ved proaktive snarere end reaktive foranstaltninger. Den tidligere identifikation af privatlivshensyn skal sikre, at der skabes de nødvendige sikkerhedsforanstaltninger for at sikre personoplysninger, før der sker misbrug heraf. Den proaktive tilgang kan understøttes ved at engagere sig på højeste niveau for at identificere, fastsætte og håndhæve høje standarder for at opretholde sikkerheden for personoplysninger. Det handler ligeledes om at etablere metoder til at genkende manglende sikkerhed, og korrigere eventuelle negative virkninger, inden de foregår på proaktive, systematiske og innovative måder.

3.1.1.2 Princip nr. 2: Privacy as the Default
At håndtere personoplysninger sikkert som en standard er et princip, som højner datasikkerheden. Databeskyttelse gennem design søger at levere den maksimale grad af sikkerhed af personoplysninger ved at garantere, at personoplysninger automatisk beskyttes i et givet IT-system eller forretningspraksis. Hvis en person ikke gør noget, forbliver deres privatliv intakt. Ingen handling er påkrævet af den enkelte for at beskytte deres privatliv - det er som standard indbygget i systemet.

Dette princip om databeskyttelse gennem design, kan betragtes som Privacy for Default, er særligt understøttet af følgende Fair Information Practices (FIP):

- **Formålsspecifikation:** Formålet, med hvilke persondata der indsamles, anvendes, bevares og offentliggøres, skal meddeles til den registrerede. Dette skal senest ske på det tidspunkt hvor oplysningerne indsamles.

- **Indsamlingsbegrænsning:** Indsamlingen af persondata skal være fair, lovlig og begrænset til det, der er nødvendigt for det angivne formål.

- **Dataminimering:** Indsamlingen af personligt identificerbare oplysninger bør holdes på et strengt minimum. Udformningen af programmer, informations- og kommunikationsteknologier og systemer bør begynde med ikke-identificerbare interaktioner og transaktioner som standard. Hvor det er muligt bør identificerbarhed, observerbarhed og sammenkobling af persondata minimeres.

- **Anvendelse, opbevaring og offentliggørelse begrænsning:** Anvendelse, opbevaring og offentliggørelse af persondata skal begrænses til de relevante formål, der er identificeret til den enkelte, for hvilken han eller hun har givet sit samtykke, medmindre andet er fastsat i loven. Persondata skal kun opbevares så længe som nødvendigt for at opfylde de angivne formål og derefter destrueres på forsvarlig og sikker vis. Hvor behovet for eller brugen af persondata ikke er klart, skal der være en formodning om privatlivets fred, og forsigtighedsprincippet skal gælde.

3.1.1.3 Princip nr. 3: Privacy Embedded into Design

Databeskyttelse gennem design er, som ordlyden fortæller, sikkerhed som bygger på design. Dette indebærer indtænkning af sikkerhed ved opbygning af strukturen og arkitekturen af it-systemer og forretningspraksis. Resultatet heraf er, at beskyttelse af personoplysninger bliver en væsentlig del af den kernefunktionalitet, der leveres. Databeskyttelse er således en integreret del af systemet uden at formindske funktionaliteten. For at inkorporere beskyttelse af personoplysninger, skal it-systemerne opbygges på en holistisk, integreret og kreativ måde. Denne holistiske tilgang betragtes som nødvendig, da det brede perspektiv er vigtig i forbindelse med at en videnskabsteoretisk retning, der lægger vægt på at betragte fænomener som helheder, snarere end som sammensatte enkeltdele. At IT-systemerne skal opbygges på en integreret måde, begrundes ud fra et perspektiv om, at alle interessenter og interesser bør høres og varetages. Den kreative del af at skabe et IT-system som tager hånd om personoplysninger, er nødvendig, fordi indlejring af privatlivets fred i nogle tilfælde betyder at genfinde eksisterende valg, fordi alternativerne er uacceptable.

3.1.1.4 Princip nr. 4: Full Functionality – Positive-Sum, not Zero-Sum

Databeskyttelse gennem design søger at imødekomme alle legitime interesser og målsætninger på en positiv "win-win" tilgang, hvor unødige afvejninger ikke foretages. For at gennemføre en succesfuld beskyttelse af personoplysninger, er det ikke et ønske at sætte beskyttelsen af data op mod sikkerheden. Det er i denne situation en kombination af begge disse elementer, som skal skabe et positivt resultat sammen. Databeskyttelse gennem design gør det muligt at opnå fuld funktionalitet - reelle, praktiske og gavnlige resultater, der skal opnås for flere parter. Ved indlejring af beskyttelse af personoplysninger i en given teknologi, proces eller system skal det gøres på en sådan måde, at den fulde funktionalitet ikke forringes og at alle krav optimeres i størst muligt omfang. Dette kræver dog, at alle interesser og målsætninger skal være tydeligt dokumenteret og ønskede funktioner formuleret. Yderligere er kreativitet og innovation nødvendigt for at opnå alle mål og funktionalitet på en integreret positiv måde. Løsninger, der lykkes med at overvinde den forældede nul-sum tilgang, demonstrerer førsteklasses global beskyttelse af personoplysninger.

3.1.1.5 Princip nr. 5: End-to-End Security – Lifecycle Protection

Databeskyttelse gennem design er et koncept som bør følge et system, en teknologi eller en proces fra vugge til grav for at opnå bedst mulig databeskyttelse. Det bør indlejres i systemet, inden det første element af information indsamles og strække sig sikkert gennem hele livscyklussen for de involverede data. Stærke sikkerhedsforanstaltninger er afgørende for data beskyttelse fra start til slut. Dette sikrer, at alt data holdes sikkert og derefter destrueres i tide i slutningen af den givne proces. Privatlivet skal beskyttes kontinuerligt på tværs af hele domænet og gennem hele livscyklussen for de pågældende data. Sådanne kontinuerlige sikkerhedsforanstaltninger kan bestå i sikker destruktion, passende kryptering og stærk adgangskontrol og logningsmetoder.

3.1.1.6 Princip nr. 6: Visibility and Transparency

Synlighed og gennemsigtighed er afgørende for at etablere ansvarlighed og tillid. Databeskyttelse gennem design søger at forsikre alle interessenter om, at uanset hvilken forretningspraksis eller -teknologi der er tale om, er det faktisk i overensstemmelse med de angivne løfter og målsætninger,

underlagt uafhængig kontrol. Dens komponenter og operationer forbliver synlige og gennemsigtige, både for brugere og udbydere. Åbenhed og gennemsigtighed er nøglen til ansvarlighed. Oplysninger om politikker og praksis i forbindelse med håndtering af persondata skal gøres tilgængelige for enkeltpersoner.

3.1.1.7 Princip nr. 7: Respect for User Privacy
Brugeren er det vigtigste element, når det kommer til anvendelsen og implementeringen af Databeskyttelse gennem design. Arkitekter og operatører skal holde individets interesser øverst ved at tilbyde foranstaltninger om stærke privatlivsstandarder, passende meddelelse og bemyndigelse af brugervenlige muligheder. De bedste resultater fra databeskyttelse gennem design er normalt dem, der bevidst er designet omkring de enkelte brugeres interesser og behov, som har den største interesse i at administrere deres egne personoplysninger. De universelle principper i FIP støtter ligeledes dette princip. Samtykke, nøjagtighed, adgang og overensstemmelse er alle FIP'er, som støtter op om dette princip:

- **Samtykke:** Individets frie og specifikke samtykke er nødvendig for indsamling, brug eller offentliggørelse af persondata, medmindre andet er tilladt i henhold til loven. Jo større følsomheden af dataene er, desto klarere og mere specifikt samtykke kræves. Samtykke kan trækkes tilbage på et senere tidspunkt.

- **Nøjagtighed:** Behovet for nøjagtighed bygger på, at persondata skal være lige så præcise, komplette og ajourførte som nødvendigt for at opfylde de angivne formål.

- **Adgang:** Personer skal have adgang til deres persondata og informeres om dets anvendelser og oplysninger. Enkeltpersoner skal være i stand til at udfordre oplysningernes nøjagtighed og fuldstændighed og om nødvendigt ændre dem.

- **Overensstemmelse:** Afsluttende skal organisationer sikre overensstemmelse ved at etablere klage- og afhjælpningsmekanismer og formidle information om disse til offentligheden, herunder hvordan man får adgang til det næste niveau af klage.

Respekt for brugernes privatliv går ud over disse FIP'er og styrker behovet for, at grænseflader mellem mennesker og maskiner altid holder menneskets behov i fokus. Dette kan gøres gennem høj brugervenlighed, således at informerede privatlivsbeslutninger kan udnyttes pålideligt. På samme måde skal forretningsdrift og fysiske arkitekturer også demonstrere samme grad af hensyntagen til den enkelte, som skal fremhæves i centrum af operationer, der involverer indsamling af persondata (Cavoukian, A., 2010).

Dr. Ann Cavoukians 7 principper er således starten til databeskyttelse gennem design, men gennem tiden er der blevet udviklet mange andre måder at håndtere og skabe den fornødne sikkerhed af de registreredes personoplysninger. I det følgende vil "Handbook of Privacy and Privacy-Enhancing Technologies" af Blarkom, G.W. van et al blive gennemgået, da den, ligesom Dr. Ann Cavoukians 7 principper, sætter en milepæl for hvad der er nødvendigt for at sikre den fornødne sikkerhed for personoplysningernes færden på tværs af landegrænser. Mere præcist tager "Handbook of Privacy and Privacy-Enhancing Technologies" udgangspunkt i at håndtere trusler som følge af personoplysningernes færden på tværs af landegrænserne.

3.1.2 Handbook of Privacy and Privacy-Enhancing Technologies
Forordningen nævner i præambel 78, hvad der kunne betegnes som værende passende sikkerhedsforanstaltninger:

"(78) Beskyttelse af fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger kræver, at der træffes passende tekniske og organisatoriske foranstaltninger for at sikre, at denne forordnings krav opfyldes. For at kunne påvise overholdelse af denne forordning bør den dataansvarlige vedtage interne politikker og gennemføre foranstaltninger, som især lever op til principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. Sådanne foranstaltninger kan bl.a. bestå i minimering af behandlingen af personoplysninger, pseudonymisering af personoplysninger så hurtigt som muligt og gennemsigtighed for så vidt angår personoplysningers funktion og behandling, således at den registrerede kan overvåge databehandlingen, og den dataansvarlige kan tilvejebringe og forbedre sikkerhedselementer. Når producenter af produkter, tjenester og applikationer udvikler, designer, udvælger og bruger applikationer, tjenester og produkter, der er baseret på behandling af personoplysninger eller behandler personoplysninger, for at udføre deres opgaver, bør de tilskyndes til at tage højde for retten til databeskyttelse i forbindelse med udvikling og design af sådanne produkter, tjenester og applikationer og til under behørig hensyntagen til det aktuelle tekniske niveau at sørge for, at de dataansvarlige og databehandlerne er i stand til at opfylde deres databeskyttelsesforpligtelser."

Her nævner forordningen nogle mulige sikkerhedsforanstaltninger, men da det ikke er en udtømmende liste, er det relevant at undersøge hvilke andre sikkerhedsforanstaltninger, der måtte være i forbindelse med databeskyttelse gennem design. Der var i 2003 stor fokus på udviklingen af teknologier i Holland, hvor dette resulterede i en "Handbook of Privacy and Privacy-Enhancing Technologies" (Blarkom, Borking, Olk, 2003). Denne håndbog er en milepæl for det såkaldte PISA-projekt (Privacy Incorparated Software Agent). Indholdet i håndbogen er i relation til, hvad der er opnået og hvad der er nødvendig handling fremadrettet i forhold til at skabe beskyttelse af personoplysninger. Dens formål er, at vise hvordan de arkitektoniske tiltag har udviklet sig ved telekommunikation, informationsteknologi, samt hvilke EU-regler der er for beskyttelse af privatlivets fred og hvad der i sidste ende kræves af Privacy-Enhancing Technologies (PET) for at skabe beskyttelse i forhold til at skabe en Privacy Incorporated Software Agent (PISA). Det skal dog tages i mente, at hele denne håndbog er udviklet i forbindelse med direktivet, som gældende ret på dette tidspunkt. Årsagen til brugen af denne i nærværende afhandling begrundes med, at den belyser PET og er en del af den udvikling, som er forekommet i forhold til personoplysninger og beskyttelse af disse. Ydermere kan den skabe en form for tjekliste af tiltag til organisationerne.

Først og fremmest skal man som organisation finde frem til hvilke regler, i forhold til beskyttelse af personoplysninger, man gerne vil designe løsninger for. Der laves dermed en konsekvensanalyse, som indikation på hvor og under hvilke omstændigheder man skal fortage sig en teknisk sikkerhedsforanstaltning. Som en del af denne konsekvensanalyse er det dermed relevant at finde ud af hvilke typer af personoplysninger, man har i sin organisation. Herefter er det så udvælgelsen af teknologier, som kan understøtte de relevante regler om databeskyttelse og danne grundlag for den tekniske sikkerhedsforanstaltning (Blarkom, Borking, Olk, 2003). Organisationen skal dermed formå at opsætte en teknologi og teknisk tilgang, så de hele tiden kan ændre dette, når verdensbilledet ændrer sig i forhold til teknologien. Derfor er det vigtigt at have en cyklus, hvor man udvikler, tester, sætter i drift og vedligeholder (Mortensen, 2017). Hele udvælgelsen af PET er derfor en vigtig faktor i databeskyttelse gennem design. Definitionen af PET er som følgende:

> *"Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system."*(Blarkom, Borking, Olk, 2003, side 33)

For at man kan beskytte ens interne opbevarede eller gemte personoplysninger, er PET blevet udviklet gennem årene med det formål at være et sammenhængende system af forskellige foranstaltninger, som skal beskytte privatlivets fred ved at eliminere eller reducere personoplysninger eller helt at forhindre unødvendig og uønsket behandling af personoplysninger. Fordelen ved PET er, at det er helt uden at miste informationssystemets funktionalitet. PET forsøger at håndtere de eventuelle trusler, der måtte forekomme og er med til at lette arbejdsgangene, idet de i sidste ende kan erstatte kontrollen af håndhævelsen af reglerne om beskyttelse af personoplysninger, da dette dermed vil forekomme helt automatisk. Det er normalt meget tidskrævende og dyrt at skulle sikre og kontrollere, at alle i en given organisation overholder reglerne. Derfor er indførelsen af PET en klar fordel ifølge forfatterne af håndbogen (Blarkom, Borking, Olk, 2003).

Generelt hjælper PET med at takle to typer af trusler mod privatlivet. Den ene trussel består, i når personoplysninger bliver opbevaret uhensigtsmæssigt og den anden trussel opstår, når udefrakommende handler på vegne af andre ved enten løbende overvågning, dataudvinding eller forsøg på at få fat på personoplysninger fra en anden dataansvarlig i det skjulte. Selvom det virker som en positiv løsning for organisationer at implementere PET i deres IT-systemer, kan der forekomme negative konsekvenser heraf. Her menes der, at selvom der er lavet regler om, at man skal have passende tekniske og organisatoriske sikkerhedsforanstaltninger, er der endnu ikke nogen veletableret og verdensomspændende tilgang for en ensartet retningslinje for beskyttelse af personoplysninger gennem design. Der er dermed heller ikke nogen direkte vejledning, om hvordan man skal indbygge PET i den pågældende software eller IT-system ved de enkelte organisationer (Blarkom, Borking, Olk, 2003).

Måden, hvorpå PET bruges i systemerne, er ved, at de identitetsbeskytter og opdeler det gældende system i identitets-, pseudoidentitets- og anonymitetsdomæner. Grundlæggende er PET ikke noget nyopfundet, eller noget der ikke er set før. Hvad der menes her er, at man sagtens kan bruge ens eksisterende teknologier til at implementere i et IT-system, hvor disse derefter vil være kategoriseret som PET. Dermed kan de tiltag, som organisationen allerede har foretaget sig på nuværende tidspunkt, sagtens betegnes som PET. Dog er det en nødvendighed for organisationerne at gennemgå deres nuværende tekniske sikkerhedsforanstaltninger og analysere hvilke der måtte mangle, for at opnå en tilstrækkelig teknisk sikkerhed af de personoplysninger organisationerne måtte have (Blarkom, Borking, Olk, 2003).

3.1.2.1 The seven PET principle

For at organisationerne kan skabe et overblik over, hvad der er tilstrækkelige sikkerhedsforanstaltninger, er det relevant at vide, hvilke PET organisationen skal tage i brug og få implementeret i sit IT-system. Håndbogen (afsnit 3.1.2) har fremført *the seven PET principle*, som klassificering af hvad der er indeholdt og en nødvendighed for at sikre personoplysninger. De syv principper vil i det følgende blive gennemgået.

- **Limitation in the collection of personal data:** Dette princip handler om at forbedre systemer til beskyttelse af personoplysninger, herunder som først og fremmest skal overholde artikel 6, stk. litra c i direktivet. Dette er tilsvarende artikel 5, stk. 1, litra c i forordningen. De personoplysninger, man indsamler, skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de indsamlet og behandles videre. I

dette tilfælde er der dermed kun tale om de data, man har indsamlet. Det er her yderst vigtigt, at man ved udformningen af ens database kun tilføjer de typer af personoplysninger, man til enhver tid kan retfærdiggøre at have et formål, som er et krav fra både direktivet og forordningen.

- **Identification/authentication/authorization:** Der bliver i artikel 16 i direktivet klargjort at enhver person, der handler under den registeransvarlige og som har adgang til personoplysninger, ikke må behandle dem, medmindre dette forgår under den instruks, der er givet fra den dataansvarlige, medmindre loven kræver andet. Dette er tilsvarende forordningens artikel 29, som fastholder direktivets regulering på dette område. Ovenstående kan bruges i forhold til brug af et IT-system, hvor der kun må behandles de personoplysninger, hvor der forekommer et formål og rette grundlag for. Det vil sige, at organisationen kun må behandle de personoplysninger, der kan relateres til den normale arbejdsgang. Et eksempel herpå kunne være en læge, der kun har ret til at bruge og behandle de personoplysninger, der er omkring hans egne patienter og ikke alle andre lægers patienter. Derfor kunne det for organisationerne være en fordel i dette tilfælde at udvikle en PET, der automatisk styrer denne regulering. Dette kunne skabes ved, at organisationerne skaber unikke identiteter til dem, der har adgang til organisationernes personoplysninger. Herved skal systemet sørge for, at man har en begrænset adgang i systemet, og kun kan tilgå de nødvendige oplysninger for at udføre ens erhverv og formål med jobbet. Dermed skaber man en kontrol over ens data og tilgåelse dertil. Denne identifikation skaber dermed opdelinger i organisationen, så økonomiafdelingen ikke har samme adgang som HR-afdelingen og yderligere kan man i hver afdeling have forskellige identiteter, så chefen måske har en anden adgang end den enkelte medarbejder.

- **Standard techniques used for privacy protection:** I dette princip er der tale om en PET omkring anonymisering. Dette er ud fra reguleringen om, at en yderligere behandling af data for historiske, statistiske eller videnskabelige formål ikke må anses for at være uforenelig, forudsat at der træffes passende sikkerhedsforanstaltninger, jf. Direktivets artikel 6, stk. 1, litra b. Denne regulering fremgår også i forordningens artikel 5, stk. 1, litra b, og må anses for forsat at gælde for alle organisationer. Betydningen af dette går på, at organisationerne skal kunne garantere, at det opbevarede data kun må anvendes til disse formål. For at opnå dette for organisationerne kan den bedste garanti opnås ved at transformere dataene, så de ikke længere kan bruges til at identificere den registrerede. Det er her anonymiseringen kommer i spil for at opretholde de fornødne sikkerhedsgarantier.

- **Pseudo-identity:** Pseudonymisering som det næste princip er en velovervejet metode til at systematisere ens data på uden at være linkbar, som kan skade den registrerede. Pseudonymisering er en PET, som deler den registreredes oplysninger op på en sådan måde, at personoplysninger bliver fordelt i IT-systemet med tal i stedet for de rigtige oplysninger. Det vil sige, at organisationen har en registreret med et nummer og ikke navn. Dette nummer kan linkes sammen med navnet på den registrerede men kun med en begrænset adgang til dette link. Organisationerne kan altså med en pseudonymisering opdele data, hvor de stadig har de oplysninger, som er nødvendige for at behandle dette data. Der er flere statistiske formål i et sådant IT-system, hvor det ikke er nødvendigt at vide den registreredes identitet.

- **Encryption:** Kryptering er et typisk eksempel på en eksisterende teknologi, der kan hjælpe databeskyttelse. Kryptering er en sikkerhedsforanstaltning som giver troværdighed. Kryp-

tering kan være en rigtig god PET-løsning, der hvor der er manglende tillid. Udover kryptering er der også mulighed for at dele hemmeligheder uden behov for at udveksle nøgler, digitale signaturer, dataintegritet og nøgleoprettelse. Ydermere kan det også sikre al form for forsendelse mellem de parter i organisationen, hvor der er kryptering tilstede. For at reducere mængden af personoplysninger, der skal behandles, uden at miste funktionen af et informationssystem, skal man træffe beslutninger vedrørende følgende: opbevaring, adgang, offentliggørelse og overførsel. Brug af kryptografi kan styrke alle disse aspekter. Eksempler på brugen af kryptografi til databeskyttelse omfatter:

- Dataopbevaringsdata: Data skal opbevares forsvarligt. Personoplysninger og følsomme personoplysninger kræver specielt opmærksomhed. Det anbefales at kryptere personoplysninger, der skal opbevares på computerenheder. Integritet af data kan også beskyttes af kryptografiske midler.

- Bemyndigelse: For at afgøre hvem der har adgang til hvad, skal der være et krav om måden, identiteter bliver verificeret på. Dataadgang og dataoplysningsapplikationer kan styres ved at kontrollere adgangen gennem godkendelse og autorisation. Ved at udføre kryptering og dekryptering på applikationsniveau i stedet for på databaseniveau, kan ukorrekt brug af personoplysninger udelukkes.

- Data Transport: Personoplysninger, der skal videregives til bestemte parter via eksterne lagringsdokumenter som f.eks. disketter eller cd-rom'er, skal krypteres. Det samme gælder for dataoverførsler via et netværk.
  Kryptering kan finde sted på flere netværkslag (OSI-niveauer), når netværksorienteret dataoverførsel er involveret:
  - På applikationsniveau (OSI lag 7, logisk): Data krypteres af applikationen, før de sendes ned til de næste OSI lag.
  - På netværksniveau (OSI niveau 1, fysisk): Før dataene faktisk overføres til netværket, behandles de ved hjælp af en krypteringsboks.

  Dette er for at sikre, at en uautoriseret part, der bryder ind på et netværk eller en applikationsserver, ikke kan fortolke eller forstå de overførte eller behandlede data. For at opnå fordelene ved kryptering på netværkslag, skal der udstedes offentlige nøgler, og forbindelsen mellem parter og deres offentlige nøgle skal være troværdige. Sidstnævnte opnås ved certifikater, hvor et betroet organ (Trusted Third Party - TTP) bekræfter forbindelsen mellem en enhed og en offentlig nøgle.

- **Biometrics:** Dette princip kan bruges som en PET af organisationerne som en anden sikkerhed end adgangskoder. Adgangskoder er ofte forbundet med en risiko for at blive glemt af medarbejderen. Derfor vælger medarbejderen ofte en adgangskode, som bygger på en relation og dermed er nemmere at huske. En anden risiko kan opstå ved, at medarbejderen vælger at skrive adgangskoden ned og opbevare den tæt ved ens computer. Derfor er biometri en mulig PET, man kan benytte sig af, hvor man bruger medarbejdernes fingeraftryk som åbningsnøgle til både computer og IT-systemerne. Dog er dette kategoriseret som en følsom personoplysning, jf. forordningens artikel 9, og man skal derfor som organisation sørge for at have den rette opbevaring af disse fingeraftryk. Dette er især vigtigt i forhold til at få dem slettet efter et endt ansættelsesforløb.

- **Audit ability:** Dette princip forløber sig på tilsynsmyndighedernes krav på at få adgang til, hvad man har af data og hvordan man både behandler og opbevarer det. Her kan organisationen bruge PET til at logge alle ens aktiviteter til databasen, og dermed er det lettere at overgive til datatilsynet. Ydermere demonstrerer organisationen herved, at de ikke har noget at skjule ved at have denne PET, som giver en stor åbenhed overfor tilsynsmyndighederne.

Ovenstående gennemgår de mulige PET, som organisationer med fordel kan implementere, og som må anses for at være meget attraktive og relevante for at overholde forordningens artikel 25. Organisationen bliver ved implementeringen af PET designere af deres informationssystemer, der har til formål at overholde lovgivningen om beskyttelse af persondata gennem teknologi, og dermed repræsentere en åbenhed omkring sin databeskyttelse. Ifølge betænkningen nr. 1565 bliver der udtalt, at implementeringen af PET kan afhjælpe den konkrete tekniske overholdelse af nogle af sikkerhedsforpligtelserne. Ydermere kan der ved hjælp af PET udformes informations- og kommunikationssystemer og tjenesteydelser, hvor indsamlingen og anvendelsen af personoplysninger kan indskrænkes, og hvor det er lettere at overholde databeskyttelsesreglerne. Det er derfor vigtigt, at organisationen som det første identificerer de områder af informationssystemet, der repræsenterer de reelle risici i forbindelse med krænkelse af privatlivets fred. Når først dette er identificeret, er udviklingen af PET en kreativ proces. Sammen med de syv PET-principper og på samme tid at kunne designe nye PET, som er relevante for ens organisation, kan dette skabe grundlaget for overholdelse af forordningen. Dette er dermed også med til at skabe den rette tillid hos de registrerede men også tilsynsmyndigheden.

Håndbogen er skrevet under direktivets regulering og kan benyttes som en fortolkning af dennes artikel 17, stk. 2. Dog må det antages, at der under den nye forordning er sket en skærpelse af databeskyttelse gennem design, som adskiller sig fra direktivet, da det er blevet et krav for organisationerne at implementere denne regulering. Derfor må det ovenstående få en større betydning og udvikling i fremtiden, da mange organisationer burde indføre dette for både at overholde reglerne i forhold til de tekniske foranstaltninger, men også for at man på langt sigt får en automatisk kontrol af sikkerheden og overholdelse i stedet for at bruge mange ressourcer på kontant fysisk kontrol.

Sammen med fortolkningen af håndbogen og Dr. Ann Cavoukians 7 principper om databeskyttelse gennem design (afsnit 3.1.1), er ENISA (EUs agentur for netværk og informationssikkerhed) et center som arbejder på at udvikle råd og anbefalinger om god praksis inden for informationssikkerhed for EU og dets borgere (ENISA, 2014). Derfor er det relevant at undersøge udviklingen og brugen af ENISAs tilgange.

3.1.3 ENISA

Beskyttelse af personoplysninger er elementært for både den enkelte borger og samfundet som helhed. Menneskerettighedskonventionen (Council of Europe, 1950) og verdenserklæringen om menneskerettigheder (United Nations, 1948) har anerkendt, at beskyttelse af personoplysninger er en grundlæggende rettighed. Den konstante udvikling, som præger informations- og kommunikationsteknologien, er især en af årsagerne til, at nye udfordringer for beskyttelse af personoplysninger er opstået. Et vigtigt element til at beskytte personoplysninger er Privacy-Enhancing Technologies (afsnit 3.1.2), som bl.a. indeholder kryptering, protokoller til anonym kommunikation og fortolkningsbaserede legitimationsoplysninger. Alle disse former for håndtering af personoplysninger er med det formål at skærpe sikkerheden omkring personoplysninger. EUs agentur for net-

værk og informationssikkerhed (ENISA) er et center for sikkerhedskompetencer for EU, dets medlemsstater, den private sektor og Europas borgere. Ligesom Privacy-Enhancing Technologies (afsnit 3.1.2) og Dr. Ann Cavoukians 7 principper om databeskyttelse gennem design (afsnit 3.1.1), arbejder ENISA på at udvikle råd og anbefalinger om god praksis inden for informationssikkerhed. ENISA hjælper EU-medlemsstaterne med at gennemføre relevant EU-lovgivning og arbejder for at forbedre modstandsdygtigheden i Europas kritiske informationsinfrastruktur og -netværk (ENISA, 2014).

3.1.3.1 Tilgange til beskyttelse af personoplysninger

Forståelsen af principper vedrørende beskyttelse af personoplysninger har udviklet sig gennem årene - på internationalt og nationalt plan. Tilgangen til beskyttelse af personoplysninger kan være bred og det essentielle er selve beskyttelsen heraf (ENISA, 2014).

Multilaterale sikkerhedskrav er en af metoderne til at beskytte personoplysninger. De multilaterale sikkerhedskrav tager højde for alle de involverede parters privatliv og sikkerhedsinteresser, og ikke blot slutbrugeren eller operatøren af det pågældende system. Det er således alle led i processen, som bliver behandlet med sikkerheden for øje. Denne tilgang kræver, at alle parter informeres om tilknyttede fordele (fx sikkerhedsgevinster) og ulemper (fx omkostninger, brug af ressourcer, mindre personalisering). Alle disse interesser og mål vil blive taget i betragtning ved valg af mekanismer til støtte og realisering af alle parters krav. Tilgangen til multilateral sikkerhed er blevet udviklet parallelt med de første begreber om privatlivsforbedrende teknologier og senere begrebet databeskyttelse gennem design (ENISA, 2014).

Privacy-Enhancing Technologies er ligeledes en tilgang til beskyttelse af personoplysninger. Nye informationsteknologier ændrer persondata og databeskyttelsesrisici, vi står over for, men teknologien kan omvendt også hjælpe med at minimere eller undgå risici mod personoplysninger. I 1995 blev ideen om formgivningsteknologi i overensstemmelse med principperne om beskyttelse af personoplysninger drøftet blandt databeskyttelseskommissærerne. Hovedprincipperne var dataminimering og identitetsbeskyttelse ved anonymisering eller pseudonymisering. Denne diskussion førte til udtrykket "Privacy-Enhancing Technologies" (afsnit 3.1.2). Udvikling og integration af PET betyder indbygget databeskyttelse og overvejelse af hele systemets livscyklus (ENISA, 2014).

Ved globalisering af forretningspraksis kan internationale standarder for beskyttelse af personoplysninger blive nødvendige. Således blev der i 2006 vedtaget en række universelle principper for beskyttelse af personoplysninger, som skal fungere som en global standard for forretningspraksis uanset grænser. Denne såkaldte "Global Privacy Standards" har været rettet mod at hjælpe offentlige beslutningstagere såvel som organisationer og teknologiske udviklere (ENISA, 2014).

Databeskyttelse gennem design blev indført som en tilgang til beskyttelse af personoplysninger af Dr. Ann Cavoukians 7 principper om databeskyttelse gennem design, ved at kræve databeskyttelse indbygget i et design som en forebyggende og proaktiv foranstaltning (afsnit 3.1.1). De syv grundprincipper karakteriserer egenskaber snarere end instruktioner til specifikke foranstaltninger, der skal træffes. Yderligere giver principperne en beskrivelse af, hvordan man implementerer beskyttelse af personoplysninger ved design (ENISA, 2014).

3.1.3.2 Lovgivningen og databeskyttelse

De ovenfor beskrevne principper og tilgange skal afspejles i lovgivningen for at være effektive. I henhold til den europæiske databeskyttelseslov er behandling af personoplysninger kun tilladt, hvis den person, hvis personoplysninger behandles (i den europæiske retlige ramme kaldet "den registrerede") utvetydigt har givet samtykke eller behandling er nødvendig for opfyldelse af en kontrakt for overholdelse af en juridisk forpligtelse for at beskytte den registreredes livsinteresser

for udførelsen af en opgave udført af almen interesse eller med henblik på legitime interesser for databehandlingsenhederne, hvis sådanne interesser ikke tilsidesættes af den registreredes grundlæggende rettigheder og friheder (ENISA, 2014).

3.1.3.3 Metoder til beskyttelse af personoplysninger

Når målene og antagelserne på konteksten er defineret, er udfordringen at finde de relevante privatlivsforbedrende teknikker og protokoller og kombinere dem for at imødekomme systemets krav. Den første forhindring, der skal overvindes, er de potentielle konflikter eller uoverensstemmelser mellem beskyttelse af personoplysninger og de øvrige (funktionelle og ikke-funktionelle) krav i systemet. Udviklingen af passende metoder eller tilgange til databeskyttelse gennem design er blevet fremsat og undersøgt af flere forskningsgrupper i løbet af det seneste årti. En måde at overvinde opgavens kompleksitet på er at definere databeskyttelse gennem design gennem designmetoder på arkitektonisk niveau (Antignac, T. and Le Métayer, D., 2014). Følgende nøglekriterier skal overvejes i ved databeskyttelse gennem design:

- **Tillid:** En afgørende forudsætning for et velfungerende databeskyttelse gennem design er valget af tillidsforholdet mellem interessenterne. Dette er en drivende faktor ved udvælgelsen af de arkitektoniske muligheder samt PET (afsnit 3.1.2). Graden af tillid kan variere fra blind tillid, verificerbar tillid til kontrolleret tillid. Den stærkeste form for tillid er den blinde tillid, som fra et teknisk synspunkt kan føre til de mest sårbare løsninger, da der i denne situation er stor risiko for misplaceret tillid. Der er ved blind tillid dermed mere på spil end ved en svagere grad af tillid. Verificerbar tillid er af en mellemliggende grad af tillid, hvor man har tillid som en standard men med mulighed for verificeringer. Disse verificeringer kan blandt andet ske ved forpligtelser eller stikprøvekontrol for at kontrollere, at den betroede part ikke bliver snydt. Til gengæld udspringer kontrolleret tillid teknisk set fra en "no trust-opsætning". Denne tillids grad bygger på kryptografiske algoritmer og protokoller, for at understøtte ønsket om minimal tillid.

- **Inddragelse af brugeren:** Endnu en vigtig forudsætning for opbyggelse af databeskyttelse gennem design er graden af brugerens interaktioner. I nogle tilfælde er interaktion slet ikke til stede og i andre tilfælde er det nødvendigt at gennemføre interaktionen, førend man kan påbegynde det givne systems videre proces. I designs hvor interaktionen er tilstede, skal følgende spørgsmål betragtes af designeren: Hvilke oplysninger meddeles til brugeren, i hvilken form og på hvilket tidspunkt? Hvilke initiativer kan brugeren selv tage, gennem hvilke midler og på hvilket tidspunkt? Der skal lægges stor vægt på, at systemets design gør det muligt for brugeren at benytte sig af alle sine rettigheder (udtrykkeligt samtykke, adgang, korrektion, sletning osv.) uden unødige begrænsninger.

- **Arkitektur:** Definitionen på arkitekturen, herunder typen af komponenter, de interessenter, der styrer dem, lokaliseringen af computere, kommunikationsforbindelserne og datastrømmen mellem komponenterne, er endnu en vigtig forudsætning for opbygningen af databeskyttelse gennem design. Beskyttelse af personoplysninger gennem design er en kontinuerlig, iterativ proces og forskellige begivenheder (såsom tilgængeligheden af nye PET eller angreb på eksisterende teknologier) kan kræve en omarrangering af prioriteter eller revurdering af visse antagelser og forudsætninger. Som for enhver proces er det også nødvendigt at kunne evaluere resultatet af det pågældende design (ENISA, 2014).

3.1.3.4 Evalueringsmidler

Anvendelsen af et veldefineret design til beskyttelse af personoplysninger er ikke i sig selv en absolut garanti for, at systemet vil overholde alle sine privatlivskrav. Dertil kommer ansvarsprincippet, hvor datakontrollanter skal kunne påvise overholdelse af interne og eksterne data. Denne forpligtelse er nedfældet i forordningens præambel nr. 74:

> *"Der bør fastsættes bestemmelser om den dataansvarliges ansvar, herunder erstatningsansvar, for enhver behandling af personoplysninger, der foretages af den dataansvarlige eller på den dataansvarliges vegne. Den dataansvarlige bør navnlig have pligt til at gennemføre passende og effektive foranstaltninger og til at påvise, at behandlingsaktiviteter overholder denne forordning, herunder foranstaltningernes effektivitet. Disse foranstaltninger bør tage højde for behandlingens karakter, omfang, sammenhæng og formål og risikoen for fysiske personers rettigheder og frihedsrettigheder."*

En måde hvorpå man kan evaluere og garantere, at man som organisation opfylder alle regler for beskyttelse af personligdata kan være gennem "privacy certificering" eller "privacy seals". Disse redskaber, som også fremmes af forordningen, præambel 40-42, giver en anden ramme for privatlivets vurdering. Faktisk er fortrolighedsforseglinger og certifikater allerede i drift med forskellige mål. Nogle af dem gælder for websites, andre til procedurer og helt tredje gør sig gældende for produkter. Uanset fortrolighedsforseglingens eller certificeringens mål er de vigtigste kriterier at fastslå certificeringsenhedens mekanismerne for at sikre, at det er tillidsværdigt. Det er ligeledes vigtigt ved beskyttelse af personoplysninger, at designet er evalueret og defineret i et omfang, så det kan tage del i et fuldendt system og leve op til det forventede brug. Afsluttende bør det overvejes, hvorledes resultatet af certificeringen meddeles til brugerne. Dette er især kritisk, når forseglingen eller certifikatet skal give information til slutbrugerne. For mere forretningsorienterede certifikater skal evalueringsresultatet uden tvetydighed beskrive evalueringsomfanget, krav for personoplysninger, niveauet for forsikring og resultatet af evalueringen (som kan indeholde bemærkninger eller anbefalinger vedrørende brugen af produktet).

I praksis bør merværdien af en fortrolighedsforsegling eller certificeringen bidrage til en øget tillid således, at et produkt opfylder krav til beskyttelse af personoplysninger. Denne øgede tillid afhænger i sidste ende af den tillid, der kan placeres i certificeringsorganet. (ENISA, 2014).

3.1.3.5 ENISAs råd og anbefalinger om god praksis inden for informationssikkerhed

Der er en tydelig sammenhæng mellem ENISA og Dr. Ann Cavoukians 7 principper om adressering af databeskyttelse gennem design. Dog kritiserer ENISA Dr. Ann Cavoukians principper for ikke at være konkrete med mekanismer til at integrere privatiseringen i udviklingsprocessen af et system. Hertil kommer ENISAs kritik af PET, grundet den ensidige tilgang til at løse de designmæssige udfordringer, da der i denne sammenhæng ikke inddrages andet end "Privacy-Enhancing Technologies". Databeskyttelse gennem design er et tosidet begrebet. I juridiske dokumenter er databeskyttelse gennem design på den ene side generelt beskrevet i meget brede vendinger som et generelt princip. På den anden side er databeskyttelse gennem design ofte blevet ligestillet med brugen af specifikke PET af computerforskere og ingeniører. Men databeskyttelse gennem design er hverken en samling af mere generelle principper eller kan reduceres til implementeringen af PET. Faktisk er det en proces, der involverer forskellige teknologiske og organisatoriske komponenter, som implementerer principper for beskyttelse af persondata og databeskyttelse. ENISAs løsning er en tilvejebringelse af en ordning til raffinering af delsystemer eller komponenter i et system eller nærmere forholdet mellem dem. Dette er resultatet af en tilbagevendende struktur af kommunikationsdele, der løser et generelt designproblem inden for en bestemt sammenhæng. Der-

med forslår ENISA, at der laves bestemte designmønstre eller arkitekturmønstre på et højere niveau. Dette giver dermed brugeren et sæt foruddefinerede delsystemer, specificerer deres ansvar og indeholder regler og retningslinjer for at organisere forholdet mellem dem. På den måde, kan man på baggrund af ENISAs arkitekturmønstre skabe integrerende databeskyttelse gennem design (Mortensen, H., 2017).

Ved at efterleve Dr. Ann Cavoukians 7 principper, PET og ENISAs arkitekturmønstre vil man i høj grad kunne efterleve det materielle indhold af artikel 25 om databeskyttelse gennem design. Der er derfor et krav til den dataansvarlige om, at foretage en konkret vurdering og beslutte en materiel løsning ud fra det brede udvalg af teknologier og metoder med det formål at opnå og implementere foranstaltninger, som understøtter sikkerheden og designet som beskytter de registreredes garantier, rettigheder og frihedsrettigheder efter forordningen (Mortensen, H., 2017).

3.2 Dansk vs. norsk håndtering af databeskyttelse gennem design

Det er relevant at undersøge forskellen på den nuværende og fremtidige norske og danske håndtering af databeskyttelse gennem design, da norsk og dansk retssystem minder meget om hinanden og næsten er opbygget på samme måde. Det er derfor væsentligt at undersøge to forskellige landes syn og håndtering af databeskyttelse gennem design, når deres retssystem er så tæt forbundet. Som en del af de nordiske lande, som engang har været forbundet som en nation under den danske konge, har der altid været en tæt forbindelse mellem de to lande og dette er derfor baggrunden for denne sammenligning (Lando, B. O., 2012)

Straffen for overtrædelse af den norske personopplysningslov er større end ved den danske persondatalov, derfor må antages, at man er på et højere niveau indenfor persondatabeskyttelse i Norge end i Danmark. Man kan i Norge få en bøde eller en fængselsstraf på enten 1 år eller 3 år, alt efter graden af overtrædelse af deres lov, jf. personopplysningsloven §§48-49 Den største straf der kan forekomme i Danmark inden for overtrædelse af persondataloven er en bøde på 25.000 kr. (Thzaskowski, J. et. Al., 2017) Det må yderligere antages, at da Norge ikke er en del af EU, må de have en særlig interesse i at overholde den nye forordning i forhold til at kunne opretholde eksport og import med hele Europa.

Forordningen skriver i præambel 77 følgende:

> *"(77) Retningslinjer til den dataansvarlige eller databehandleren om implementering af passende foranstaltninger og for påvisning af vedkommendes overholdelse af denne forordning, navnlig for så vidt angår identificering af risikoen i forbindelse med behandlingen, deres vurdering med hensyn til risikoens oprindelse, karakter, sandsynlighed og alvor og om identificering af bedste praksis med henblik på at begrænse denne risiko, kan opstilles, navnlig gennem godkendte adfærdskodekser, godkendte certificeringer, retningslinjer fra Databeskyttelsesrådet eller en databeskyttelsesrådgivers anvisninger. Databeskyttelsesrådet kan også opstille retningslinjer for behandlingsaktiviteter, som anses for sandsynligvis ikke at medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder, og give anvisninger for, hvilke foranstaltninger der kan være tilstrækkelige i disse tilfælde for at afhjælpe en sådan risiko."*

Ovenstående stykke beskriver, hvad der skal til for at finde frem til passende sikkerhedsforanstaltning og hvordan man identificerer risikoen ved behandlingen af persondata. Det er derfor relevant at undersøge, hvordan dette bliver håndteret af henholdsvis den danske nation og den norske nation på baggrund af deres lignende retssystemer.

Den danske vurdering og håndtering af betydningen af forordningens artikel 25 er før den 25. maj 2018 blevet udformet i Betænkning nr. 1565 og en vejledning fra datatilsynet til de danske organisationer. Forordningens mål er at genskabe tilliden til de registrerede ved at påkræve den dataansvarlige og dennes databehandler at gennemføre passende tekniske og organisatoriske foranstaltninger, som i betænkning nr. 1565 betegnes som værende:

> *"…designet med henblik på effektive garantier i behandlingen af personoplysninger for at opfylde kravene i forordningen og beskytte de registreredes rettigheder"* (Betænkning nr. 1565, side 416).

Den danske betænkning fortolker artikel 25 i forordningen som værende både et middel, såsom et IT-systems tekniske indretning og brugergrænseflade, samt måden hvorpå den dataansvarlige organisatorisk er indrettet på.

I betænkningen bliver der vægtet mellem de tekniske sikkerhedsforanstaltninger og de organisatoriske sikkerhedsforanstaltninger. Her gives der et eksempel på, at såfremt omkostningerne og ressourcerne ved anskaffelse af et nyt IT-system er for markante i forhold til at imødekomme de tekniske sikkerhedsforanstaltninger, kan man foretage justeringer i sit nuværende IT-system. Herved kan der i organisationen suppleres op for at imødekomme det restbehov, der måtte være ved hjælp af de organisatoriske sikkerhedsforanstaltninger. Betænkningen laver altså en fortolkning på, at de to former for sikkerhedsforanstaltninger hænger sammen, og at den ene type sikkerhedsforanstaltning ikke foretrækkes frem for den anden (Betænkning 1565). Der fastslås yderligere, at det er tilstrækkeligt såfremt man under etableringen af passende sikkerhedsniveau gør brug af interne procedurer, undervisning af ansatte eller andre organisatoriske foranstaltninger ved brugen af sit nuværende IT-system. Betænkningen laver en antagelse om, at de foranstaltninger, man som dataansvarlig må være forpligtet til at implementere, er en sikring af de midler, der anvendes, såsom ens IT-system hvor kravene i forordningen skal efterleves gennem fornødne sikkerhedsforanstaltninger. Det er også en dansk betragtning, at implementeringen af PET kan afhjælpe den konkrete tekniske overholdelse af nogle af sikkerhedsforpligtelserne. Ydermere kan der ved hjælp af PET udformes informations- og kommunikationssystemer og tjenesteydelser, hvor indsamlingen og anvendelsen af personoplysninger kan indskrænkes og hvor det er lettere at overholde databeskyttelsesreglerne.

Der lægges endvidere i Danmark vægt på, at man som dataansvarlig forsøger at håndhæve artikel 25, ved at man kontraktuelt stiller krav om, at systemet udvikles i overensstemmelse heraf. Det er her en god idé som dataansvarlig at sætte sig ind i hvilke PET-krav, organisationen vil stille overfor IT-udbyderen i forhold til deres forretning. Dette vil i sidste ende give det bedste resultat, da man som IT-udbyder har mange forskellige kunder og deres forretninger alle sammen har forskellige krav til datasikkerhed. Derfor er det ikke altid en simpel opgave at udføre for IT-udbyderen, hvis den dataansvarlige ikke selv har gjort sig overvejelser om, hvilke krav der skal stilles til designet.

Det tekniske og organisatoriske område har dermed et meget tæt sammenspil, og man skal i hver situation overveje, hvorvidt de passende sikkerhedsforanstaltninger skal løses teknisk eller organisatorisk. I mange tilfælde ville det være lettere at håndhæve, hvis organisationen har nogle automatiske processer, dog kan dette være meget omkostningsfuldt. Derfor er den organisatoriske tilgang til databeskyttelse gennem design af stor vigtighed for de organisationer, der allerede har en form for IT-system implementeret. I forhold til den danske udmeldelse på, hvad der ligger i artikel 25, nævnes det yderligere, at det er relevant at undersøge forordningens artikel 5 og dennes betydning. Der lægges her vægt på, at man som organisation skal tænke over formålet for databe-

handling, dataminimering, begrænsede opbevaringsperioder, datakvalitet, retsgrundlag for behandling, behandling af særlige kategorier af personoplysninger, foranstaltninger til at sikre datasikkerhed og krav til videreoverførsel. Dette er alle principper, som organisationen skal efterleve som dataansvarlig og efterfølgende udføre en handlingsplan og implementering heraf. Dette skal gøres ud fra forordningens krav i artikel 35 om konsekvensanalyse, hvor man som udgangspunkt skaber et godt fundament for ens databeskyttelse gennem design.

Datatilsynet har udsendt et udkast til en vejledning om databeskyttelse gennem design (bilag 5) til alle private og offentlige instanser, med udgangspunkt i den allerede udformede Betænkning nr. 1565 og Forordningen. Den har opstillet fire trin, som man som dataansvarlig med fordel kan benytte sig af i det praktiske:

- Trin 1: Identifikation og vurdering af risici

  I dette trin skal organisationen vide hvilke persondata, de har, hvor de befinder sig, hvordan de behandles og hvordan de bevæger sig rundt i systemerne. Herefter kan man finde frem til hvilke risici, der kunne være for den fysiske persondata og den måde den bliver behandlet og opbevaret på.

- Trin 2: Identifikation af mulige foranstaltninger

  I dette trin skal organisationen, efter at have fundet frem til alle de risici der måtte forekomme, lave en vurdering af og kortlægge hvilke foranstaltninger der skal til, for at opnå et passende sikkerhedsniveau.

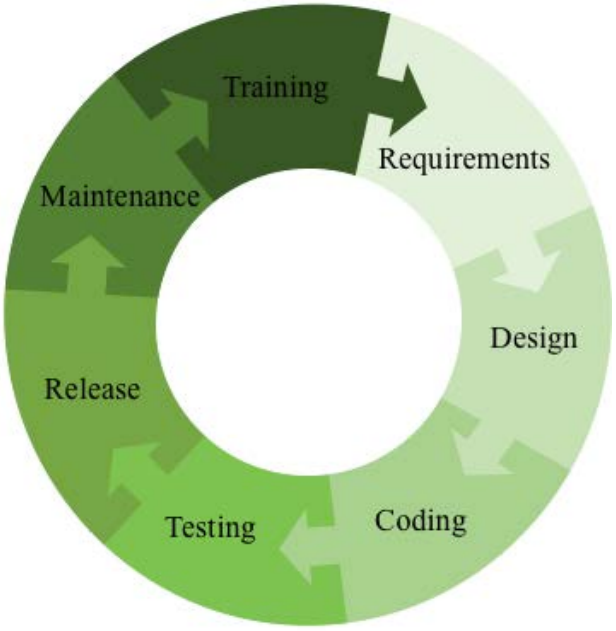
- Trin 3: Gennemgang af hvilke kortlagte foranstaltninger der imødegår relevante risici, så et passende sikkerhedsniveau opnås

  Man skal i dette trin bruge de fremfundne risici til at finde frem til en kombination af flere foranstaltninger, som komplementerer hinanden og derved reducerer de identificerede risici.

- Trin 4: Implementering af de foranstaltninger, som det besluttes at gennemføre

  På baggrund af ovenstående trin skal organisationen her træffe en beslutning om, hvilke foranstaltninger der skal bruges og gennemføres for at skabe et passende sikkerhedsniveau, som passer lige netop til de risici, der er fundet frem til tidligere i organisationen. Til sidst implementeres de valgte sikkerhedsforanstaltninger så i organisationen.

Det norske datatilsyn har udviklet en vejledning for, hvad organisationerne skal gøre for at blive compliant på forordningens artikel 25. Det er en kontinuerlig proces, som går i ring og som hele tiden skal cirkulere rundt i organisationen. Denne udvikling er baseret på Dr. Ann Cavoukians 7 principper om databeskyttelse gennem design (afsnit 3.1.1). Dog udtaler det norske datatilsynets direktør Bjørn Erik Thon, at databeskyttelse gennem design er gået fra at være 7 principper til at blive et koncept med konkret indhold (Kjernejournal av direktoratet for e-helse vant innebygd personvern i praksis 2017). Den norske vejledning er derfor meget relevant, da de som land har taget en aktiv tilgang til implementeringen af forordningen og har lavet en fortolkning af, hvad der skal til for at skabe et godt databeskyttelsesdesign. Valget af metode er typisk forbundet med den service organisationen udbyder, industrien, typer af software der bliver udviklet og overvejelserne og forberedelserne i forhold til organisationens egen niveau af risiko.



Figur 1. Kilde: Egen tilvirkning

Med udgangspunkt i ovenstående, vil den norske vejlednings procedure (figur 1) i det følgende blive gennemgået med det formål at klarlægge Norges tilgang til databeskyttelse gennem design. Det første tiltag i den norske vejledning er træning. Her finder man frem til de specifikke typer af træning, som er nødvendige for ens organisation. For at sikre at alle i organisationen forstår både behovet for og de risici, der er forbundet med databeskyttelse og sikkerhed, skal træningen struktureres.

Det er en forudsætning, at man har en forståelse for databeskyttelse og informationssikkerhed for at kunne have den rette tekniske udvikling med databeskyttelse gennem design. Det er vigtigt at medarbejderne ved, hvilke krav der skal anvendes til at sikre, hvad de skal passe på og hvilke værktøjer der skal til for at opretholde den rette viden om databeskyttelse. Medarbejdere skal også vide, hvilke metoder og rutiner der skal følges. Det er organisationen selv, der skal afgøre, hvad der er relevant og hvilken type træning, der kræves for de enkelte medarbejdere i de forskellige afdelinger i forhold til både de interne krav, men også de eksterne krav. Det er derfor også relevant for organisationen at udarbejde en træningsplan.

Det næste tiltag er krav. Her drejer det sig om indstillingskravet til databeskyttelse i forhold til slutproduktet. Kravene til organisationen er dermed en afspejling af behovet for databeskyttelse og hvor dette behov er i organisationen. Først og fremmest er det vigtigt at vide, hvilke typer af personoplysninger man har, herunder hvilke kategorier af personoplysninger der skal behandles i softwaren. Hvilke konklusioner kan der drages om individer baseret på de data, der behandles, hvem er brugeren og ejeren af dataene og hvis det er relevant, hvem der er databehandler eller modtageren af personoplysningerne. Dette er nødvendigt for at bestemme hvilke love, regler, retningslinjer og adfærdskodekser der gælder for ens IT-systemer. Organisationen skal skabe de relevante krav til databeskyttelse via deres forretningspraksis, politikker for databeskyttelse, forskellige sikkerhedsstandarder og adfærdskodekser eller andre relevante love og bestemmelser. De skal selv bestemme, hvilke krav der er relevante for deres forretning, den software, der udvikles, og den sammenhæng hvori slutproduktet skal anvendes. Organisationen skal skabe sikkerhed for persondata under f.eks. indsamling, opbevaring, ændring, visning, kommunikation og sletning. Den

norske guideline nævner kryptering og adgangskontrol som to typer af PET til at sikre ovenstående. Kravene er også baseret på, hvor risikotolerant organisationen er.

Det næste punkt i vejledningen er design. Det er her, hele databeskyttelsen skal udformes i organisationerne gennem design. De krav, man har identificeret i trinnet inden, skal her opfyldes. Der skelnes her mellem to forskellige designkrav nemlig det dataorienterede og det procesorienteret. Det dataorienterede designkrav indeholder fem underliggende krav, som består af, at man minimerer og begrænser sine data ved at indføre sletteprocedure. Så skal man som det andet krav skjule og beskytte persondata ved hjælp af kryptering, pseudonymisering og aggregering. Det tredje krav er en separering af ens persondata, hvor man opbevarer data i adskilte databaser, enheder, komponenter og områder baseret på deres formål. Det fjerde krav er aggregat, hvor man reducerer detaljerne og følsomheden af personoplysninger vedrørende enkeltpersoner og ved at fjerne unødvendige eller overdrevne oplysninger, når det er muligt. For at illustrere generelle tendenser eller værdier kan man kombinere statistiske data om et stort antal mennesker uden at identificere personer. Det femte og sidste dataorienterede designkrav er databeskyttelse som standard, hvor alle ens indstillinger som standard skal henstille til den mest privatlivsvenlige indstilling. Når man for eksempel installerer en app, skal standardkonfigurationen være, at appen ikke sporer brugerens placering eller deler brugerens data med andre. Hvis brugeren ønsker at bruge sådanne funktioner, skal man aktivt selv vælge at ændre indstillingerne.

Det procesorienterede designkrav består af fire underliggende krav, som først indeholder et informationskrav, hvor IT-systemet formår at informere den registrerede om sine rettigheder og hvordan behandlingen foregår og til hvilket formål. Det skal være i et klart og almindeligt sprog, hvor man også kan bruge billeder, ikoner og symboler til at gøre informationen mere klar og tydelig. Animation, video og lyd kan også være gode værktøjer til at tilpasse information til brugerens forståelsesniveau. Det andet krav er kontrollen. Her menes der, at den registrerede har ret til at kontrollere ens egen persondata, hvor man kan få adgang til denne, lave opdateringer og eller slette ens data. Man kunne her som organisation bruge en menu eller en separat side i ens IT-system til at give og tilbagekalde samtykke, tillade at se, blokere, opdatere og slette egne personlige data. Det tredje krav er håndhævelsen og dokumentation for dette, så der ved en inspektion let kan illustreres, hvordan dette udføres. Man kunne som organisation have en databeskyttelses- eller privatlivspolitik, der beskriver, hvordan softwaren sikrer håndhævelsen af den registreredes rettigheder, hvordan man overholder databeskyttelsesforordningen og hvilke tekniske foranstaltninger, der er på plads for at beskytte persondata. Tekniske foranstaltninger kan herunder omfatte adgangskontrol og kryptering i forhold til en håndhævelse. Det sidste og fjerde krav er i forhold til at demonstrere overholdelsen af forordningen. Her kunne man som organisation vise, at softwaren er udviklet ved hjælp af en metode, der sikrer databeskyttelse ved design og informationssikkerhed (SSDLC, Secure Software Development Life Cycle), rapporter fra sikkerhedsrevisioner, sårbarhedsscanning, sikkerhedstests som penetrationstest og rapporter om udøvelse af databrudstyring.

Når kravene til designet er på plads, skal man i gang med sin kodning som det næste i vejledningens cyklus i forhold til det IT-system, man har i en given organisation. Dette er med til at muliggøre, at udviklere kan skabe sikre koder, hvor man deaktiverer usikre funktioner og moduler og laver en statistisk kodeanalyse og kodeanmeldelse til at sikre databeskyttelse gennem design.

Herefter er man nået til testen i denne cyklus, hvor man kontrollerer, at kravene til databeskyttelse er implementeret som planlagt samt sikre, at kravene er blevet opfyldt korrekt. Man skal herefter afprøve sikkerheden i ens IT-system for at opdage de sårbarheder, der måtte være og sikre at den kodning der er udarbejdet, er tilstrækkelig. I vejledningen anbefaledes der, at man etablerer en

procedure til en automatisk udførelse af test, som man kan køre hver gang, man udvikler sin software. Der er nogle forskellige former for test, som man kan gøre brug af. Dette kunne fx være en dynamisk test, hvor man tester funktionaliteten. Der kunne også gøres brug af en Fuzz-test, hvor der forsætligt udløses fejl i softwaren. Slutteligt kan der gøres brug af en penetrations test (sårbarhedsanalyse), hvor man belyser sårbarhederne i et givent IT-system løbende.

Efter man har testet sine krav og design i sit IT-system, skal man lave en planlægning for, hvordan organisationen effektivt kan klare hændelser, der måtte opstå efter frigivelse, samt procedurer for opdatering af IT-systemet. Der bør udarbejdes en plan for håndtering af hændelser relateret til IT'en. Planen skal indeholde definerede ressourcer og et kontaktpunkt eller responscenter, der kan håndtere henvendelser. Planen skal indeholde relevante kontaktoplysninger til støtte og eskalering, herunder kontaktoplysninger til organisationens databeskyttelsesansvarlige. Der gives et eksempel, hvor software relateret til nødhjælp i sundhedssektoren sandsynligvis vil kræve, at et døgnåbent responscenter er tilgængeligt 365 dage om året. Det er vigtigt at overveje hvilke kommunikationskanaler, der skal bruges til at rapportere hændelser.

Det sidste punkt i den norske vejledning er vedligeholdelse, som betegnes for at være det vigtigste element i denne cyklus. Det er vigtigt, at organisationen har implementeret en plan for håndteringen af hændelsesrespons og at man følger denne. Organisationen skal yderligere være parat til at håndtere hændelser, sikkerhedsbrud og angreb, der kan resultere i brud på fortrolighed, integritet eller tilgængelighed vedrørende personoplysninger. De skal have et responscenter, der kan håndtere hændelser og levere opdateringer, retningslinjer og information til brugere og registrerede.

Afslutningsvis bør det nævnes, at denne vejledning ikke bør diktere en streng, sekventiel og stiv proces for hver aktivitet i udviklingsprocessen. Det bør snarere tilpasses til den specifikke metode, organisationen har valgt at bruge. Organisationer, der udvikler og frigiver software i et hurtigt tempo, bør overveje, hvordan vejledningen bedst kan bruges til at sikre, at der findes grundlæggende databeskyttelses- og sikkerhedsparametre og hvordan databeskyttelse og sikkerhedstest kan indgå i fuldt automatiseret testregimer.

Norge har altså udviklet en meget udførlig vejledning til organisationerne om hvordan, de mener, at man skal håndhæve forordningens artikel 25 i relation til at skabe det bedste resultat og opretholde den rette tillid til de registrerede, som nævnt i afsnit 3.1.2 er Henning Mortensen og Norge dermed enige om, at databeskyttelse gennem design skal være en cyklus der hele tiden kører i ring.

Norge har yderligere afholdt en konkurrence i at skabe den bedste platform for databeskyttelse gennem design. Her konkurrerer det norske erhvervsliv, studerende og professorer for at skabe den bedste platform til håndtering af databeskyttelse gennem design. Dette må også antages at være et taktisk tiltag for den norske tilsynsmyndighed, da det er en god måde at inddrage hele landet til at højne deres indblik og forståelse af databeskyttelse. Selvom det må antages, at Norge har haft en større indgangsvinkel til, hvad der ligger i betydningen af databeskyttelse gennem design, så må en sammenfatning af de forskellige nationers fortolkning kunne fremme til en bedre håndhævelse af databeskyttelse gennem design. I sidste ende skaber dette både ensartethed, som kommissionen ønsker i deres strategi omkring digitalisering af det indre marked og en bedre håndtering af persondata på tværs af landegrænserne. Endnu en faktor der bør overvejes for de enkelte organisationer er, hvorvidt man vil benytte sig af en certificering eller en adfærdskodeks, som nævnt tidligere. Dette kan skabe en tillid til den enkelte organisation i og med, man ved, at de har en god databeskyttelse og har skabt et godt design heraf. Forordningen bruger selv de to begreber i artikel 41 og 42 som værende måder, hvorpå organisationerne kan bevise denne gennemførelse og overholdelse af forordningen.

3.3 Praksis af databeskyttelse gennem design

Selvom der ikke findes en bestemmelse i direktivet, som kan sammenlignes med forordningens artikel 25 (afsnit 2.1.2), er databeskyttelse gennem design ikke et nyt fænomen. Artikel 29-gruppen har udtalt, at direktivets artikel 17 iscenesætter en forpligtelse for den dataansvarlige om at gennemføre de passende organisatoriske og tekniske foranstaltninger. Dette betyder med andre ord, at artikel 17 (i nationalret implementeret i persondataloven, § 41, stk. 3) forpligter medlemsstaterne til at implementere foranstaltninger, som tilvejebringer et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen af data indebærer. Dermed beskytter forordningens artikel 17 personoplysninger mod hændelig eller ulovlig tilintetgørelse, hændeligt tab, forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang. Dette er gældende, når det pågældende system bliver idriftsat, men også tidligere i processen i testfasen er dette nødvendigt. Datatilsynet har i denne sammenhæng udtalt, at test i forbindelse med program- og systemudvikling bør omfatte testdata og dermed kun bero på oplysninger fra fiktive personer og ikke eksisterende personer. Der er et krav fra Center for Cybersikkerhed og Digitaliseringsstyrelsen, at reglerne i persondataloven og den dertilhørende sikkerhedsvejledning ibrugtages allerede inden, behandlingen af personoplysninger sker. Dette anbefales med henblik på at styrke sikkerheden ved IT-driften (Center for Cybersikkerhed og Digitaliseringsstyrelsen, 2014).

Foranstaltninger foretaget på det organisatoriske plan betyder, at den dataansvarlige skal sikre, at personoplysninger ikke kommer uvedkommende til kendskab. Dette kan afværges ved en "clean-desk"-policy. Derved forebygger man, at informationer kommer uvedkommende til kendskab ved at være tilgængelig på eksempelvis HR-ansvarliges skriveborde (Justitsministeriet, 2017). Det er uden tvivl det menneskelige element på det organisatoriske plan, som især er en stor og betydningsfuld faktor. I afgørelsen af en sag mellem Datatilsynet og Sønderborg Kommune om manglende sikkerhed ved transmission af fortrolige og følsomme oplysninger via e-mail (j.nr. 2014-313-0389) sendte en ansat ved Sønderborg Kommune en ikke krypteret e-mail med fortrolige og følsomme oplysninger i strid med persondataloven. Sønderborg Kommune bekræfter, at e-mailen blev sendt ikke krypteret grundet en forglemmelse hos medarbejderen. Jf. persondatalovens § 41, stk. 3, skal den dataansvarlige træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Hertil kommer sikkerhedsbekendtgørelsens § 14, som understreger, at der kun må etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger. Dette indebærer netop, at en offentlig myndighed som Sønderborg Kommune ikke må sende fortrolige og følsomme personoplysninger på e-mail, uden at denne er blevet krypteret. Derfor lever Sønderborg Kommune ikke op til de fornødne sikkerhedsforanstaltninger i persondatalovens § 41, stk. 3. jf. sikkerhedsbekendtgørelsens § 14. Dette finder Datatilsynet meget kritisabelt og henstiller derfor Sønderborg Kommune til at ændre praksis til fremover udelukkende at sende fortrolige og følsomme personoplysninger via e-mail i krypteret form. Dette kan derfor betragtes som et minimumskrav for praksis ved fremsendelse af e-mails indeholdende fortrolige og følsomme personoplysninger (Datatilsynet, 2014).

Sagen med Sønderborg Kommune er især interessant, da Datatilsynet tidligere (j.nr. 2011-313-0438) har rettet henvendelse til kommunen grundet deres fremsendelse af e-mails indeholdende fortrolige og følsomme personoplysninger i ikke krypteret form. Ved denne lejlighed i 2011 oplyste direktionen i Sønderborg Kommune i en redegørelse af d. 9. december 2011, at reglerne for transmission af fortrolige og følsomme oplysninger via e-mail blev overholdt, samt at det var blevet besluttet at opprioritere viden om afsendelse af sikker e-mail i kommunen og at vicekommunaldirektøren i denne forbindelse havde henstillet til, at samtlige ledere i Sønderborg Kommune

sikrede, at alle medarbejdere i kommunen ville overholde persondatalovens regler. Ydermere blev der i redegørelsen d. 9. december 2011 vedhæftet en vejledning til, hvordan man fra Sønderborg Kommunes side sender fortrolige og følsomme oplysninger til borgere, organisationer m.fl. Denne vejledning blev også lagt ud på Sønderborg Kommunes intranet. Lederne i kommunen blev ligeledes bedt om senest d. 18. november 2011 at give medarbejderne instrukser om, hvorledes fortrolige og følsomme oplysninger udsendes via krypteret e-mails. Trods alle disse anstrengelser og forsøg på at instruere medarbejdere, og dermed styrke de organisatoriske foranstaltninger for at sikre fremsendelse af e-mails med fortrolige og følsomme oplysninger, skete en menneskelig fejl (j.nr. 2014-313-0389) på netop dette område som følge af forglemmelse i selv samme kommune. Datatilsynet udtrykker i denne forbindelse en bekymring, da Sønderborg Kommune har dokumenteret implementering af sikkerhedsmæssige foranstaltninger, men alligevel fejler og giver anledning til en række sager (Datatilsynet, 2014). Det må altså hermed konstateres, at Sønderborg Kommunes sikkerhedsmæssige foranstaltninger på det organisatoriske plan ikke har været tilstrækkelige og at minimumskrav i praksis kræver, at enhver e-mail indeholdende fortrolige og følsomme oplysninger udelukkende sendes i krypteret form.

På det tekniske plan kan det være foranstaltninger, som underbygger "indbygget privatlivsbeskyttelse", som skal gennemføres. Dette kan ske ved at app-udviklere, app-butikker, OS- og enhedsproducenter skal tage højde for principperne om at indbygge databeskyttelse som standard i enhederne, udtaler Artikel 29-gruppen (Justitsministeriet, 2017).

Af konkrete krav til beskyttelse af personoplysninger i offentlige myndigheder, findes autorisation, logning og at der videregives de nødvendige instrukser til medarbejdere. Disse organisatoriske og tekniske foranstaltninger beror ikke på en risikovurdering, men påkræves uanset hvordan den pågældende myndighed er indrettet. Hertil kommer yderligere sikkerhedsforanstaltninger som adgangsbegrænsning, som er et eksempel på databeskyttelse gennem design og standardindstillinger (Justitsministeriet, 2017).

Det tidsmæssige perspektiv i forhold til, hvornår de fornødne organisatoriske og tekniske foranstaltninger skal være indtruffet, er ikke fastsat. Det er kun oplyst af Datatilsynet, at foranstaltningerne skal forberedes og implementeres forud for, at en behandling påbegyndes. Dette omfatter også testefasen som nævnt ovenfor. Dog findes der nogle foranstaltninger, som fx fuld test af backup systemer, som først er muligt efter behandling af personoplysninger (Justitsministeriet, 2017).

I Datatilsynets praksis findes eksempler på behandlingsbetingelser som de registreredes rettigheder, legalitetsprincippet og sikkerhedskrav, som skal inkorporeres ved udvikling af systemer og digitale løsninger. I denne forlængelse skal en udtalelse fra Datatilsynet omhandlende en sag (Datatilsynets j.nr. 2015-631-0108) om login til helbredsoplysninger på sundhedsområdet nævnes, hvor brugere havde mulighed for at oprette en personlig helbredsboks med adgang til helbredsoplysninger fra læger på en hjemmeside. Sagen udsprang af, at Datatilsynet blev bekendt med, at en person havde været udsat for, at personoplysninger vedrørende den pågældendes sundhedsprofil på hjemmesiden Cure4you var blevet offentliggjort. I denne sag gjorde Datatilsynet det klart, at den anvendte løsning på hjemmesiden med login baseret på brugernavn (personnummer) og adgangskode ikke var tilstrækkeligt og dermed ikke levede op til den grad af sikkerhed, som var nødvendig, når det gælder adgang til følsomme personoplysninger inden for sundhedsområdet (Datatilsynet, 2015).

Cure4you har oplyst, at der forud for etableringen af systemet er foretaget en grundig risikovurdering, hvilket har betydet, at hjemmesiden er krypteret, password (personnummer) gemmes krypteret og separat, der gøres brug af firewall samt en række sikkerhedsprocedurer i Cure4you's supportcenter, som har til formål at sikre, at password eller andre data kun udleveres til den rette

person. Der foretages derudover logning i Cure4yous bagvedliggende system, som kan afsløre misbrug. I forbindelse med oprettelse af en ny profil i Cure4yous database, har Cure4you oplyst, at brugeren danner en personlig adgangskode samt et personligt sikkerhedsspørgsmål med dertilhørende personligt svar. Adgangskoden skal være på minimum seks tegn. For at adgangskoden ikke fremstår læsbar i adgangskodefeltet, skjules koden i skrivefeltet af prikker. Yderligere skal den nyoprettede kode indtastes to gange som bekræftelse af sikkerhedsmæssige årsager. Tastes en adgangskode eller et personnummer forkert ind tre gange i træk, er systemet opbygget på en sådan måde, at der spærres for adgang i de følgende ti minutter. Dette er en foranstaltning, som er foretaget for at beskytte imod maskinhackere eller lignende misbrug. Samme procedure gør sig gældende ved forkert indtastning af svaret på sikkerhedsspørgsmålet. Skulle brugeren glemme sin adgangskode, kan man anmode systemet om en ny midlertidig engangskode til den mailadresse, som er tilknyttet brugeren i Cure4yous system. Den nye midlertidige kode fremsendes først, når brugeren har indtastet sit personnummer samt svaret på det personlige sikkerhedsspørgsmål. Dette svar skal skrives præcist, som det er blevet oprettet, da systemet sondrer mellem store og små bokstaver (Datatilsynet, 2015).

Til trods for Cure4yous ihærdige forsøg for at imødekomme sikkerhedsforanstaltninger for at beskytte persondata for brugere af deres system, vurderer Datatilsynet, at når der er tale om denne type kommunikation mellem patienter og læger, ikke er tale om de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger. Persondatalovens § 41, stk. 3 fastslår, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Dette er Datatilsynets opfattelse, at den anvendte løsning med login baseret på brugernavn og adgangskode ikke i tilstrækkelig grad lever op til den sikkerhed, som må kræves, når et system giver adgang til følsomme personoplysninger inden for sundhedsområdet. For visse brugere kan der være tale om en betydelig mængde følsomme personoplysninger. I forhold til sammenlignelige løsninger i praksis er der stillet krav om, at adgang via internettet baseres på NemID eller en anden løsning med flere faktorer (Datatilsynet, 2015). Det blev altså i denne sag vurderet fra Datatilsynets side, at der i praksis er minimumskrav om adgang gennem NemID ved følsomme personoplysninger inden for sundhedsområdet.

I et høringssvar (Datatilsynets j.nr. 2013-112-0268) fra Datatilsynet, opfordrer de til et lovforslag fra Digitaliseringsstyrelsen om obligatorisk selvbetjening til at udforme de nødvendige forretningsgange og løsninger til, at borgerne kan stole på, at deres persondata til enhver tid opnår den fornødne beskyttelse. Datatilsynet mener, at beskyttelsen af privatliv og personoplysninger burde indgå som en integreret del af udviklingen af det pågældende system - med andre ord, skal der gøres brug af databeskyttelse gennem design eller privatlivsfremmende teknologier. Yderligere er der ifølge Datatilsynet et behov for, at borgeren får rettigheder til selv at bestemme, hvor beskyttelse af persondata er relevant. Desuden er en transparent tilgang over, hvilke data der behandles, vigtig, således at brugeren selv har et overblik over, hvem der har adgang og anvender personoplysningerne (Justitsministeriet, 2017).

God databehandlingsskik medfører jf. Datatilsynets j.nr. 2007-632-0014, ligesom ovenstående (Datatilsynets j.nr. 2013-112-0268), at borgeren skal kunne stole på, at deres persondata til enhver tid opnår den fornødne beskyttelse. Dette var i imidlertid ikke tilfældet i Datatilsynets j.nr. 2007-632-0014, hvor Københavns Universitet i 2009 ved en fejl offentliggjorde oplysninger om studerendes personoplysninger på universitets hjemmeside. Der var tale om 39 studerendes personnumre, holdinddelinger, navne, privatadresser, telefonnumre og e-mailadresser, som blot ved søgning på ordet ”cpr” på Københavns Universitets hjemmeside blev vist. Der var altså dermed tale

om en ringe håndtering af de studerendes personoplysninger, brud på persondataloven og dårlig databehandlingsskik. Yderligere fandt datatilsynet en liste med oplysninger om 50 studerendes deltagelse i eksamen med personnumre. Københavns Universitet har til sagen oplyst, at personoplysningerne relateret til de 39 studerende ved en beklagelig fejl fik tilføjet personnumre ved en opdatering af siden. Oprindeligt var det ikke meningen, at personnumrene skulle angives, da de blev lagt på internettet. Efter Datatilsynets indblanding blev personnumrene straks fjernet. Efterfølgende blev privatadresser, telefonnumre og e-mailadresser ligeledes fjernet, hvorefter listen af de 39 studerende kun indeholdt oplysninger om de deltagendes navne (Datatilsynet, 2007).

Som modsvar til Datatilsynet, har Københavns Universitet oplyst, at de studerende selv har givet deres personoplysninger til underviseren med det formål, at underviseren som en service til de studerende skulle udarbejde en oversigtsliste. Underviseren var imidlertid ikke klar over, at de oplysninger, som de studerende oplyste, ikke måtte offentliggøres uden de studerendes udtrykkelige accept. Københavns Universitet har oplyst de berørte studerende om, at oplysningerne var offentligt tilgængeligt, men at de nu er fjernet (Datatilsynet, 2007).

Listen med de 50 studerendes deltagelse i eksamen samt personnumre, oplyste Københavns Universitet ligeledes var sket ved en beklagelig fejl, hvorefter siden er blevet krypteret. De berørte studerende i dette forhold er ligeledes blevet informeret. Det er fra Datatilsynets side blevet konstateret, at siden ikke længere er tilgængelig, hvorefter Københavns Universitet bestræbelser derfor har afhjulpet sagen. Som en reaktion på hele Datatilsynets indblanding som følge af problematikkerne omkring offentlige personoplysninger, har Københavns Universitet udsendt en e-mail til alle enheder relateret til universitet med gældende regler på området. Der blev heri grundigt orienteret om behandling af personoplysninger. Ydermere bliver de berørte hjemmesider løbende kontrolleret for at sikre, at reglerne bliver overholdt (Datatilsynet, 2007).

Datatilsynet er af den opfattelse, at når der er tale om en potentiel risiko for offentliggørelse af følsomme og fortrolige oplysninger, skal der udvises en særlig påpasselighed. Denne påpasselighed skal afspejles i tilrettelæggelsen af arbejdsgange samt ved indretning af myndighedernes systemer. Dette underbygger behovet for databeskyttelse på både det organisatoriske- og det tekniske plan, som er behandlet tidligere i dette afsnit. Datatilsynet finder ikke, at Københavns Universitet har udvist den nødvendige påpasselighed eller omhu ovenpå offentliggørelse af i alt 89 studerendes personoplysninger. Dermed har Københavns Universitet ikke overholdt kravene, som følger af persondatalovens § 41, stk. 3, hvilket Datatilsynet finder meget beklageligt, da de henviser til, at offentliggørelse af personoplysninger indeholdende personnumre vil kunne få alvorlige konsekvenser for de berørte studerende (Datatilsynet, 2007).

Som følge af kravene fra den nye forordning bliver ovenstående blot minimumskrav for praksis af databeskyttelse gennem design. Derfor vil den fremtidige praksis kun blive yderligere skærpet. Når den nye forordning træder i kraft d. 25. maj 2018, bliver der efter al sandsynlighed tale om en langt strengere tendens for praksis til trods for, at ovenstående kan give et udtryk for, at praksis inden d. 25. maj 2018 i forvejen havde høje krav til beskyttelse af personoplysninger.

3.4 Delkonklusion

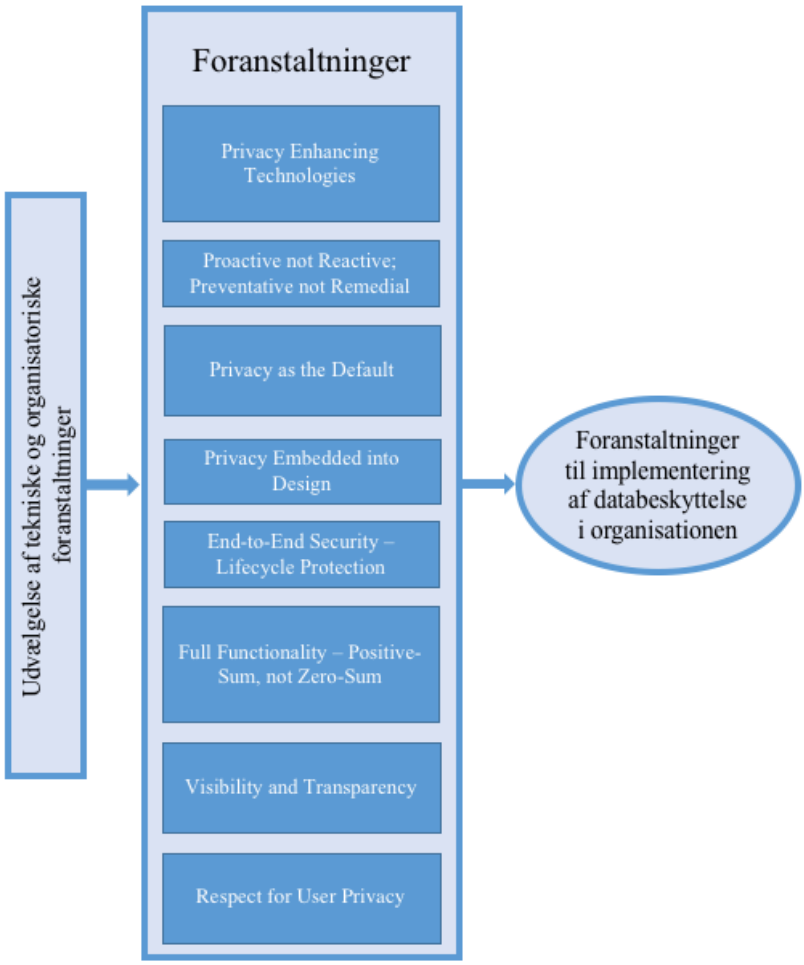
Ud fra ovenstående afsnit om brugen af juridiske virkemidler til at varetage sikkerheden for personoplysninger ud fra artikel 25, stk. 1, kan det sammenfattes, at det ikke er tilstrækkeligt at iværksætte sikkerhedsforanstaltningerne, de skal også følges op på og kontrolleres. Men for at være sikker på, at der er taget de nødvendige skridt til at skabe et sikkerhedssystem tilpasset behovet for

sikkerhed, dannes dette bedst gennem databeskyttelse gennem design. På den måde kan organisationerne med fordel benytte sig af Dr. Ann Cavoukians syv principper, som er en metode til proaktivt at beskytte personoplysninger gennem designspecifikationer for informationsteknologier, netværksinfrastruktur og forretningspraksis. I forhold til de tekniske sikkerhedsforanstaltninger må det antages, at organisationerne kan tage udgangspunkt i udarbejdelsen af PET-håndbogen, som giver en række tekniske foranstaltninger, som er relevante i organisationerne. Sideløbende med PET-håndbogen finder ENISA en måde at tilvejebringe løsningen på et generelt designproblem inden for en bestemt sammenhæng. På den måde understøtter ENISA raffinering af delsystemer eller komponenter i et system.

Den danske betænkning nr. 1565 ligger op til, at man på nuværende tidspunkt skal bibeholde sine nuværende IT-systemer og fokusere på de organisatoriske sikkerhedsforanstaltninger. Betænkningen er noget af det eneste materiale, som findes som en fortolkning af forordningens artikel 25 stk. 1 i Danmark. I modsætningen til Danmark, har man i Norge en større tilgang til databeskyttelse gennem design, hvor man har lavet en syvtrins vejledning, med eksempler på hvordan organisationerne kan opnå at blive compliance. Dette er et resultat af, at Norge har større sanktioner i deres "personopplysningslov", og befinder sig uden for EU.

Når det kommer til praksis på området om databeskyttelse gennem design, er dette først muligt at undersøge efter d. 25. maj 2018. Men ud fra hvad der tidligere er blevet brugt som minimumskrav til praksis på området, er det klart, at de krav og foranstaltninger, som kommer til at dominere, vil være omfattende for organisationerne. Dette gør sig gældende både på det organisatoriske- og forretningsmæssige plan, da der er høje krav til beskyttelse af personoplysninger.

Ovenstående er alle tiltag, der skal bruges forskelligt på baggrund af en konkret konsekvensanalyse i de enkelte organisationer. Det handler derfor for organisationerne om at få indkørt en cyklus, hvor man konstant kører i ring og hele tiden tilpasser sine IT-systemer og organisationen generelt, til at kunne overholde databeskyttelse gennem design. For at skabe en bedre visuel oversigt over de vigtigste juridiske foranstaltninger, er der i denne afhandling valgt at udforme en juridisk figur (figur 2), som skal ende ud i et endeligt og brugbart framework under diskussionsafsnittet til organisationerne i praksis.



Figur 2. Kilde: Egen tilvirkning. (Denne figur er udviklet med inspiration fra Nijssen, M. et al., "HRM in turbulent times: How to achieve organizational agility", The international journal of human resource management, 2012, se bilag 4).

Del IV – Erhvervsøkonomiske ramme – Agilitet

4.1 Drivkræfter i organisatorisk agilitet under databeskyttelse gennem design

Organisatorisk agilitet anses for at være en god egenskab for organisationerne at være i besiddelse af, da det hjælper dem til at tilpasse sig forandringer, som både kan være interne og eksterne faktorer. Der er dog ikke nogen præcis formular eller metode for udviklingen af en agil organisation (Harraf et. Al., 2015). Men det kan være svært at gennemskue anvendelsen af organisatorisk agilitet i alle implementeringsprojekter i en organisation. At få et menneske til at ændre deres vaner kan være svært, og det kan udsætte organisationen for vanskeligheder, når det er i form af en lovændring som er påkrævet hos alle. Dette afsnit vil derfor belyse, hvordan man som organisation kan gøre brug af den organisatoriske agilitet til implementeringen af databeskyttelse gennem design og dermed opnå det bedst mulige resultat både i forhold til lovgivningen, men også i forhold til ens medarbejdere og organisationen som helhed.

Agilitet kan deles ind i to områder, nemlig fleksibilitet og forandringsvillighed. Der er mange forskellige omstændigheder, som spiller ind, når man skal opnå agilitet i organisationen. Disse

omstændigheder kan defineres ud fra nogle forskellige drivkræfter, som samlet set skal opnå organisationens mål og danne en kerne for organisationens agilitet. Agilitet er vigtigt, da det er essentielt i forhold til at opnå effektivitet. Agiliteten skaber en høj performance for organisationen. Det vigtigste at have i mente ved en agil fremgangsmåde er menneskerne, teams og organisationens overordnede kultur (Harraf et. Al., 2015). En organisations udvikling er utrolig vigtig, da den teknologiske verden er i konstant vækst. Det er vigtigt, at alle i organisationen har viden for at øge hastigheden på at tilpasse sig forandringer. Dette er noget, der både bliver nævnt i interviewet med den dataansvarlige i virksomhed Y og i interviewet med den rådgivende advokat (bilag 1 og 3). Her siger de begge, at der en sammenhæng mellem, hvor interesseret man er i forandringer og ens uddannelsesniveau (bilag 1, spm. 7 og bilag 3, spm. 41). Jo højere akademisk uddannelse man har, jo mere forstående er man over for en lovgivende forandring i organisationen. Så det er vigtig for ledelsen af have alle medarbejdere med.

Derfor er det relevant at analysere, hvilke af de tidligere beskrevet drivkræfter i organisatorisk agilitet (afsnit 2.2.3) der har størst betydning for implementeringen af forordningens artikel 25. De mest relevante drivkræfter med størst indflydelse på implementeringen vil i det følgende blive udvalgt (med symbolet: ✓) og sammenkoblet med resultaterne fra de udarbejdede interviews.

#	Drivkræfter:	Vigtigheden af organisatorisk agilitets betydning for implementering af forordningen s artikel 25:	
1	Culture of Innovation	Kulturændringer gennem politikker implementeres som del af de organisatoriske foranstaltninger i forordningens artikel 25.	✓
2	Empowerment	Lederen giver sine medarbejdere ejerskab gennem ansvar over de opgaver, de får om databeskyttelse gennem design (bilag 2, spm. 6).	✓
3	Tolerance for Ambiguity	Denne drivkraft spiller en rolle i forhold til at implementeringen af forordningen, da der kan forekomme stor tvetydighed omkring vigtigheden af projektet blandt medarbejdere.	X
4	Vision	Den overordnede vision er at få lavet en generel udredning af indholdet i forordningens artikel 25 og ud fra det få den implementeret i organisationen.	X
5	Strategic Direction	Eftersom organisationerne har haft to år til at implementere forordningen fra maj 2016 til maj 2018, er det en drivkraft, at de har haft et tydeligt og skarpt fokus, da Danmarks bevidsthed omkring databeskyttelse er gået fra 0 til 100 (bilag 2, spm. 11).	✓
6	Change Management	Forandringsledelse i forhold til implementeringen af forordningen igennem organisatorisk agilitet opstår i de Gap-analyser, der udarbejdes. Forandringsledelsen kommer til sin ret i form af, at man lægger ansvaret ud til medarbejderne i højere grad (bilag 2, spm. 6).	✓
7	Communication	Det er vigtigt ved en implementering af forordningen i organisationen, at ledere kommunikerer ændringer i øjenhøjde med medarbejderne og ikke som hierarki.	✓
8	Operations Management	Anerkendelse af hvad den enkelte medarbejder beskæftiger sig med for at få dem til at forstå baggrunden for databeskyttelse gennem design.	X
9	Structual Fluidity	Kortlægning af organisationens dataflow for at finde frem til, hvad/hvor/hvordan persondata behandles i de enkelte afdelinger.	X
10	Development of organizational learning	At anlægge en positiv vinkel til medarbejderne gennem vidensdeling, ved at involvere dem og lade dem påvirke resultatet.	✓
11	Scalable workforce	Arbejdsstyrken og generelt de menneskelige ressourcer formår at tilpasse sig. Dette er betinget af, at der er en forståelse for grundlaget for implementeringen.	✓
12	Highly adaptable organizational infrastructure	Det er vigtigt, at man har en infrastruktur i organisationen, hvor medarbejderne ikke føler de får trukket en masse juridisk ned over hovedet fra den juridiske afdeling.	✓

Tabel 2. Kilde: Egen tilvirkning.

Der er i ovenstående tabel 2 udvalgt 8 drivkræfter, baseret på deres relevans for implementering af databeskyttelse gennem design fra et agilt udgangspunkt. Udvælgelsen er sket på baggrund af de praktiske erfaringer, som de tre interviews (bilag 1 – 3) biddrog med, og hvor der måtte antages at være en manglende fleksibilitet og forandringsvillighed. De 8 udvalgte drivkræfter vil i det følgende blive gennemgået og sammenkodes med den praktiske tilgang, som de tre interviews bidrager med.

4.1.1 Culture of Innovation

Det har gennem alle tre interviews været et gennemgående tema, at organisationernes agile håndtering og -evne til at sørge for implementeringen af forordningen har været stærkt præget af kulturen i den pågældende organisation. Når en organisation ændrer noget så fundamentalt som medarbejderes arbejdsgange, det er ikke noget, som gøres uden videre. Derfor afhænger en succesfuld implementering af medarbejdernes vilje, tilgang og i allerhøjeste grad agilitet i forhold til at adoptere nye arbejdsgange. Disse forhold er noget, der er rodfæstet i det enkelte individ, nøjagtigt som med kultur.

> ”*… så selve kulturændringerne, systemændringerne og hvad ved jeg, det tager tid*” (bilag 1, spm. 3).

Når det på internationalt plan er besluttet, at databeskyttelse inden for fællesskabets grænse skal højnes gennem forordningen, er det en implementering og ændring af jura, som vedrører mange forskellige typer af kultur. Nogle mere agile anlagt end andre.

> ”*Vi har en tysk advokat ansat her, han er helt blown away, når han hører, hvordan det er, tingene de foregår i Danmark. Han kunne aldrig nogensinde drømme om, når han går til frokost ikke at låse sin computer inde*” (bilag 2, spm. 10).

Forestående citat er et af de tydeligste eksempler på, at ganske almindelige forretningsgange for én kultur, kan synes ganske overdrevet for en anden. Medarbejderens kulturelle baggrund er umulig at negligere, og at denne kulturelle baggrund skulle være ubetydelig, er direkte forkert.

> *”… det også lidt kulturelt bestemt, om man tager lidt mere laissez faire på lovkravene eller om man er meget stringent. Der er polakkerne mere detaljeret, end man er fx i Danmark. I Tyskland og Polen har jeg helt klart set, at man er mere stringent. Jeg tror også, at det er fordi de har en lidt anden tilgang til databeskyttelse.*” (Bilag 3, spm. 15).

Ud fra denne udtalelse, er det klart, at forandringsparathed ved brug af eksterne drivkræfter (forordningen) til at fordre forandring bliver betydeligt påvirket af kulturelle baggrunde. Evnen til at gøre nye ting og evnen til at gøre gamle ting på nye måder er foranderlig og en af de ting, som udfordrer kulturændringer i aller højeste grad. Kulturændringer skal foregå:

> ”*… gennem nogle meget direkte og pædagogiske politikker.*” (Bilag 1, spm. 7).

Disse politikker er en del af de organisatoriske foranstaltninger i forordningens artikel 25.

En ting er, hvordan en given kultur modtager ændringer i forretningsgange som følge af en forandring som implementering af forordningen. En anden ting er, hvordan en given kultur modtager selve introduktionen og præsentationen af en forandring som implementering af forordningen.

> ”*I nogle af kulturerne kan jeg godt mærke, at jeg ikke er øverst i hierarkiet (qua lav anciennitet og kvinde), så det er nemmere når man har snakket med folk.*” (Bilag 3, spm. 40).

Derfor er det ganske tydeligt, at der findes klar evidens for, at den kulturelle bagage har en betydelig indflydelse for organisationernes agilitet i forbindelse med implementering af den nye forordning.

4.1.2 Empowerment

For at skabe den bedste implementering af databeskyttelse gennem design er det vigtigste forhold mellem ledere og medarbejdere, at man som leder giver sine medarbejdere ejerskab over de opgaver de får (bilag 2, spm. 6). Det vigtige i denne drivkraft er effekten af decentralisering og centralisering i forhold til beslutninger. I et af de interviews, som blev gennemført i forbindelse med udfærdigelse af nærværende afhandling, var håndteringen af netop denne drivkraft lagt klart op til at skulle blive et resultat af decentralisering.

> *”Jeg giver dem en opgave, og det er noget jeg har fundet ud af hen af vejen, at det er den eneste måde, at jeg har kunnet gøre det på. De skal have ejerskab i processen, og den eneste måde, at man kan få folk til at få ejerskab, det er hvis de forstår vigtighed*

og hensynene og at de også forstår, at det også er en interesse for virksomheden som sådan, og at det faktisk bliver prioriteret af deres managers." (Bilag 2, spm. 6).

I virksomhed X er håndteringen af implementeringen af forordningen blevet et klart resultat af, at man har overdraget myndighed og dermed skabt selvstændighed. Denne decentralisering i virksomhed X har givet et godt og effektivt resultat:

"*Men jeg tror helt klart, at det har gjort en forskel, at det kommer fra deres egen leder.*" (Bilag 2, smp. 8).

Ved ikke at trække den nye forordning og dennes forandring af arbejdsgange ned over hovedet på medarbejderne, har virksomhed X skabt en mere agil organisation som helhed. Denne betragtning underbygges af Teori O, som er udviklet af to akademiske professorer fra Harvard University, som har gennemført 40 års forskning i forandringsledelse. Teorien bygger på, at forandringer fra et organisatorisk perspektiv har et formål om at forbedre medarbejdernes indbyrdes tillid og samarbejde samt hele organisationens kultur. Resultatet af en forbedring af medarbejdernes indbyrdes tillid og samarbejde og organisationens kultur giver det resultat, at organisationen opnår større agilitet. Dette begrundes og understøttes med, at organisationens evne til at omstille sig i takt med skiftende forandringer forbedres (Beer, M. og Nohria, N., 2000). Det er derfor klart, at både Teori O og virksomheds Xs tilgang til implementering af den nye forordning er grebet an på en sådan måde, at drivkraften om empowerment understøttes, hvormed organisationens agilitet forbedres bedst muligt.

4.1.3 Strategic Direction

Ud over at vurdere hvilke drivkræfter der er relevante for medarbejderne og for at skabe en agil organisation, er det også relevant at inkludere ledelsen i organisationen. Hvilken strategisk retning, de bevæger sig i, kan være afgørende for, hvordan deres oprindelige vision om at skabe databeskyttelse gennem design bliver succesfuld. Det er en konstatering, at man i de danske organisationers bevidsthed omkring databeskyttelse er gået fra 0 til 100 (bilag 2, spm. 11). Derfor er denne drivkraft vigtig i organisationernes søgen efter at blive agile ved implementeringen af databeskyttelse gennem design. Værktøjet i denne drivkraft er dermed et engement i fokusset på at opnå det ønskede optimale mål. Det vil altså sige, at man på ledelsesniveauet i organisationen skal have et skarpt og tydeligt fokus, som dermed skaber den strategiske retning for implementeringen af databeskyttelse gennem design. Fokusset er også med til at underbygge en klar indikation af, hvordan den dataansvarlige skal forholde sig til ledelsen. Formår en ledelse at opnå dette fokus, må det også antages, at den dataansvarlige har følelsen af en opbakning på alle de nye tiltag og dermed også en bedre indgangsvinkel til de resterende medarbejdere, som skal ændre deres normale arbejdsprocesser.

I forhold til ledelsens fokus har det ud fra interviewene været en klar indikation af mangel på dette område til at begynde med. Virksomhed Y udtaler blandt andet følgende:

"Så i starten var det rigtig svært i forhold til ledelsen, men fra december af har jeg ikke haft svært i at få lydhør, fordi folk stresser over det nu, da de ikke føler, at man er kommet langt nok. De vil gerne have krydset nogle flueben af, uden de behøver at gøre så meget." (Bilag 3, spm. 30).

Her må det antages, at ledelsen først har fået fokus, efter det er gået op for dem, at det snart blev den 25. maj 2018. Virksomhed X udtaler sig også på dette område og siger blandt andet følgende:

> *"…nu snakker jeg om den der stearing komiteen, som jeg rapporterer indtil, som er vores C level managers. De har om nogen, fordi det er stor en opgave og fordi de har så meget andet, nedprioriteret det. Og måske givet udtryk for at så længe vi har en plan den 25. så er det okay. Hvor at det nogle gange er frustrerende og nogle gange gør mit arbejde mere besværligt. Jeg vil ikke sige, at jeg har fuld blowen support, hvor de har sagt, at vi bare skulle gå i krig med det samme. Der har helt klart været skepsis til det."* (Bilag 2, spm. 14).

Der er altså en klar indikation af, at man som ledelse har nedprioriteret forordningen og ikke haft det nødvendige fokus fra starten, så man som dataansvarlig har kunnet opfylde sit formål og det har gjort arbejdet mere besværligt. Derfor må det konkluderes, at denne drivkraft er utrolig vigtig i forhold til ledelsesniveauet for at opnå den bedst mulige implementering af databeskyttelse gennem design via en organisatorisk agilitets tilgang.

4.1.4 Change Management

Forandringsledelse er en sammenfatning af mange af de andre drivkræfter, da alt i en organisation kan blive ramt af en form for forandring, uanset om det er eksterne forhold eller interne forhold. Derfor er denne drivkraft en af de helt essentielle i denne afhandling. Formår en organisation at håndtere denne drivkraft, så kan alle de andre drivkræfter også håndteres succesfuldt (Harraf et. Al., 2015).

Forandringsledelse i organisatorisk agilitet skaber en sammenhæng mellem det overordnede mål, altså visionen, og forholdet mellem lederne og medarbejderne, da man giver medarbejderne ejerskab over selv at håndtere de huller, de har i deres afdeling i forhold til passende organisatoriske og tekniske sikkerhedsforanstaltninger. Dermed får man inddraget alle i vigtigheden af forordningen og databeskyttelse samtidig med, at organisationen får mulighed for at effektivisere nogle arbejdsgange, og i fremtiden har en bedre forudsætning for at være mere fleksibel ved korrektioner og forandringer.

Denne afhandling ønsker at give et billede af, at implementeringen af databeskyttelse gennem design ikke kun er en juridisk vurdering, men også problematikken omkring den store forandring det medfører i organisationerne. Den dataansvarlige i virksomhed X siger blandt andet følgende:

> *"… det tror jeg er svært for danskere at forstå, fordi vi har jo ikke den der datahygiejne, som de har i andre lande… Det er i hvert fald mit indtryk, at det er der mange mennesker, der slet ikke kan forstå problemet i, og som synes, at det her er totalt overgearet. Og at der går Bruxelles i den. Men det er et udtryk for, at vi går fra 0 til 100 i vores bevidsthed om databeskyttelse."* (Bilag 2, spm 11).

Med det sagt så kan det antages, at man i Danmark ikke har haft en særlig stor bevidsthed omkring databeskyttelse og derfor er håndteringen af forandringsledelse meget vigtig, da det er så nyt for mange organisationer lige pludselig at skulle tage hensyn til. Som nævnt tidligere i nærværende afhandling, så består forandringsledelse i agile organisationer af tre dele herunder opfattelse af ændringen, implementering af ændring og testændring (Harraf et. Al., 2015). Disse tre dele synes egentlig at være tre lette ord at forstå alment, men håndteringen af dem i praksis kan være svært. For hvordan får man medarbejderne til at efterleve kravene i databeskyttelse gennem design? Det er ikke længere bare et spørgsmål om en IT-afdeling, som sikrer organisationen, nu er det også på det organisatoriske plan, at man skal kunne efterleve reglerne og derfor er det vigtigt, at medarbejderne er med i denne implementering. Som nævnt tidligere har det i praksis været utrolig svært, både ved virksomhed X og virksomhed Y er der ytret problemer omkring efterlevelsen af deres

krav til processer og politikker, som de skal indføre jf. forordningen. De siger blandt andet følgende:

> *"… det sværeste i den her stilling det ville være helt konkret at vurdere reglerne og finde ud af, hvornår gælder dét, hvornår gælder dét? Men det sværeste, det er at få organisationen med. Det er det uden tvivl."* (Bilag 2, spm. 4). *" Ved nogen har vi fået meldingen om, at det ikke er en prioritering for dem. Her er jeg så nødt til at gå op i systemet igen og bruge nogle med flere stjerner på skulderne for at få medhør. Og det har jeg gjort tit, for at sige det pænt." (*Bilag 3, spm. 27).

Der har dermed været nogle helt klare udfordringer i forhold til den forandring, der skulle til i dette projekt i organisationerne og man har som den dataansvarlige hele tiden haft ledelsen til at skære igennem. Det kan dermed konstateres, at implementeringen af databeskyttelse gennem design ikke kun er et juridisk problem, som skal løses, men i den grad også et organisatorisk problem. Derfor spiller denne afhandlings tankegang omkring organisatorisk agilitet en helt klar og essentiel rolle i forhold til den organisatoriske implementering. Dette har den dataansvarlige i virksomhed X haft samme mening om.

> *"Og den indgangsvinkel, jeg har haft til Gap-analyserne, har været, at netop for at undgå, at det bliver mig, der sidder og dikterer, hvad de skal gøre. Jeg kom ud i nogle scenarier, hvor jeg slet ikke kender de medarbejderes daglige arbejde godt nok til at give et bedre bud på, hvordan de kan løse deres opgaver på en GDPR compliant måde, end de selv gør. Så min indgangsvinkel har faktisk været at lægge ansvaret ud til dem i højere grad og så i højere grad at få dem til at forstå principperne."* (Bilag 2, spm. 6).

Her var der en klar indikation af, at man ikke kom nogen vegne hos medarbejderne ved at diktere, hvad de skulle gøre. I stedet for brugte man Gap-analysen til at opnå dette.

> *"Så jeg har egentlig prøvet, når jeg har snakket med folk at bruge en del tid på at sætte dem ind i kernen i lovgivningen og hvilke hensyn vi forsøger at varetage og så sige til dem: "I forhold til det I gør nu, hvordan kan vi gøre det bedre for ligesom at tage hensyn til de databeskyttelsesprincipper, som er i lovgivningen?""* (Bilag 2, spm. 6).

På den måde har den dataansvarlige i virksomhed X sat stor fokus på at møde medarbejderne i øjenhøjde, hvilket har haft en både positiv og effektiv effekt på implementeringen af forordningen.

> *"Min teori er, at hvis det bare kommer ovenfra og ned, så er der mindre sandsynlighed for, at medarbejderne følger det, end hvis de selv er med i beslutningsprocessen, med i udviklingen, altså policy-arbejdet, med i afregningen af hvor man kan få mest value for den ændring, som man nu lægger for dagen. … Så hele den her baggrundsforståelse det er det primære. Så det bliver ikke bare taget ud af hænderne på dem.*" (Bilag 2, spm. 6).

Beviset i forhold til tilstedeværelsen og aktualiteten af problemstillingen i denne afhandling har dermed i praksis vist sig at være tydelig at genkende for organisationerne. Selvom projektet måske synes at virke mere omfattende, må det antages, at det i det lange løb giver en mere succesfuld implementering af databeskyttelse gennem design. Det helt essentielle i lederudvikling under agilitet er, at opfattelse af ændringen, implementering af ændring og testændring skal ske i et klart og tydeligt samarbejde med medarbejderne og dermed give alle en fornemmelse af vigtigheden og en fælles følelse af succes.

4.1.5 Communication

Kommunikation kan være noget af det sværeste i en organisation med mange forskellige afdelinger og mange forskellige kompetencer. Det kan yderligere være svært at håndtere kommunikation rent sprogligt. Det har den dataansvarlige i virksomhed Y en daglig udforing med:

> *"Det har også meget med de medarbejdere at gøre, som jeg får fat i. Både om de har ressourcen til det, men også hvordan de er som individer, altså om de er til at snakke med, og om de overhovedet kan engelsk.*" (Bilag 3, spm. 19).

Man bliver som organisation derfor nødt til at forhold sig til denne drivkraft og vurdere, hvordan man bedst muligt kommunikerer i ens organisation. Det må konstateres, at kommunikation er en meget vigtig drivkraft for at skabe en succesfuld implementering af databeskyttelse gennem design.

> *"Min teori er, at hvis det bare kommer ovenfra og ned, så er der mindre sandsynlighed for, at medarbejderne følger det, end hvis de selv er med i beslutningsprocessen, med i udviklingen, altså policy-arbejdet, med i afregningen af hvor man kan få mest value for den ændring, man nu ligger for dagen."* (Bilag 2, spm. 6).

Ovenstående er en udtalelse fra den dataansvarlige fra virksomhed X, og opfattelsen her må dermed vurderes til at være en vigtig drivkraft i implementeringen af forordningen i organisationen, at ledere kommunikerer ændringer i øjenhøjde med medarbejderne og ikke fra et hierarkisk udgangspunkt. I forhold til kommunikation ved organisatorisk agilitet så er det vigtigt at vurdere hvorvidt, man som ledelse vælger at kommunikere. Der findes, som nævnt tidligere tre primære retninger i forhold til, hvilken kommunikationskanal man vælger, om det er top-down, horizontal eller bottom-up kommunikation. I forhold til denne afhandling er det derfor vigtigt, at man som ledelse vurderer, hvordan man griber dette an på bedste vis for at opnå den fleksibilitet, der er nødvendig til forandring. Dette kan være altafgørende for implementeringen. I praksis er det også noget, der er blevet en del af håndteringen i at få medarbejderne med på projektet.

> *"Folk har så mange forskellige kompetencer, så det er vigtigt, at man ikke taler ned til dem. Der er så sindssygt meget psykologi i det. Jeg har gjort sindssygt meget ud af det, når jeg har talt med folk og anlægge en positiv vinkel i det." (Bilag 2, spm. 24).*

Ved at skabe en god kommunikation mellem organisationen og den enkelte medarbejder er den dataansvarlig i virksomhed X af den opfattelse, at man opnår et meget bedre resultat.

> *"Det kan hjælpe dig med at få mindre travlt, det har været noget, der har hjulpet meget. Man bliver nødt til at anerkende, at det kan være svært for en medarbejder at komme ud af sin skal og sin daglige rutine. Så jeg tror på, at det gør meget, at man anerkender det hos medarbejder og gør opmærksom på, at man godt ved, at det er en svær ting. Så det at man indikerer, at man har stor respekt for det, de laver og at man vil prøve at lave de bedste løsninger for alle. Dermed er der også en større tilbøjelighed til, at de hjælper." (Bilag 2, spm. 24).*

Ud fra ovenstående må det konstateres, at det bedste resultat af databeskyttelse gennem design skabes gennem horisontal kommunikation. Gennem denne kommunikationsmetode erkender ledelsen medarbejdernes daglige arbejde og kompetencer, men formår at videregive vigtigheden af implementeringen af databeskyttelse gennem design. Den åbne kommunikation i organisationen skaber et godt miljø for godt teamarbejde. En ulempe ved teamarbejde består i, at det kan øge mængden af tid, der kræves for at træffe en beslutning. Dog vil kvaliteten af beslutningerne gennem teamarbejde blive af højere afgørende effekt. Dette er i sidste ende en forudsætning for at nå i mål med organisationens vision omkring databeskyttelse.

4.1.6 Development of a learning Organization

En drivkraft som hjælper med at skabe agiliteten i organisationer, omfatter organisationens evne til at skabe en god vidensdeling i forhold til implementeringen af forordningen. Indgangsvinklen i denne drivkraft har bestået af at anlægge en positiv vinkel til medarbejderne ved at involvere dem og lade dem få medbestemmelse. Ud fra denne forudsætning er der en større mulighed for:

> *"… at optimere og få smidt de ting ud vi ikke bruger mere og effektiviseret de arbejdsprocesser vi har."* (Bilag 2, spm. 24).

En læringsorganisation søger løbende at forbedre og omdanne, samtidig med at de samlede organisatoriske processer forbedres. Alle organisationer er i samme situation i forhold til implementeringen af forordningen, og de kan gennem vidensdeling opnå en agil tankegang, da man dermed kan have en hurtig tilpasningsmulighed baseret på den eksterne viden, man får fra andre organisationer (Krarup, 2016). Udvikling af en læringsorganisation fremføres af agilitet, fordi den giver de nødvendige værktøjer og kulturelle implikationer til at gøre det muligt for organisationen at eksistere på en harmonisk måde. Derfor er denne drivkraft en ikke ubetydelig del af, hvad der kræves af en organisation for at være agil og dermed implementere forordningen i alle dets processer. Organisationer søger måder at imødekomme deres stigende behov for databeskyttelse og dette løses ved at dele vigtig viden, som sikrer implementeringen af forordningen på en måde, som understøtter agiliteten. Ved at dele viden skaber organisationerne et langt bedre grundlag, hvis de befinder sig i en konstant optimerende form, hvor den iterative læringsproces skaber udvikling (Nijssen, M. et. Al., 2012).

4.1.7 Scalable workforce

Når menneskelige ressourcer vurderes som vigtige aktiver i en organisations aktivstruktur, skal kompetencer til at konfigurere og omdanne arbejdsstyrken holdes for øje. Arbejdsstyrkens skalerbarhed anses som et krav til organisationer, der opererer i et dynamisk miljø (Dyer og Ericksen, 2006). Dette understøttes af, at en agil organisation kræver løbende omfordeling af ressourcer, herunder de menneskelige ressourcer. Begrebet "arbejdsstyrkens skalerbarhed" bruges til at fange en organisations kapacitet til at holde sine menneskelige ressourcer i overensstemmelse med forretningsbehov ved at overføre hurtigt og nemt fra en menneskelig ressource til en anden. En agil organisation forbedres af arbejdskraftens fleksibilitet, fordi det sandsynligvis vil opfylde de nødvendige og tilstrækkelige betingelser, der kræves for at implementere forordningen succesfuldt. Når der skal implementeres en forordning om databeskyttelse i en given organisation, er det nødvendigt at arbejdsstyrken og generelt de menneskelige ressourcer formår at tilpasse sig (Nijssen, M. et. Al., 2012). Denne fleksibilitet i arbejdsstyrken er betinget af, at der er en forståelse for grundlaget for implementeringen. Manglende forståelse for grundlaget og derfor årsagen til ændring af forretningsgangen, giver ikke organisationen en skalerbar arbejdsstyrke (bilag 1, spm. 3). Ved at fokusere på arbejdsstyrkens skalerbarhed, kan organisationen bruge arbejdsstyrken til at styre udformningen af en strategi, som forbedrer agiliteten og implementeringen som helhed.

I interviewet med virksomhed X blev det klarlagt, at det at inddrage medarbejderen og skabe en plan for implementeringen i fællesskab, skaber et langt bedre forhold til medarbejderen og giver dem ejerskab. Ejerskabet udsprang af, at medarbejderen deltog i workshops og selve udformningen af Gap-analyserne (bilag 2, spm. 9). Dette ejerskab er ikke bare en hjælp for medarbejderen til at forstå baggrunden for forordningen men en kæmpe værdifaktor, når det kommer til organisationens behov for en skalerbar arbejdsstyrke. Gennem medbestemmelsen, workshops og ejerskabet skabes en agil og skalerbar arbejdsstyrke.

4.1.8 Highly adaptable organizational infrastructure

Det er betydningsfuldt, at infrastrukturen i organisationen skaber et miljø, hvor medarbejderne ikke føler, de får trukket en masse juridisk ned over hovedet fra den juridiske afdeling, men selv formår at forstå vigtigheden gennem deres nærmeste leder og på den baggrund skabe en god infrastruktur i deres afdeling.

> *"Medarbejderne skal have ejerskab i processen og den eneste måde, at man kan få folk til at få ejerskab, det er, hvis de forstår vigtighed og hensynene og at de også forstår, at det også er en interesse for virksomheden som sådan og at det faktisk bliver prioriteret af deres managers"* (bilag 2, spm. 6).

Behovet for tilpasning af infrastruktur kan opstå fra flere forskellige aspekter om skiftende behov. Især ved implementering af databeskyttelse gennem design vil der blive behov for en infrastruktur, som kan tilpasse sig nye retningslinjer og nye politikker. Tilpasningsevnens bidrag til effektive forandringer ved enten forventede behov eller til nye behov er essentiel for en agil organisation. En organisation skal forme og skabe ændringer i fællesskab, for at organisationens infrastruktur når en høj tilpasningsevne.

Gennem interviewet med virksomhed Y viste det sig, at de ikke havde fundet den endelige struktur ved implementeringen af forordningen. Det blev i denne sammenhæng klart, at strukturen for implementeringen for det første afhang af resultaterne fra deres Gap-analyser og at det for det andet var nødvendigt at føre kontrol for at sikre, at strukturen er tilpasset og opfylder ønsket om databeskyttelse gennem design (bilag 3, spm. 21).

4.2 Framework af organisatorisk agilitet fra et menneskeligt motiveringsperspektiv

Hurtige teknologiske forandringer, øget risiko, globalisering samt forventninger om tilpasning hertil er karakteristika for miljøet, som organisationer står overfor i det nuværende konkurrenceforhold (Narasimhan, R. og Das, A., 1999). For at en organisation skal lykkes i et sådant miljø, er agilitet især en vigtig byggesten i organisationens fundament, da det skaber en konkurrencefordel, som opretholder innovation og kvalitet. En agil organisation forener organisationsprocesserne med medarbejderne (Kidd, P., 1994). Ledelsens rolle i en agil organisationskultur er essentiel, da det er den ledelsesmæssige base, som bygger og vedligeholder. Derudover kommer vigtigheden af medarbejdere med den rette motivation og kompensation ved gennemførelse af ændringer. Medarbejderne i sig selv om deres engagement i en agil organisationskultur af kvalitet og stærke beslutninger er en væsentlig del af den samlede kvalitetsstyring (Spencer, B., 1994).

Udtrykket organisatoriske medlemmer eller organisatoriske medarbejdere anses som værende en væsentlig komponent i organisatorisk agilitet. Tankegangen om at den menneskelige del og indsats gennem et teamwork erstatter den traditionelle afgrænsning mellem ledere og arbejdere blandt funktionelle områder af specialisering. Skiftet til disse relationer og væk fra den traditionelle arbejdsgiver-medarbejderordning er beskrevet af Arthur og Rousseau, 1996. De bemærker, at karrierer nu er præget af bevægelse på tværs af organisatoriske grænser til flere arbejdsgivere, betydningen af netværk og omdømme baseret på seneste projektresultater. Det skaber også et ansvar for organisationen at fortsætte med at levere et vitalt og frugtbart miljø for at bevare agilitet samt bevare værdifulde personers talenter. Organisationer ville være bedre i stand til at deltage i vores skiftende forretningsmiljø, hvis de vedtager det grænseløse perspektiv. På den måde skaber man

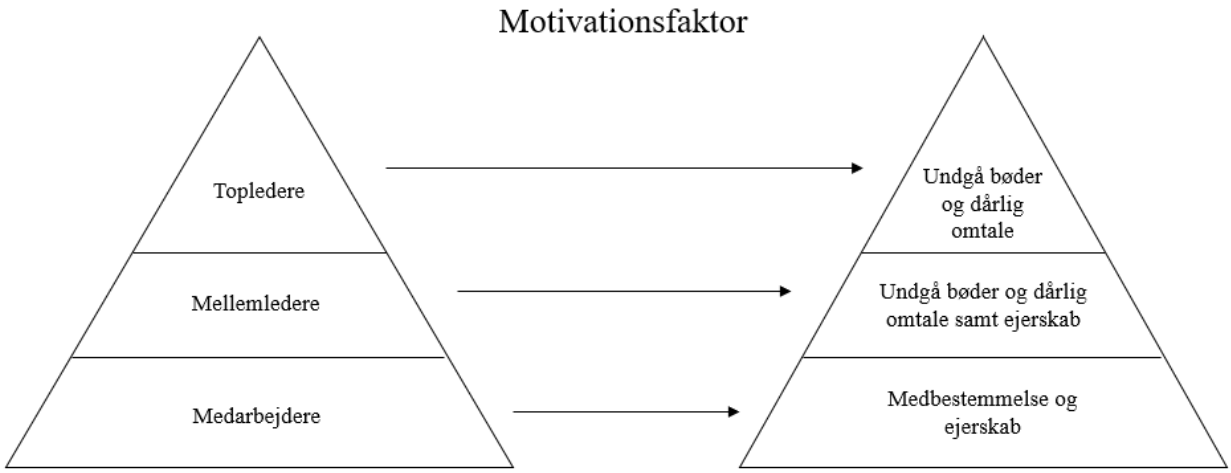
også som organisation det bedste fundament for agilitet ved at lade det menneskelige perspektiv sætte sit præg på organisationen (Crocitto, M., 2003).

Ledere på alle niveauer, ikke kun øverste ledere, skal implementere agilitet som en organisatorisk værdi. Således skal en kultur af forandring være gennemgribende på alle niveauer. Verden er kompleks, det bedste modsvar på kompleksiteten er at skabe de bedste forhold i organisationens struktur til at håndtere konstant skiftende miljø (Lawrence og Lorsch, 1967).

En af årsagerne til at området om organisatorisk agilitet ikke har fået den anerkendelse, som det burde, kan være på grund af nye organisatoriske former og relationer trodser de traditionelle organisatoriske tilgange. Agiliteten fra det menneskelige perspektiv i organisationerne modarbejder den traditionelle ledelse og hierarkiske pyramide. Den mest værdifulde løsning for en organisation ville bygge på at indregne den menneskelige faktor som en kombination af indikatorer til organisatoriske medlemmer gennem belønninger, magt og kompensation, at de understøttes som en vigtig del af en organisation i læring og tilpasning til agilitet (Crocitto, M., 2003).

Når organisationer opnår smidighed i form af agilitet, er det afgørende for enhver organisations succes. Men implementering og opretholdelse af agilitet i en organisation skal understøttes af den menneskelige faktor. Hvis ikke det menneskelige perspektiv kan forenes med agiliteten, er tilstedeværelsen af samme tvivlsom. I langt de fleste organisationer er det også her, at den største udfordring består, især når det kommer til kultur, kommunikation og lederskab (Crocitto, M., 2003). Denne betragtning understøttes ligeledes i ekspertinterviewet og i interviewet med de dataansvarlige i virksomhed X og virksomhed Y. I begge disse tilfælde blev det klarlagt, at det er den menneskelige faktor, som er en udfordring og som derfor kræver en omfattende håndtering. Selvom man som ledelse har en strategi for implementeringen af agilitet, vil dette aldrig slå igennem som et grundlag for organisationens agilitet alene. Det menneskelige perspektiv er således ikke kun en del af agiliteten, men på samme tid også grundlaget for eksistens og eksekvering af samme. Under udarbejdelse af nærværende afhandling, blev det klart, at mennesker og deres kultur, kommunikation og lederegenskaber er organisationernes største udfordringer ved implementering af databeskyttelse gennem design. Det blev især klart, at disse udfordringer er endnu mere omfattende for organisationernes implementering af databeskyttelse gennem design, når de fortsat opstiller krav om at være agile.

Ud fra ovenstående er det meget varierende, hvilket niveau organisationerne befinder sig på i forhold til kravet om awareness i forordningen omkring databeskyttelse gennem design og hvilken motivationsfaktor de har. Dette kan opstilles som nedenstående model:

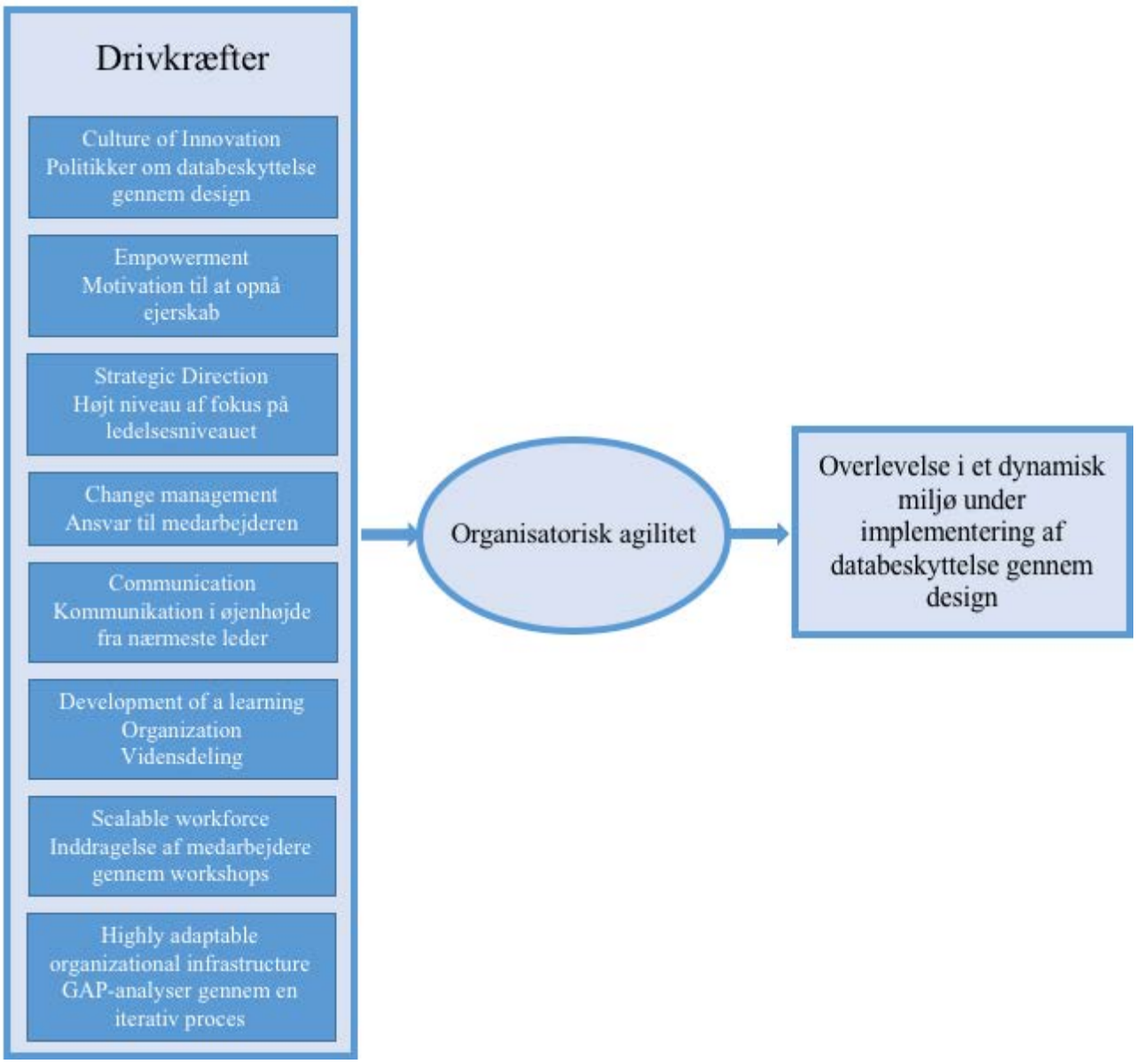


Figur 3. Kilde: Egen tilvirkning

Ovenstående figur bidrager til præciseringen af organisationernes motivationsniveauet, og skal bruges til at finde de korrekte værktøjer til implementeringen af forordningen. Det er i denne sammenhæng vigtigt at udarbejde et framework indenfor organisatorisk agilitet til at præcisere, hvor man som organisation skal have størst fokus for at opnå en succesfuld implementering af databeskyttelse gennem design. Frameworket med dets dertilhørende værktøjer vil blive analyseret og sammenholdt med resultatet fra de udarbejdede interviews senere i dette afsnit.

Sammenspillet mellem organisations opbygning, som ovenstående model viser, har en stor betydning for at skabe en god forståelse og implementering gennem de organisatoriske agilitetsdrivkræfter. Motivationen hos både topledere og mellemledere består hovedsageligt i, at man gerne vil undgå en dårlig omtale, hvis organisationen ikke overholder reglerne om at beskytte persondata, samt undgå de enormt store bøder på henholdsvis 4 % og 2 % af organisationens omsætning, jf. forordningens artikel 83, stk. 4 og 5. I forhold til medarbejderne er det nogle andre motivationsfaktorer, der spiller ind. Hos dem handler det om ejerskab og medbestemmelse. Det er altså altafgørende for en succesfuld implementering af databeskyttelse gennem design, at man inkluderer medarbejderne i projektet, i stedet for at overtrumfe dem med juridiske krav (bilag 2, spm. 6).

Baseret på analysen og valget af de 8 drivkræfter, ønsker denne afhandling at skabe en visualisering af et framework (figur 4). Frameworket skal på baggrund af de relevante motivationsfaktorer give en række værktøjer til en organisation, når denne skal implementere forordningen og går i dybden med databeskyttelse gennem design. De ovenstående udvalgte drivkræfter (afsnit 4.1) bidrager dermed med nogle håndgribelige værktøjer. Understående ses frameworket (figur 4) med de udvalgte drivkræfter og dertilhørende værktøjer:



Figur 4. Kilde: Egen tilvirkning (Denne figur er udviklet med inspiration fra Nijssen, M. et al., "HRM in turbulent times: How to achieve organizational agility", The international journal of human resource management, 2012, se bilag 4).

Under hver af de 8 drivkræfter er udvalgt det mest repræsentative værktøj for organisationen at implementere databeskyttelse gennem design uden at gå på kompromis med agiliteten. Relevansen af de 8 drivkræfter kan variere organisationerne imellem, men overordnet set er alle disse værktøjer relevante for organisatorisk agilitet som helhed. De 8 udvalgte drivkræfter og dertilhørende værktøjer er med til at skabe et dynamisk miljø, der kontinuerligt skal sørge for at databeskyttelse gennem design gennemgår en iterativ proces i organisationerne. Alle 8 drivkræfter er understøttet gennem de tre fremførte interviews (bilag 1 - 3). Ovenstående framework er denne afhandlings anbefaling til organisatorisk agilitet ved implementeringen af databeskyttelse gennem design.

4.3 Delkonklusion

En organisation har mange tangenter at spille på og det er vigtigt at alle tangenter er i takt, førend organisationen som helhed kan opnå konkurrencefordele og et succesfuldt virke. En af de vigtigste tangenter i denne sammenhæng er at kunne bestride agilitet, da dette forener organisationsprocesserne med medarbejderne.

Det kan konkluderes, at for at opnå organisatorisk agilitet er det vigtigt at tage udgangspunkt i de 12 drivkræfter inden for agilitet fra teoriafsnittet (afsnit 2.2.3). Disse 12 drivkræfter er blevet indskrænket i analysen til 8 drivkræfter, og disse 8 drivkræfters individuelle håndgribelige værktøjer er blevet beskrevet. Organisationerne skal på individuelt plan anvende værktøjerne fra drivkræfterne for at understøtte deres motivation, for at skabe en succesfuld implementering. De 8 drivkræfter skal tilsammen skabe en fleksibilitet i organisationen, når der implementeres nye projekter, som i dette tilfælde er beskyttelse af persondata gennem design. De vigtigste drivkræfter er forholdet mellem ledelsen og medarbejderne samt kulturforandring. Det er vigtigt, man som organisation sammensætter teams og skaber ejerskab i disse teams, da dette skaber en medbestemmelsesfølelse hos medarbejderne, og dermed skaber succes i organisationens vision. Slutteligt kan det konkluderes, at udviklingen af organisationen og dennes medarbejderes læring hele tiden er i bevægelse gennem en iterativ proces og derfor kræver kontinuerlig kontrol.

Tankegangen bag den økonomiske del af en organisation bygger på at være på forkant med nye markeder og undgå tab. Netop disse to elementer kan med fordel bruges, når forordningen skal implementeres. Dette underbygger netop den tilgang som klarlægger hvilke krav databeskyttelse gennem design stiller til organisatorisk agilitet – at være på forkant med databeskyttelse og undgå tab af sikkerhed.

Del V – Diskussion

Det er en vigtig faktor, at databeskyttelse gennem design og agilitet går hånd i hånd, da databeskyttelse gennem design må anses for kontinuerligt at være i bevægelse. Det er dog utvivlsomt, at kombinationen af databeskyttelse gennem design og organisatorisk agilitet medfører en langt større arbejdsbyrde på ledelses- såvel som på medarbejderniveau. Derudover kommer tidsfaktoren i spil, da implementeringen og vedligeholdelse af organisatorisk agilitet kræver mange ressourcer. Den økonomiske ressource er ydermere en ikke ubetydelig faktor, som for flere organisationer kan have store konsekvenser. Dog må retssikkerheden gennem databeskyttelse, samt bødeniveauet i øvrigt, antages at være en mere betydningsfuld faktor end omkostningerne til at indføre databeskyttelse gennem design i organisationerne.

Denne afhandling ønsker at danne et overordnet framework (figur 5), som kan bruges af organisationerne i praksis. Tilblivelsen af dette framework (figur 5) er først sammensat af de juridiske foranstaltninger og dernæst forenet med drivkræfterne bag en agil implementering af databeskyttelse gennem design. Brugen og anvendelsen af det endelige framework (figur 5) vil blive diskuteret i afsnit 5.1 – 5.3.

5.1 De juridiske foranstaltninger

Implementeringen af de rette sikkerhedsforanstaltninger i organisationen kan skabe en positiv indvirkning, hvor organisationerne får ryddet op i både deres data samt deres processer og i sidst ende

opnå en optimering. Ydermere skal den kontinuerlige cyklus skabe en fordel for konstant at være på forkant og undgå sanktioner. Den negative vinkel i databeskyttelse gennem design er det store økonomiske aspekt i og med, at både IT-udstyr og organisatoriske ressourcer kan være omkostningsfulde. Dog må den positive effekt for undgåelse af de betydningsfulde sanktioner opveje for det økonomiske aspekt i implementeringen. Helt overordnet må den største positive effekt være beskyttelsen af persondata.

Det juridiske perspektiv på udvikling af databeskyttelse gennem design udspringer fra kommissionens strategi om at skabe datasikkerhed på det indre marked. Dette er gjort med henblik på at skabe et større og lettere flow over landegrænserne. I den sammenhæng har denne afhandling belyst hvilke juridiske foranstaltninger og drivkræfter, dette kræver. En særlig vigtig årsag til kommissionens udvikling af forordningen udspringer fra organisationernes tilgang til implementeringen. De organisatoriske elementer spiller en større rolle end først antaget, da organisationerne ikke kan implementere forordningen uden at have agilitet og forandringsledelse på plads.

Denne afhandling belyser de foranstaltninger, der måtte anses for at være betydningsfulde af forordningens artikel 25, stk. 1. Foranstaltningerne udspringer fra betragtningen af de 7 principper om databeskyttelse gennem design (afsnit 3.1.1) og de 7 tekniske PET-principper (afsnit 3.1.2.1). Disse understøttes af den norske regerings tilgang omkring deres design krav, hvilket består af de dataorienterede og de procesorienterede krav (afsnit 3.2). Ydermere har det danske datatilsyn igennem årene udsendt retningslinjer til forskellige offentlige instanser i henhold til krypteringskrav og adgang til data. Ovenstående må anses som værende minimumskrav til databeskyttelse gennem design og er dermed en understøttelse til det juridiske framework (figur 2). Det juridiske framework (figur 2) skal ved hver organisation ved opstart være baseret på en konsekvensanalyse, som er forskellig fra organisation til organisation. I forhold til det overordnede framework (figur 5) er den juridiske figur fra afsnit 3.4 en klar indikation af, at der i denne afhandling er valgt at tage udgangspunkt i 8 overordnede foranstaltninger, som er valgt ud fra den juridiske analyse.

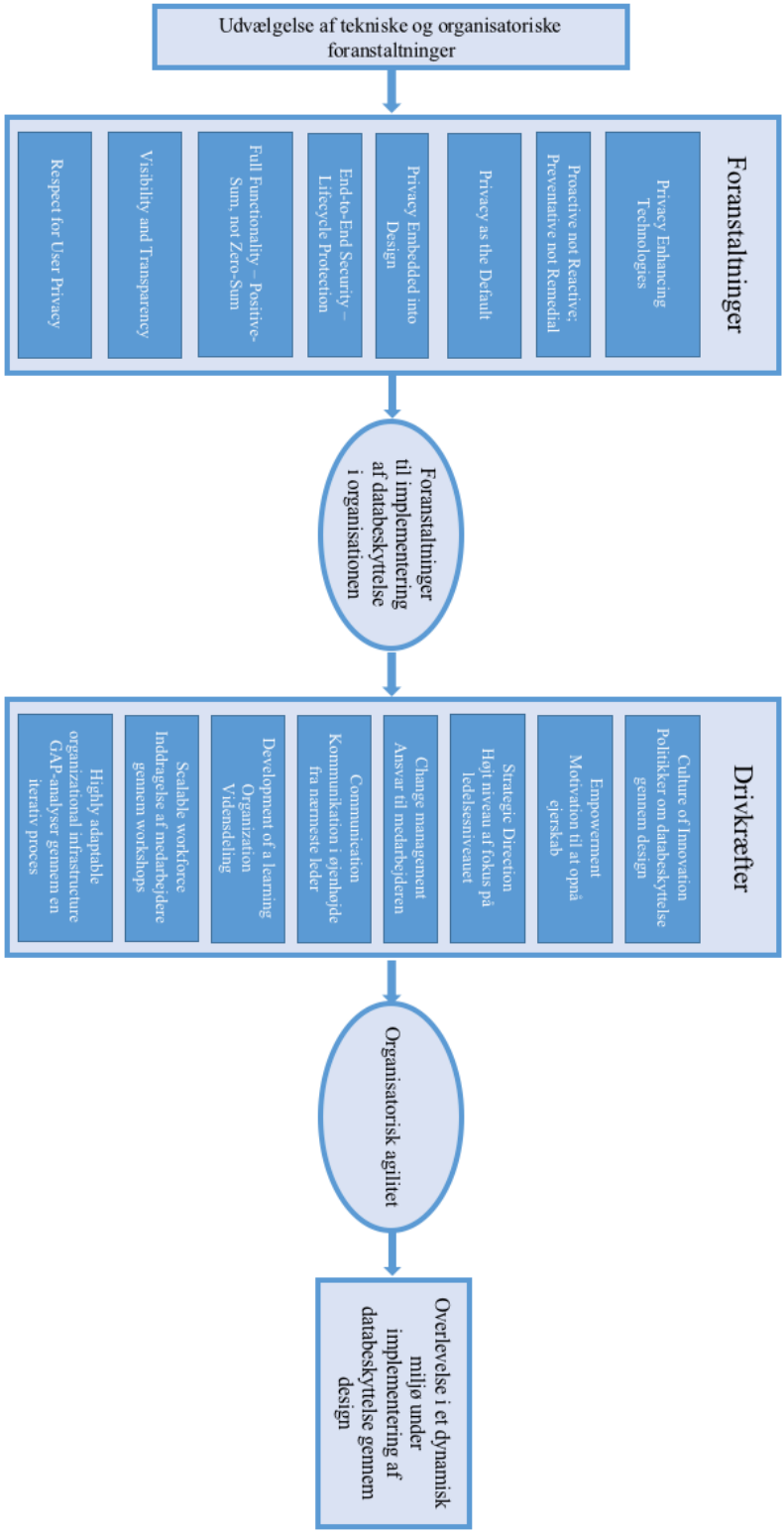
5.2 De 8 drivkræfter

I udvælgelsen af de 8 drivkræfter blev der udviklet et visuelt framework (figur 4), som er den med i den videre udvikling til det endelige framework (figur 5). Nærværende afhandling er ud fra den kvalitative undersøgelse kommet frem til, at det fremtidige perspektiv i implementering af databeskyttelse gennem design har et behov for organisatorisk agilitet, for at opnå en kontinuerlig succes og i sidste ende kunne skabe den manglende værdi ledelsen ikke mener, er til stede i implementeringen og overholdelsen af forordningen. Der må i fremtiden antages at ske en udvikling i teknologien generelt og i organisationerne, hvilket må antages at give optimerende processer. For at organisationen skal kunne følge med i den fremtidige teknologiske udvikling, skal overholdelsen af frameworket om organisatorisk agilitet (figur 4) sørge for, at organisationerne bibeholder en konkurrencemæssig fordel og hele tiden udvikler organisationen under et fortsat compliance-niveau.

Det er forskelligt fra organisation til organisation, hvilke drivkræfter det er relevant at lægge størst vægt på. Derfor er det væsentligt først at udarbejde en analyse over, hvilke af de foranstaltninger i det juridiske framework (figur 2), der er mest betydningsfulde for organisationen. Herefter udvælges de relevante drivkræfter til implementering gennem organisatorisk agilitet, som understøtter visionen i organisationen.

5.3 Det endelige framework

De relevante juridiske foranstaltninger og drivkræfter under organisatorisk agilitet til implementering af databeskyttelse gennem design er belyst i følgende framework (figur 5).



Figur 5. Kilde: Egen tilvirkning.

Ovenstående framework (figur 5) og afhandlingen som helhed er udarbejdet med et ønske om at skabe en praktisk håndbog for organisationerne ved implementeringen af databeskyttelse gennem design. Det fremtidige perspektiv vil uden tvivl medføre databeskyttelse samt kontrol heraf i stigende grad. Dette underbygger vigtigheden og væsentligheden af problemstillingen og i særdeleshed anvendelsen af ovenstående framework.

Formålet med afhandlingen har været først at skabe et overblik over de juridiske foranstaltninger og derefter at belyse en implementeringsmetode via organisatorisk agilitet, som i sidste ende skaber en samlet overlevelse i et dynamisk miljø. Ovenstående framework (figur 5) skal ses som en proces for organisationen i håndteringen af databeskyttelse gennem design. Frameworket skal følges fra udvælgelsen af foranstaltningerne til implementeringen via drivkræfterne ud fra inspirationen af den norske implementeringsvejledning (figur 1), hvor processen kontinuerligt skal køre i ring.

Det endelige framework (figur 5) må antages i fremtiden at kunne præciseres yderligere, når de første afgørelser bliver truffet og kommissionen dermed skaber mere klare retningslinjer på indholdet af databeskyttelse gennem design. Dog antages det ud fra brugen af resultaterne i den juridiske analyse, i forhold til de krævede sikkerhedsforanstaltninger i forordningens artikel 25, stk. 1, at de skal sikre, at organisationerne overholder forordningen.

Udgangspunktet for organisationerne har været, at forordningen ikke skaber værdi for deres organisation men blot opfattes som en forsikring. Denne afhandling ønsker overordnet set at ændre dette syn og få organisationerne til at arbejde henimod agilitet og i sidste ende skabe en bedre fleksibilitet og flow i alle processerne samtidig med, at beskyttelsen af persondata bevares. Brugen af frameworket (figur 5) opfylder dermed de opstillede motivationsfaktorer (figur 3), hvor topledere og mellemledere undgår bøder og dårlig omtale samtidig med, at medarbejderen opnår større medbestemmelse og ejerskab i organisationerne.

Del VI - Konklusion

Denne afhandling har analyseret hvilke krav, databeskyttelse gennem design stiller til organisatorisk agilitet. I analysen er det centralt at undersøge, hvad databeskyttelse gennem design i forordningens artikel 25, stk. 1 betyder. Ydermere er det elementært for analysen at undersøge, i hvilken grad organisatorisk agilitet kan anvendes ved implementeringen af databeskyttelse gennem design. Formålet med afhandlingen er at give organisationerne en vejledning gennem en håndbog, som iscenesætter de mest væsentlige drivkræfter til at skabe det bedst mulige resultat i hele organisationen ved implementering af databeskyttelse gennem design.

Udformningen af det endelige framework og besvarelsen af problemstillingen er blevet inddelt i 3 faser. Første fase er besvarelsen af det underspørgsmål, hvor der bliver præciseret, hvad der forstås ved databeskyttelse gennem design. Anden fase er besvarelsen af det andet underspørgsmål, hvor der bliver præciseret i hvilken grad, organisatorisk agilitet kan anvendes i implementeringen af databeskyttelse gennem design. Endelig er den tredje og sidste fase en besvarelse af den centrale problemstilling, hvor frameworket (figur 5) visualiserer, hvilke krav databeskyttelse gennem design stiller til organisatorisk agilitet.

Del II i denne afhandling søger at skabe klarhed over det teoretiske fundament for både databeskyttelse og organisatorisk agilitet herunder at udlede hvilke forudsætninger, der er relevante for at besvare problemformuleringen. Databeskyttelse gennem design må konkluderes at være en in-

dividuel håndtering fra organisation til organisation, da forskelligheden i persondata i organisationerne varierer. Denne afhandling har derfor givet en udførlig analyse af, hvad der må anses for at være gældende ret under forordningens artikel 25, stk. 1. Først og fremmest kan det konkluderes, at databeskyttelse gennem design kontinuerligt vender tilbage til udtrykkets oprindelse af Dr. Ann Cavoukian, som er skaberen af konceptet om de 7 principper, som er fundamentet for databeskyttelse gennem design. Det er i denne afhandling derfor en klar anbefaling, at disse 7 principper skal gennemgåes af organisationerne i deres konsekvensanalyse af hvilke data, de har og hvordan flowet af disse skal designes ind i organisationernes processer for at opnå en succesfuld overholdelse af forordningen. De 7 principper giver dermed den stærkeste beskyttelse af privatlivets fred, der er tilgængelig i vores samfund.

Dog må det konkluderes, at de 7 principper ikke kan stå alene ved implementeringen af databeskyttelse gennem design, da retskravet yderligere henvender sig til implementeringen af tekniske foranstaltninger. Her danner PET-håndbogen grundlag for attraktive og relevante måder at overholde forordningens artikel 25, stk. 1. De teknologiske redskaber, som PET-håndbogen er bygget op omkring, udformer informations- og kommunikationssystemer, hvor behandlingen af personoplysninger kan indskrænkes for at overholde reglerne om databeskyttelse.

De 7 princippers relevans bliver også underbygget i norsk ret, hvor de udvikles fra at være teoretiske principper til praktisk håndtering af databeskyttelse gennem design. Her konkluderes det, at valget af metode til håndtering er forbundet med den service, organisationen udbyder, industrien, typer af software, der bliver udviklet og overvejelserne i forhold til organisationens egen villighed for niveauet af risiko. Den norske tilgang til databeskyttelse gennem design udspringer dermed af organisationernes kontinuerlige værn om datasikkerheden, da det aldrig bliver en afsluttet proces, idet den teknologiske udvikling aldrig afslutte men kun i stigende grad bliver en del af vores liv og hverdag.

Denne afhandling konkluderer, at den nuværende retspraksis, som findes på området for den danske persondatalov, er et minimumskrav til databeskyttelse gennem design. Selvom den nye forordning skaber en ny retspraksis, er det i denne afhandling sammenfattet, at de tekniske foranstaltninger, der anses for at skulle være tilstede i organisationerne, som minimum skal bestå af kryptering. Det kan dog konkluderes, at den fremtidige retspraksis bliver en skærpelse med udgangspunkt i resultaterne på de nuværende afgørelser.

Nærværende afhandling præciserer, at databeskyttelse gennem design med al sandsynlighed er betinget af at opretholde fleksibiliteten for at få en succesfuld implementering. Dette skabes gennem teorien bag organisatorisk agilitet. Baseret på denne teori kan det konkluderes, at implementeringen af databeskyttelse gennem design skal foregå ud fra de 8 udvalgte drivkræfter i analysen. De 8 faktorer danner grundlag for udformningen af denne afhandlings framework. Dette framework bør benyttes som retningslinje for enhver organisation og skal dermed bruges som værktøj til at overholde databeskyttelse gennem design. Det kan konkluderes, at implementeringen af databeskyttelse gennem design skal gå igennem alle organisationens niveauer, hvorved denne afhandlings framework er det mest optimale værktøj hertil. Vores anbefalingen til nuværende og fremtidig databeskyttelse i organisationerne er, at den enkelte organisation som helhed skal tage udgangspunkt i frameworket for at opfylde kravene, som databeskyttelse gennem design stiller til organisatorisk agilitet. Det er i høj grad nødvendigt for organisationerne at vedligeholde agilitet som en del af en iterativproces for at kunne stille den fornødne sikkerhed til den teknologiske udvikling.

Kommissionens strategi omkring et digitalt indre marked kan dermed konkluderes at opnåes i organisationerne gennem nærværende afhandlings framework. Dermed udvikles organisationer, som

gennem agilitet kontinuerligt kan tilrette deres håndtering af databeskyttelse. Kommissionens ønske om at opretholde individernes tillid, samtidig med at organisationerne gnidningsløst kan få adgang til at udføre deres services under en stigende teknologisk udvikling og fri bevægelighed, lykkedes hermed og den ønskede harmonisering synes at kunne opfyldes.

Dermed kan det afslutningsvist konkluderes, at det endelige framework i denne afhandlings diskussion først og fremmest er en vurdering af, hvilke tekniske og organisatoriske tiltag en organisation skal implementere ud fra de 7 principper og PET baseret på konsekvensanalysen. Dernæst sker implementeringen af disse gennem de 8 udvalgte agilitets drivkræfter, som dermed skaber overlevelse i et dynamisk miljø for organisationerne.

Reference

- Aldrich, H., "Organizations Evolving", Thousand Oaks, CA, 1999.
- Antignac, T. and Le Métayer, D., "Databeskyttelse gennem design: From technologies to architectures", Second Annual Privacy Forum, 2014.
- Article 29, Data protection Working Party, Working Party on Police and Justice, WP 168, "The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", 2009.
- Arthur, M. B. og Rousseau, D. M., "The Boundaryless Career: A New Employment Principle for a New Organizational Era", Oxford University Press, 1996.
- Beer, M. og Nohria, N., "Cracking the Code of Change", Boston, MA: Harward Business Review, (2000).
- Blarkom, G.W. van et al., "Handbook of Privacy and Privacy-Enhancing Technologies - The case of Intelligent Software Agents", College bescherming persoonsgegevens, 2003: http://andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf – tilgået d. 25. februar 2018.
- Blume, P, "Persondata retlige grundfigurer – strejftog i den nye persondataret", Djøf Forlag, 2017.
- Cavoukian, A., "Privacy by design – Strong Privacy Protection – Now, and Well into the Future", 2011.
- Cavoukian, A., "Privacy by design - The 7 Foundational Principles Implementation and Mapping of Fair Information Practices", Information & Privacy Commissioner, Ontario, Canada., 2010: https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf – tilgået d. 15. februar 2018.
- Center for Cybersikkerhed og Digitaliseringsstyrelsen, "Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift", 2014.
- Council of Europe, "Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14", 1950.
- Crocitto, M. et al., "The humanside of organizational agility", Emeral Insight – Industrial Management & Data Systems, 2003.
- Dall, N. P., et. Al. "Persondataforordningen – en håndbog for praktikkere", Ex Tuto Publishing, 2016.
- Datatilsynets j.nr. 2015-631-0108, "Login til helbredsoplysninger på sundhedsområdet", 2015.
- Datatilsynets j.nr. 2013-112-0268, "Høring over lovforslag om "bølge 3"", 2013.

- Datatilsynets j.nr. 2011-313-0438, ” Manglende sikkerhed ved transmission af fortrolige og følsomme oplysninger via e-mail”, 2011.
- Datatilsynets j.nr. 2007-632-0014, ” Københavns Universitets offentliggørelse af studerendes personnumre”, 2007.
- Det danske sprog- og litteraturselskab (DSL), ”Agil”, Den Danske Ordbog, 2018: http://ordnet.dk/ddo/ordbog?query=agil – tilgået d. 10. april 2018.
- Dom C-362/14, Schrems, 2015: http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A62014CJ0362 – tilgået d. 11. februar 2018.
- Dyer, L. og Ericksen, J., ”Dynamic Organizations: Achieving Marketplace Agility Throug Workforce Scalability”, CAHRS Working Paper, 2006.
- Eriksson, Päivi og Kovalainen, Anne, “Qualitative Methods in Business Research”, SAGE Publications, 2012.
- ENISA, “Privacy and Data Protection by Design – from policy to engineering”, 2014: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design – tilgået d. 27. februar 2018.
- EU Kommissionens meddelelse om bedre databeskyttelse med teknologier til beskyttelse af privatlivet, KOM(2007)228: http://ec.europa.eu/transparency/regdoc/rep/1/2007/DA/1-2007-228-DA-F1-1.Pdf – tilgået d. 13. marts 2018.
- EU Kommissionen, ”EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV 95/46/EF af 24. oktober 1995, om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger”, De Europæiske Fællesskabers Tidende.
- EU Kommissionen, ”EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016, om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF” (generel forordning om databeskyttelse), De Europæiske Fællesskabers Tidende.
- EU Kommissionen, ”Forslag til EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV om visse aspekter af aftaler om levering af digitalt indhold”, 2015.
- Fløe, P.,” Agile Manufacturing – det glemte koncept”, Børsen - Ledelsen, 2014: http://ledelse.borsen.dk/article/view/735/demand_management/artikel/agile_manufacturing.html - tilgået d. 10. april 2018.
- Greenwald, G. og Poitras, L., ”Edward Snowden: 'The US government will say I aided our enemies' – video interview”, The Guardian, 2013: https://www.theguardian.com/world/video/2013/jul/08/edward-snowden-video-interview –tilgået d. 6. februar 2018.
- Harraf, A. et al., ”Organizational Agility”, The Journal of Applied Business Research, 2015.
- Heeager, L. T. et al., “How Agile Methods Inspire Project Management - The Half Double Initiative”, Association for Information Systems, 2016.
- Justitsministeriet, Betænkning nr. 1565, 2017: http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf – tilgået d. 15. marts 2018.
- Justis- og beredskapsdepartementet, ”Lov om behandling av personopplysninger (personopplysningsloven)”, 2001: https://lovdata.no/dokument/NL/lov/2000-04-14-31#KAPITTEL_8 – tilgået 17. maj 2018

- Kidd, P., “A 21st Century Paradigm. In Agile Manufacturing: Forging New Frontiers”, Addison-Wesley, Wokingham, 1994.
- Krarup, H. J., “Forandringsledelse uden forandringslede”, Erhvervs psykologiserien, Dansk Psykologisk Forlag, 2016.
- Lawrence, P. R. og Lorsch, J. W., ” Organization and Environment: Managing Differentiation and Integration”, Harvard University Press, 1967.
- Lando, B. O, “Norge – retssystem, Gyldendal Den Store Danske, 2012: http://denstoredanske.dk/Samfund,_jura_og_politik/Jura/Retssystemer_i_verden/Norge_(Retssystem) – Tilgået den 17. maj 2018.
- Lov nr. 429 af 31/05/2000, ”Lov om behandling af personoplysninger”, (persondataloven), Justitsministeriet.
- Mortensen, H., “Databeskyttelse gennem design - en nyskabelse i databeskyttelsesforordning?”, Brødrene A og O Johansen A/S, 2017.
- Mortensen, H., ”Persondataforordningen – Implementering i danske virksomheder”, DI Digital, 2018: https://digital.di.dk/SiteCollectionDocuments/Vejledninger/Persondataforordningen/Vejledning%20om%20persondataforordningen%20med%20bilag.pdf – tilgået d. 24. maj 2018
- Myers, M. D. og Newman, M., ”The qualitative interview in IS research: Examining the craft”, Elsevier, ScienceDirect, 2006:
- Narasimhan, R. og Das, A., ”An Empirical Investigation of the Impact of Strategic Sourcing on Manufacturing Flexibility and Performance”, Decision Sciences, 1999.
- Nijssen, M. et al., ”HRM in turbulent times: How to achieve organizational agility”, The international journal of human resource management, 2012.
- Privacy and Data Protection by Design – from policy to engineering, ENISA, 2014: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design – tilgået d. 15. februar 2018.
- Spencer, B., “Models of organization and total quality management : a comparison and critical evaluation", Academy of Management Review, 1994.
- Thzaskowski, J. et. Al ”Internetretten” Ex Tuto, 2017.
- United Nations, “Universal Declaration of Human Rights”, 1948.
- Vocabulary.com Dictionary, “Agile”, Vocabulary.com, 2018: http://www.vocabulary.com/dictionary/agile - tilgået d. 10. april 2018.

Bilag 1 - Ekspertinterview med advokat og specialist i databeskyttelse

Interviewer: Frederikke Schlitterlau og Julie Enø Jensen = F/J

Respondent: Advokat og specialist i databeskyttelse = R

1. ***F/J:*** *Vores indgangsvinkel er lige så meget at forstå indholdet af art. 25, så når du er ude at rådgive, hvad er det så egentlig, du fremlægger som værende det, man skal være opmærksom på i forhold til art. 25? Hvad er det, der er indeholdeth i ordlyden "passende sikkerhedsforanstaltninger"? På nuværende tidspunkt?*

   R: Ja, på nuværende tidspunkt er det som rådgiver svært at slippe afsted med at skubbe kravet om privacy by design og privacy by deafult (herefter pbd/d) ind i den compliancedokumentation, som jeg hjælper virksomhederne med at udarbejde, fordi jeg får spørgsmålet hver eneste gang. Jamen vi kan også godt læse, vi kan godt forstå det, men hvad jeg skal sætte de her fire udviklere, ud af de 25 mand vi er, hvad skal de gøre anderledes frem til 25. maj 2018? Så vi ikke bliver sanktioneret? Eller hvad skal de gøre anderledes over de næste 2-3 år? Og der kan jeg jo bare stikke dem de 7, 3, 4 mere eller mindre konkrete retningslinjer fra rådet for digitalsikkerhed, som så er blevet til den artikel, som hedder "Privatlivsindstillinger" af ham Henning Mortensen, og det er udemærket, men det er meget konkret. Sådan noget med at man skal have en drop down i stedet for fritekstfelter, og i det hele taget det her med hvordan man generelt får samtykke. Om det bare er noget, som er upt-in eller upt-out. Det er ikke upt-in, i virkeligheden siger jeg til dem, at det er en skærpelse, at art 25 er egentlig bare en understregning af, synes jeg, en af de andre generelle principper i forordningen. Altså fordi der er også noget pbd i at overholde oplysningspligten osv. Men konkrete softwareudviklingsanvisninger det tør jeg faktisk ikke give dem, for der kan jeg jo meget nemt miste en kunde, fordi hvis jeg siger, det der, det der, det der og det der, det skal ændres inden den 25. maj – nu lægger jeg hånden på kogepladen. Så risikerer deres løsning jo at komme til at være mere besværlig eller se anderledes ud end konkurrentens. Lad os nu bare tage det eksempel fra før med Føtex, hvor Føtex er gået til et webbureau, kald det hvad du vil, og de har fået sådan en webservices protokolstak som er fyldt med koder, og den her stak består af en masse software, som ikke er udviklet efter pbd/d. Skulle jeg så sige til de rådgivere: "Nu skal I gennemgå jeres stak, og så udtage det der ikke duer, indsætte noget andet som ikke er så brugervenligt, så ordentligt eller hvad ved jeg? Så vil de jo risikere at miste deres slutkunde. Og jeg må bare sige, som rådgiver, der skal man hjælpe folk med at tjene penge. Først og fremmest. Det er det. Hvis man er jurist i staten, så skal man hjælpe staten med at overholde reglerne, hvis man er advokat. Og det gælder for mange andre konsulenter, nu snakker jeg bare om mig selv, ikkå? Det kan ikke nytte noget, hvis ikke de kan se, at du kan bruges til hjælp eller tjene penge. Eller undgå at tabe penge, hvilket det her jo meget er. GDPR compliance rådgivning handler for mig at se meget om, at folk skal have en vaccine mod at betale penge, det er jo ikke nødvendigvis, altså jeg ved godt, at det er blevet udskreget som sådan en konkurrencefordel, og vi er "best in class" og sådan nogle ting. Men der tror jeg bare ikke, at vi er endnu i Danmark. Det er vi måske i Tyskland. Det er vi på vej til at blive i England for mig at se. Østeuropa er også rigtigt stærkt med på det her område af historieske årsager.

2. ***F/J:*** *De har jo også haft nogle andre bøder fra starten af.*

R: Lige præcis. Men jeg må bare sige, pbd/d har svære rigtige livsvilkår i det, hvad jeg har kendskab til private IT-liv. Og det har det, for det først fordi, og det er nok faktisk den egentlige årsag, det er så uklart. Det er meget svært at finde ud af, hvad det er. Det er så forblommet, og så tør jeg som rådgiver heller ikke, eller "tør" det er et vrøvleord, men jeg mener heller ikke, at jeg har rygdækning for at sige til en IT-leverandør fx i webservices: "Nu skal du bruge 400 mandetimer fordelt over de næste tre måneder for at indarbejde den, den og den funktion i systemet. Nu har jeg gennemgået U/I, og det og det og det er galt og skal laves om"… Det kommer ikke til at ske. Haha! Det gør det ikke.

3. ***F/J:*** *Hvad så i forhold til den betænkning der er kommet ud her i Danmark, som skriver, at de eksisterende IT-systemer der er det egentlig nok med de organisatoriske sikkerheds-foranstaltninger. At sørge for at have ordentlige procedure og sådan noget. Bruger du så det mere?*

R: Helt sikkert! Ja, ja, ja! Det som jeg jo altid siger mht. det her med sikkerhed, som det fremgår af art. 32. Sådan generelle sikkerhedsforanstaltninger man skal træffe, så vidt jeg lige husker. Ja, for art. 28 databehandler, det glemmer jeg. Jeg bytter altid rundt på de to. Men passende organisatoriske sikkerhedsforanstaltninger, der siger jeg jo altid: "Indtil vi får IT-systemer, altså du har HR-oplysninger hér i dit IT-system, bokset inde på den rigtige måde og vedrørende roller og ansvar. Og du har, hvad skal man sige, B2B oplysning hér, du har forretningshemmeligheder hér, du har en udviklingsafdeling hér, og ligesom de der klassiske sikkerhedsforskrifter har du adskilt mellem tingene. Så hvis det her eksploderer, så eksploderer det andet ikke. Og du kan ikke snable ind fra de forskellige systemer fra forskellige sider. Og der er ikke åben adgang til nettet." Alt det der indtil vi, så at sige, får puttet de rigtige oplysninger ned i de rigtige kasser, så er det håndholdt sikkerhed. Så er det for mig at se passende sikkerhedsforanstaltning, der er håndholdte. Medarbejdere i en HR-afdeling - der er det noget med at lave en opgave, en vejledning, en instruks, en kontrolforanstaltning, I don't give a shit hvad du kalder det, til medarbejderne om alt det kører efter det, jeg plejer at kalde Camilla Vest-princippet. Camilla Vest-princippet er "need to know" og ikke "nice to know". Camilla Vest er den her model som fløj rundt i hele verden, kom til Danmark, så sagde SKAT: "Du skal betale SKAT i Danmark". Så røg den til højesteret, og hun slap for at betale skat i Danmark, men det er ikke det, der er pointen. Pointen var, at undervejs blev to skattemedarbejdere fyret, fordi hun var jo spændende, så de var inde at kigge i hendes sag, og det må de ikke, fordi det var ikke sagligt i forhold til deres konkrete funktion. Og det er jo sådan en af de politikker, som jeg går og stanger ud til alle de virksomheder, jeg kommer ud til: "Og i øvrigt så skal du lige pålægge dine medarbejdere, at det kan få ansættelsesretlig konsekvenser, hvis de ligger og roder i naboens." Og så kan vi altid diskutere, hvis nu Bente, Hanne og Svend bliver syge, så skal Søren kunne tilgå det. Og der skal altid være en administrator af den adgang. Fint nok. Men generelt skal man altså holde sig til det, man arbejder med. Så ind til videre er meget passende sikkerhedsforanstaltninger, det er organisatorisk, og det er det jeg kalder håndholdt. Fordi de der IT-systemer, jo de findes et eller andet sted, men de er slet ikke udbredt, og hvis folk … og det som man slet ikke ser, som jeg ser som det mest indlysende, det er, at man er nødt til i hvert faldt at være åben overfor at skifte sine IT-systemer ud. Men det kan jeg love dig for, det vil man ikke. Jeg kan bare tage vores butik, vores SDH-system leveres

af… Ja det må jeg godt sige, Unique. Og det er håbløst. Det er baseret på DOS-byggeklodser. Det er fuldstændigt åndsvagt. Vi kan ikke engang slette vores gamle sager og sådan nogle ting. Amen jeg tør godt at sige, at alle advokatfirmaer vi bliver compliant på papir. Og det tror jeg altså, at der er mange virksomheder, som der ender med at blive compliant på papir. Og så selve kulturændringerne, systemændringerne og hvad ved jeg, det tager tid, det kommer til at tage tid. Og det som vi, hvis jeg lige skal sige noget, i advokatbranchen, vores lille butik venter på, det er at advokatsamfundet kommer med en vejledning i hvordan de her persondataregler skal håndteres. De nye i hvert fald. Revisorerne har fået deres vejledning. Den er sådan set udmærket. Men jeg har ikke tænkt mig at flytte rundt på Elsebeth derinde, eller Helle dernede, uden at have rygdækning og sige: "Nu skal vi til at gøre sådan." Jeg har sådan fodret dem løbende, og sagt at nu står vi og overvejer at kryptere. Det begynder kunderne selv at spørge om. Og alt det der. Så de ved godt, at der kommer et eller andet. Men jeg sidder og venter på at den kommer. Men… øh… Det var vist ikke det, der var spørgsmålet. Tilbage til hvad der er passende organisatoriske sikkerhedsforanstaltninger. For mig at se er det stadigvæk, selv for IT-virksomheder af en hvis størrelse, som i øvrigt har styr på deres informationsaktiver, som sådan breder puljen ud af deres persondata. Det er fandme håndholdt. Det er eddermame håndholdt. Fordi det er der jo ikke nogen, der har styr på. Vi skal jo fandme være her fra 8-15.30, så skal vi ud af døren, langt størstedelen af arbejdsstyrken, så skal de hente børn og sådan nogle ting. Det der med at tænke på de der sådan lidt meta-driftsorienteret opgaver, forget it! Så sidder der en ledelse måske, men det er de da slet ikke interesseret i. Det gider de da ikke. Find nogle nørder, ikk? Det som man også lige skal huske på, at det er i selv ret store virksomheder, som er over de der 150 medarbejdere, så det ikke længere er en SMV, det er det jo ikke… Danske virksomheder er skåret ret godt til som udgangspunkt. Der har man jo ikke en større administration eller en kyndig og faglig dygtig stabsfunktion, som lige kan lave det der projekt. Det har man ikke! Du har en salgsafdeling, der sidder sælgere! Der er en HR-afdeling, der sidder folk der administrerer folks løn og ansætter og fyrer. Så har vi en ledelse, som konstant er på jagt efter nye markeder, og er panik for at miste. Og så har du folk, der er ude og køre i lastbiler, ikk? Altså who the fuck skal tage sig af det her, punkt 1. Punkt 2, det er jo ikke lige som et parforhold, hvor manden ikke lige får hængt de der billeder op eller ryddet ud i garagen, hvor opgaven er nem at gå til, og den er veldefineret. Her er opgaven sådan fuldstændig kaos, ikk? Og det som mange SMV'er, eller virksomheder generelt, er lidt nervøse for, det er, så ringer vi bare til Bech Bruun, for så ved vi godt, hvad der sker. Det kan godt være, med mindre man er Novo Nordisk eller Lego, de har deres egen, de er så længere oppe i hierarkiet, de har deres egne folk, men et eller andet sted, så har man jo heller ikke lyst til at ringe til syv konsulenter, som farer rundt i huset og efterlader sig en kæmpe regning. Så ved man ikke rigtig hvad det er, fordi når reglerne er så svære at forstå for mange og luftige. Så kan du ikke engang forstå værdien af dét. Altså du forstår ikke engang, at du har et behov. Jeg har i dag holdt et møde i en anden virksomhed hvor vi skulle lave en IT-kontrakt med nogle web-folk, og så, det jeg jo altid gør, man skal jo aldrig prøve at levere en opgave uden at prøve at se, om man kan få en med igen, sådan er det jo, man skal jo tjene penge. Current business og alt det der. Så nævner jeg lige, at jeg går ud fra, at de har en anden advokat til at tage sig af deres databeskyttelse, siden de ikke har nævnt det. "Databeskyttelse, hvad for noget?" Jaaaa, altsåååå… Og det vidste de slet ikke. Det er en web-baseret portal, hvor…Nu skal jeg prøve at formulere det så forblommet som muligt, så I ikke ved hvem det er, fordi det er jo ikke så godt, det er en IT… Altså de kører på web, men de har selvfølgelig et fysisk lager, og det de gør, det er, at de leverer til en masse dagsinstitutioner. Det er ikke fordi, de får navnene på børnene og alt muligt, men de får en masse oplysninger, købshistorik, og de skriver mails frem og tilbage med de her

medarbejdere og B2B oplysninger, som jeg forstår det, også er persondata. Det er også noget, som skal håndteres sikkerhedsmæssigt korrekt. De har absolut kæmpe arkiver, og de har aldrig tænkt over noget som helst, osv. Og hvad skal man sige, de tjener penge og har det godt, men hvad er de, de er 20-30 mand, og der er ikke nogen der har tænkt over det. Overhovedet. De er på 0. De fleste har efterhånden set en EY-, KPMG-, Bech Bruun-, Kromann-pamflet. Det var blankocheck. Derfor sagde jeg også til dem, prøv at gå ind og google "databeskyttelse GDPR", og ring til mig hvis I ryger helt op i det røde felt af nervøsitet, så skal jeg nok få jer ned igen. Og hvis i googler det, og ligesom 0 reagerer, "hvad der det? Det er irrelevant for os." Så prøv lige at ringe alligevel. Hvis I er på et af ydrepunkterne så ring. Men hvis I er in the middle of the road, hvor du begynder at forstå hvor I er, og at I selv kan se, okay der skal ske et eller andet her, så vent med at ringe til mig, til I rent faktisk vil have gjort noget. Men hvis I overhovedet ikke synes, det er relevant, eller I ryger helt op i det røde felt - så ring lige. Men det er bare for at sige…

4. ***F/J:*** *Og de har ikke ringet endnu?*

R: Nej, nej, nej… Folk har bare hovedet nede i den spand, der hedder "vi skal tjene penge". Det har jeg jo selv. Jeg glæder mig jo ikke til at skulle sidde og bruge fire dage på det her, vel? Men herinde kommer jeg jo så til det.

5. ***F/J:*** *Nu skal jeg lige se hvad vi har været inde på, og hvad vi ikke har været inde på. Vi har jo snakket lidt om det, men nu nævnte du meget IT-virksomhederne, men føler du, at alle dem du er rådgiver for stejler på den her art. 25?*

R: Ja!

6. ***F/J:*** *Er det simpelthen den værste nærmest?*

R: Det værste er, at de skal gøre noget overhovedet, så det er sådan en samlet følelse af træls. Især for IT-virksomheder, men rigtig mange produktionsvirksomheder, de almindelige virksomheder. Når først IT-chefen, han eller hun, står med det her, så er det egentlig bare oprydning. I skal ikke tage fejl af, når man siger til selv kyndige IT-virksomheder: "Hvem er jeres databehandler", "Hva' for noget??" Det er sgu ikke sikkert, at de ved det. Det er ikke sikkert, at de har tænkt over det. Fordi, så begynder de lidt, "Vi har da egentlig nogle servere stående selv", og "jamen vi har da noget back-up dér". Så er der også nogen, der finder ud af, jamen hov alle de dér, dem er der aldrig blevet gjort noget ved. Så de sidste 15 år når folk er gået fra, så er der ikke blevet gjort noget ved det. Så kan det jo sagtens have været sådan, fordi man ikke har haft kontrol og styring, med hvad folk kunne downloade. Jamen så er der nogen der har downloadede dét system gratis, og det betaler vi så stadig til. Det er det der hedder skygge-IT. I rigtig mange organisationer, er det et rigtig godt spørgsmål at sige: "Hvad bruger I egentlig af IT-systemer?" "Hvad?" Selv nogle af de der virkelig professionelle drenge, som sætter softwarekoder sammen, der har jeg været til to møder, hvor de simpelthen kom op at slås. Så gennemgik vi listen over alle deres byggeklodser, og så stod de: "For helvede jeg sagde til Mikkel for 400 år siden, at vi

skulle sige det dér op!" Så er der en af dem, der siger: "Det bruger vi da stadigvæk engang imellem." "Jamen I skal bruge det hér…" De ved sgu ikke nødvendigvis, hvad de har af IT. Og de ved slet ikke, hvad de har af skygge-IT. Det er så de værste eksempler. Så har jeg også været ude ved det, jeg vil kalde igen en almindelige produktion/servicevirksomhed, de havde så kun et IT-system, så det var super nemt. Manøvre nummer 1: Slet for helvede, slet! Fordi det du skal tage ansvar for, det er det du har. Du kan bare komme af med det. Hvor meget skal du forsikres for? Hvis du har fire huse, så er det dyrt at forsikre, især hvis du ikke skal bruge tre af dem. Og det er da bare med at komme af med det, man ikke skal ha'. Hvis du skal have compliance dokumentation på det, jamen så, som jeg siger, det er lidt som at købe en forsikring. Jo mere du vil have liggende, jo større og dyrere bliver forsikringen. Så…

7. ***F/J:*** *I forhold til den her forandring som der egentlig sker ved, hvis man kigger på medarbejdere og hvis man kigger på brugen af ressourcer, hvor er det så, man egentlig ikke er villig som organisation til at forandre sig. Altså hvor er problemerne henne? Er det hvis du snakker medarbejdere – stejler de så?*

R: Dem der altid stejler, det er dem der, nu siger jeg det som det er, dem der har tre års uddannelse eller mindre. De gider ikke det her. Regnskabsassistenten, sekretæren, HR-medarbejderen de synes, at det her, det er røv og nøgler. Men det er jo også fordi, og nu siger jeg det bare, det er måske også sådan en medarbejdergruppe, som ikke sådan føler det helt store tilknytningsansvar for virksomheden. De gør det dér, og så går de på dét tidspunkt, og så får de den dér løn. Det der; "Vi skal tage ansvar for andre folks data, det er dig der holder dem, du låner dem i virkeligheden, og så skal du slette dem. Du skal passe på andre folks privatliv." Det der med at der kommer en eller anden etisk dimension, der lyser ned i deres stilling, det bliver lynhurtigt: "Okay, når jeg sender en mail, skal jeg så ikke skrive…" Det er dét niveau, man skal ned på, eller sker der ikke en skid. Fordi at få den medarbejdergruppe til at klappe i hænderne og synes: "Neeeeej, vi skal lige løbe den ekstra kilometer, mega spændende!" Det er måske i virkeligheden også den medarbejdergruppe, som forstår mindst af, hvad der foregår af udvikling og ikke udvikling på nettet, og som en gang for alle, især i en hvis alder, har stemplet: "Internettet; du bliver overvåget i hoved og røv!" 100 % mistillid. Det virker som huller i luften. Så hvis vi snakker forandringsledelse, så er en kulturelændring i dét medarbejderlag, det skal foregå gennem nogle meget direkte og pædagogiske politikker ellers sker der ikke en skid. Så… Fx sådan noget med du må ikke lige sende det til din g-mail, så det er nemmere at tilgå om aftenen, fordi det er svært at tilgå sin VPN-forbindelse, fordi den kan godt være besværlig eller hoppe af engang i mellem. Så fx hvis du sender medarbejderoplysninger på en g-mail, så flyver det som udgangspunkt, i hvert fald som jeg forstår det, til et tredjeland, og det er jo bare et fucking mareridt det dér. Sådan nogle ting som det dér, det bliver svært.

8. ***F/J:*** *Og hvad med hvis man kigger på ledelsesniveau i forhold til at bruge ressourcer? Oplever du så, at folk…*

R: Den er vendt 180 grader! Og den er vendt 180 grader efter sommerferien. Før sommerferien, så var deeeet… Det er tre år siden, at jeg hørte i LEGOs legal compliance risc management group, der sidder jo 40 mand høj, M/K i øvrigt, de har jo også penge til det, og

der var ligesom styr på det. Fordi de havde verdensomspændende klubber for børn og medlemmer, så ja nemlig… Der er noget der. Men ellers så tror jeg godt, at man kan lave sådan et hierarki. Nu er Danmark godt nok sådan et SMV-land, jeg mener, at vi har 23.000 registrerede SMV'er, og vi har jo hvad, C20 det er lige præcis C20, haha! Det er ikke C120, men jeg tror godt, at man kan sige, at den er ved at gå op for folk. Men den kan gå op for folk af flere veje, har jeg fundet ud af. Fx har jeg en produktionsvirksomhed, det er gået op for dem, fordi gammelfar har fået en søn eller en datter, som ikke orker at overtage det, så skal det sælges, så kommer der smarte virksomhedskonsulenter fra København, som siger: "Hvis det skal sælges, så skal der laves en due diligence." Og det der står på de der clipboards, udover at man har styr på sine leverandørkontrakter, det er jo dine medarbejderkontrakter. Er der forurenet osv. Osv. Det er jo, hvad skal man sige, potentielle krav, der kan dukke op for en køber, som er ubehagelige. Og så kommer det jo lidt: "Har du styr på din persondata?" "Persondata, hvad snakker du om??" Jo, jo men der er ikke nogen der vil købe et persondataretligt-håndværkertilbud, med de risici der er forbundet på nuværende tidspunkt. Det er nok ikke så store risici i sidste ende, men det kan vi altid diskutere. Men at det nu er et punkt, som man skal have afklaret, det er helt utvetydigt.

9. ***F/J:*** *Så folk er blevet mere villige til at skyde nogle flere penge af?*

   R: Lige præcis, ja, ja, ja!

10. ***F/J:*** *Nu nævner du selv, at det var sommeren der gjorde det, men var det det tidsmæssige pres?*

    R: Ja, det er det da! Det er det da! Og det er gået helt bananas efter jul. Nu er der ikke noget, der står i vejen for nu og så 25. maj. Og om man vil det eller ej, så er sådan en data ret effektiv, skal jeg hilse at sige. Men nu tror jeg ikke, at der sker så meget. Ikke lige med det samme i hvert fald.

11. ***F/J:*** *Jeg tror, at vi alle sammen kommer til at stå sådan lidt d. 25. maj:"Nå….."*

    R: Ja, ja, ja der skal helt sikkert nok være en CEO eller to der på LinkedIn sidder: "Jeg gjorde ikke en skid, hvor mange penge har I brugt? Y2k problem!!"

12. ***F/J:*** *Hvilke typer af virksomhedsbrancher oplever du, har bedst styr på det her?*

    R: Ikke nogen!

13. ***F/J:*** *Okay, vi kan også vende den rundt, hvem har mest interesse, eller hvem tænker på det enkelte individ?*

R: Der er ikke nogen, som tænker på det enkelte individ. De tænker på deres forretning. Det er det de tænker. De tænker: ”Vi skal til læge og have en vaccine, og det er irriterende, det koster penge, men det er vi nødt til, for ellers risikerer vi at dø af det.” I virkeligheden kan man sige, at de registreredes rettigheder, det er kronjuvelerne. Det er det, som vi alle sammen med de her regler skal passe på. Pbd/d er for at beskytte de enkelte personer. Men når jeg er ude i virksomheder at snakke om implementering, så har jeg efterhånden vænnet mig til, hvad de gider at høre. Og de registreredes rettigheder, som jeg som jurist kan se, er absolut det væsentligste, det kan jeg godt som advokat se, at det er ikke det, som de gider at høre om. Så vi skal lige have en gennemgang af det, så de er opmærksom på det. Men de vil høre implementering, de vil høre om sikkerhed de vil høre praktiske tiltag, de vil høre hvad er det så for nogle dokumenter, vi skal ha’. Det der med en gennemgang af indsigtsretten, begrænsning af dataportabilitet, de er bedøvende ligeglade. ”Du skal kunne klare en anmodning, hvor der står det her! Hvad gør du konkret? Lav en vejledning på det – fint, done! Hvad mere?” Der er ikke nogen, der tænker: ”Pas på nogens data.”

14. ***F/J:*** *Lige for at vende tilbage til det du egentlig spurgte om, med hvem klarer sig bedst? Omvendt hvem er mest udfordret? Er det IT-branchen?*

R: Ubetinget! Ubetinget! Og du kan jo lave en skala, for IT-branchen er jo mange ting. Men de der data-brokers, markedsføringsfolkene, de er jo hardcore ramt på det her. Men alle softwareleverandører, uanset om det bare en ESDH-løsning, allesammen er jo ret hårdt ramt på det her. Og jeg kan ikke se andet, end at de der må sætte sig ned og tage det her pbd/d meget seriøst. Men det er bare svært for den dataansvarlige at gå hen til sin databehandler og sige: ”Du skal overholde pbd”, så siger databehandleren: ”Okay, kom, giv lige 10 linjer om hvad jeg skal rette i mit IT-system.” Arrrrgggh. ”Det er noget med nogle fritekstfelter, som skal være nogle dropdown-menuer. Og jeg vil gerne have noget… måske noget kryptering.” ”Når okay, jamen det kan vi godt lave.” Bum! ”Var der andet??” ”Naarjj, jaaa…” En dataansvarlig skal jo hyre en kompetent IT-konsulent, for det har de jo ikke. Det er jo outsourcet til at have den der kontakt. Så skal den dataansvarlige jo være så bevidst og stærk, at man kan sige til IT-konsulenten, klæde den IT-konsulent for at kunne gå til en reel forhandling med databehandleren om det her. Det kommer ikke til at ske!

15. ***F/J:*** *Har I her i huset skabt nogle redskaber, som I bruger, når I er ude?*

R: Jamen jeg har min kære skabelonsamling. Ja, ja, ja, ja det bruger jeg meget af. Det har vi brugt hele sommerferien på.

16. ***F/J:*** *Men du har ikke et decideret IT-mæssigt redskab?*

R: Ja, ja, jamen den måde jeg rådgiver på, der er jeg aldrig én mand på posten. Det er jeg, hvis de selv stiller med nogle IT-folk, men ellers så er jeg altid rådgiver som del af en klynge. Den måde jeg får opgaver på, hvis jeg står i midten, så flyder der opgaver fra et IT-hus som har nogle kunder, som de laver noget for. Så trækker vi så nogle IT-specialister ind. Jeg er altid en del af et hold. Altid. Fordi noget af det jeg ikke har tid til, eller ikke kan

finde ud af, det er projektledelse. Jeg er ikke projektleder. Jeg kan sagtens stille nogle planer op og så videre. Men det der med at sørge for at få indkaldt til nogle møder, at sørge for det ene, det andet og det tredje, og få den rigtige information på det rigtige tidspunkt – forget it! It's never gonna happen. Det er ikke en del af mit job. Det… Mit job er at ligge hånden på kogepladen, og sige om noget er okay, eller om det ikke er okay. Og så lave nogle formuleringer så det flyver nogenlunde igennem nåleøjet.

17. ***F/J:*** *Vi har været ude at interviewe en stor koncern, og der blev der blandt andet nævnt, at det der var problematikken, det var hele ledelsen og hele kulturen i det. Og det er jo det, du også har sagt. Så sagde de blandet andet også, at det der var svært, det var, hvis man får de her nye IT-systemer ind, eller tools som de har, bla. Bech Bruun som har et eller andet fancy tool, det er, at man først skal lære det, og så skal man samtidig implementere det. Er det noget af det, du også oplever ude ved dine kunder, at de går lidt i panik over, at de ikke kan finde ud af det?*

R: Det som de alle sammen sidder… Jeg arbejder sammen med (en række programmer), alle de dér. Som har i virkeligheden ledelsessystemer, som de gerne vil lave procesunderstøttelse på. Problemet er bare, det er stadigvæk håndholdt! Det er bare en fancy måde at have sit skide excelark på. Det er stadigvæk bare et excelark, det ser bare pænere ud. Sorry to say! Et glorificeret fucking excelark. Og det som er svært at sælge, med mindre man er en væsentlig større virksomhed, som har noget brugbart, det er fint nok, at du skal betale nogle konsulenttimer, hmm okay! Så skal du også betale for et IT-system, som er en løbende ydelse. Jeg kan godt fortælle jer, at det IT- og softwareudvikleren lever af, det er jo at som udgangspunkt, når først man er kommet ind i en virksomhed som software, så ryger man sgu ikke ud igen. Når først man får lagt folks compliance over i dét her system, så bliver de ved med at betale for det. Så der er nogen af de der folk der, hvis vi laver noget sammen for en virksomhed, det er ikke fordi de ikke er dygtige, det er ikke det. Deres udgifter til mig er jo sådan her. (Tegner graf.) Og deres udgifter til IT-system det ligger her. (Tegner graf.) Hvor mange kvadratcentimeter er der hér, mod hvor mange kvadratcentimeter er der hér? Og så tegner vi bare, ikkå. Det her, det er jo ingenting, i forhold til, men det er stadigvæk rigtig svært at sige til dem: "Jamen du skal i virkeligheden betale et ekstra stykke for dit excelark i en glorificeret udgave". Nu er jeg en lillesmule hård. Men jeg bliver ved med at spørge de her folk, der leverer det her, de kalder ledelsessystemer: "Jamen er der en reel integration med mail-systemer?" Hvis vi vedtager, at der er en slettefrist på 30 dage i det her system, og du så siger "OK" til det, og du så skyder det ud til medarbejderen. Er det så sådan, at der er fuld integration med Outlook? Så der allerede ved at skyde den slettefrist ud til folk, at der så også bliver slettet? Nej! Det skal du selvstændigt ind og ændre. Så det der system er for mig et se, et system ovenpå de andre systemer hvor der ikke er nogen forbindelse. Og så er jeg sådan lidt…. Så det er meget ambivalent det dér. Jeg kan godt se for nogen virksomheder, hvor man i forvejen har mange systemer, til at kommunikere med, altså mange detaljesystemer. Dét her system til HR, dét her er vores mail, dét her er vores journalisering, dét her er vores salg, dét her er vores udvikling. Så giver det fin nok mening, at man har en klods herovre, der hedder ledelses compliance, et eller andet hvor man kan have nogle andre ting i forvejen, fordi man måske ligger meget decentralt. Butikskæde med ét hovedkarter med flere forskellige afdelinger rundt omkring. Fint nok at man sådan skal skyde informationen ud til folk andet end på en mail med en pdf. Den sletter folk, den læser de ikke. Lige så snart det kommer fra IT-afdelingen og det

ikke umiddelbart handler om noget de skal lave i dag eller en mulig/potentiel kunde – UD! Det er sådan det er. Så det her med, at alle er koblet op på det her ledelsessystem, du får en ny vejledning vedr. din funktion, du skal nu afgive en listekvittering, og hvis ikke du overholder det, kan det få ansættelsesretlige konsekvenser. Jeg kan godt se, at det giver mening i nogle sammenhænge. Men det som jeg synes, for de flest må give mening, det er at vente på, at de rigtigt IT-systemer kommer. Som reelt er bygget på det I skriver om pbd/d og som reelt på en teknisk måde kan løse mange af de der udfordringer. I stedet for at man bare har endnu et system ovenpå de andre systemer, fordi det system er for mig at se bare et journaliseringssystem, det gør jo ingenting! Du skal selv sidde og skrive din processer ind. Nu har jeg så hjulpet de forskellige med at lave nogle standart processer i HR-systemer, fordi det er meget standart det der forgår i forvejen. Der ligger en databehandleraftale i forvejen og der er nogle dropdown-menuer man kan tjekke efter: "Hvem er din databehandler?" "ja/nej" til databehandleraftale. Har vi tjekket 3. land "ja/nej". Underdatabehandling "ja/nej". Og så videre. Men det er bare stadigvæk under et IT-system, så det handler om hvordan man generelt pædagogiskset har behandlet det internt i virksomheden.

18. ***F/J:*** *Så summa summarum er, at man egentlig skal fortsætte med det her håndholdte compliancearbejde, indtil man måske skal ud og investere i et IT-system, der faktisk kan give dig hele pakken?*

R: Det synes jeg!

19. ***F/J:*** *Så er det gode spørgsmål så, hvornår de her IT-systemer så kommer?*

R: Det er et totalt åbent marked, som for få har set. Jeg kan desværre ikke gøre det, jeg har ikke tid til det, jeg har ikke muskler til det. Jeg har ikke indsigt til det. Men jeg synes, at lave et compliancejournaliseringssystem – come on! Jeg kan slet ikke forstå, at man ikke kan få nogle reelle konkurrenter ind til Windows. Jeg kan ikke forstå, at vi ikke kan få en reel konkurrent til fx mail. Noget af det der irriterer mig allermest med Windows er, det der irriterer mig allermest med Outlook 365 er, hvis man har kørt noget big data på hvilke funktioner folk rent faktisk anvendte i Windows, i Outlook 365, jeg tror det er under 1 % af de knapper der reelt er der, der bliver anvendt. Hvorfor laver man ikke, for at sige det som det er, en baby-udgave af et mailprogram, hvor der bare er top styr på sikkerheden, og du kan kun det her. Så kan du gå ind og vælge det til i stedet for at knapperne er synlige, altså hvorfor skal det være så kompliceret? Og jeg tror, lidt tilbage til det jeg startede med at sige omkring den digitaleudbygning der nu er ved at komme, det svarer jo lidt til, at hvis du i game dage gik fra Aarhus til København, så er det eddermame besværligt, du skal gå ikkå, du skal måske lidt med hestevogn, det tager lang tid. Underforstået at når vi skal journalisere, når vi skal sende en mail, jeg ved godt, at det er et plat eksempel, så alle de der klik, klik, klik, klik, klik frem og tilbage og sådan nogle ting. Alle de der muligheder på standartindstillingerne, det er grus i maskineriet, det forstyrrer hjernen! Hvorfor skal man bruge tid på alt det der skrammel? Lav et simpelt, enkelt setup. Jeg fatter ikke, hvorfor der ikke er nogen, der ikke har lavet det?! For fanden! Jeg fatter heller ikke hvorfor der ikke er nogen der lavet et social media netværk, hvor folk er anonyme, vi tracker lige præcis ingenting, vi sender lige præcis ingenting videre. Men det er nok fordi i sidste ende, og det er jo der den er svær, vi vil jo gerne have noget digitaludbygning. Hvis folk, og det er jo i

virkeligheden forbrugeren der rent faktisk skal vænne sig til at betale for det, hvis folk ikke vil betale for det, og man ikke kan bruge dem som produkter, altså tracke dem, putte dem ind til profiler, sælge dem videre til markedsføringsfolk – hvor skal pengene så komme fra? Hvem fanden er det så, der skal gøre det her? Græsrodsorganisationer? Eller hvad? Er det studerende fra DTU? Google Maps er vi jo også glade for, men hvor kommer pengene fra? De der lorte-biler er jo kørt rundt! Hvor skal det komme fra? Der er nogle ting dér, som jeg synes er interessant.

20. ***F/J:*** *Nu er vi faktisk løbet tør for tid, men vi er også løbet tør for spørgsmål, så det passer rigtig godt. Tak!*

Bilag 2 - Interview med dataansvarlig i virksomhed X

Interviewer: Frederikke Schlitterlau og Julie Enø Jensen = F/J

Respondent: Dataansvarlig i virksomhed X = X

1. ***F/J:*** *Jamen altså, vores tanke, det var at, i forhold til det juridiske, så går vi egentlig ind og analyserer på hvad der er indeholdt i artikel 25. Privacy by design. Og er egentlig mere eller mere nået i mål med hvad der ligger i dét. Det er baseret på hvad der tidligere er skrevet alle mulige steder.*

   X: Så det er en komparativanalyse? Gældende ret og fremtidig?

2. ***F/J:*** *Ja, lige præcis. Og der bygger vi så på, for jeg har været i praktik med hele det her GDPR, hvor jeg skulle implementere det ude i en virksomhed. Og det jeg egentlig mødte, det var at det var sværeste at få folk til at gøre det. Det var ikke så meget, om jeg kunne forstå loven, og om jeg kunne sige, hvad der skulle til, og hvad der ikke skulle til og give min anbefaling. Så derfor har vi bygget det op på, hvordan man kan få folks interesse og få dem mere engageret. Organisatorisk agilitet omkring forandringsledelse og fleksibilitet. Og at man måske skal fokusere på de søjler, der er i den teori for at kunne implementere det, som man ret faktisk gerne vil i forhold til GDPR. Så det er egentlig sådan det er bygget op. Hvor vi starter med hvad der er indeholdt i art. 25 og så bygger det op på et framework på de her forskellige søjler inden for organisatorisk agilitet.*

   X: Tænker I så, at det her problem der kan opstå i forhold til at få folk til at følge det flowchart, man nu har lavet? Eller følge den procedure man nu har udarbejdet? At det er særligt relateret til art. 25? Eller er det bare jeres udgangspunkt?

3. ***F/J:*** *Det er ikke kun særligt art. 25.*

   X: Min umiddelbare tanke i forhold til art. 25 er, at den er så bred – altså det er alle bestemmelserne i forordningen jo til dels. Men at den er introduceret som et helt nyt regime, på en eller anden måde, som ikke er kendt før. Derfor bliver den lidt mere uhåndterbar. Så hvordan er art. 25 og forandringsledelsens vinkel koblet på hinanden?

4. ***F/J:*** *Vi har fokuseret på, at de tiltag man skal gøre i art. 25, det skal man have nogle mennesker til at gøre. Hvordan får du de mennesker til at gøre det? Og bagefter opfølgning, for det er jo ikke kun at du siger, "nå men så krypterer vi alt vores", der er jo også en håndtering i hvordan du bruger din computer i din dagligdag. Hvordan du som medarbejder bare smider det ene og det andet fysiske papir. Så det er på den måde, at vi ligesom siger hvad der er indeholdt, men hvem er det så der skal gøre det? Det er jo faktisk med-*

arbejdere. Hvordan får du så medarbejderne til det, for du kan jo godt sidde som dataansvarlig og sige, "I skal helst ikke have fysiske papir", men hvordan får du folk til at gøre det? Osv. Osv. Osv. Så det er egentlig den vinkel vi har taget på det.

X: Det er også det allersværeste overhovedet. Som du selv siger, så er det også det, jeg har oplevet her. Det var egentlig noget af det, jeg tænkte, før jeg startede, at det sværeste i den her stilling det ville være helt konkret at vurdere reglerne og finde ud af, hvornår gælder dét, hvornår gælder dét? Men det sværeste, det er at få organisationen med. Det er det uden tvivl. Og som jeg lige sagde før; når man har lavet sådan et flowchart, eller når man har lavet sådan en procesbeskrivelse, hvor der står, at folk de skal hoppe – hvorfor hopper de så ikke? Det gør de ikke, fordi de ikke… Altså det er jo ikke af nogen ond vilje, det er vane og det er et spørgsmål om at det går hurtigt og at der er travlt og at der er pres på.

5. ***F/J:*** *Og der er også mange, som måske ikke forstår vigtigheden i det. Det er ikke en del af deres hverdag og det de laver normalt.*

X: Det første step har været at finde ud af, hvad har vi overhovedet har af politikker – og så få det udviklet. Og det næste step kommer så, når det så er udviklet – vil folk så følge det? Jeg synes, at det er en rigtig god idé, at I tager fat i forandringsledelse, fordi jeg tror, at det er det helt centrale aspekt. Man ser jo tit i forhold til data breaches, når processer ikke bliver fulgt. Det er egentlig ikke så tit, at det er et IT-system der svigter, som når det er en medarbejder, der ikke har været fuldstændigt sat ind i en proces for hvordan en given databehandling skal foregå. Og det ved, at det vores IT-afdeling har highlightet mange gange, det er at det er person behaviour og ikke IT-systemer. Man kan ikke bare ligge det ned i en IT-afdeling og så bede dem om at være GDPR compliant, det mener jeg i hvert fald ikke. Det ved jeg, at man gør mange steder, og der vil jeg være nysgerrig på, hvordan man sikrer netop privacy by design.

6. ***F/J:*** *Det er jo ikke kun teknisk, det er også organisatorisk.*

X: Præcis! Og det jeg har gjort, det er, at jeg har planlagt vores compliance-projekt sådan, at jeg først har mappet – det gør man, og det har været nødvendigt alle steder. Data-mapping; fundet ud af, hvad har vi på hylderne? Hvordan bliver det behandlet nu? Hvad bliver det brugt til nu? Hvor får vi det fra? Hvem bliver data videregivet til? Efter hele den her mapping-proces blev afsluttet, så har jeg lavet GAP-analyser. Det jeg har ikke lavet bare for virksomheden som sådan, det har jeg egentlig inddelt efter hvordan vores organisation er opbygget på, både produktionsfaciliteter, HR-afdelingen, Health and Safty-afdelingen, Legal and Riscs som jeg selv sidder i, Finance, rigtig mange forskellige IT-afdelinger, Marketing og kommunikations-afdelingen, Salgsafdelingen. Hver eneste afdeling har jeg snakket med, lavet workshops med, lavet interviews med og mappet data. Så har jeg lavet GAP-analyser. Og den indgangsvinkel jeg har haft til GAP-analyserne har været, at netop for at undgå, at det bliver mig der sidder og dikterer, hvad de skal gøre. "Nu har vi haft det her interview, det kommer til at munde ud i en ny proces inden for det her område, den bliver klar inden d. 25. maj, og efter d. 25. maj skal I bare følge den." Jeg kom ud i nogle scenarier, hvor jeg slet ikke kender de medarbejderes daglige arbejde godt nok til, at give

et bedre bud på, hvordan de kan løse deres opgaver på på en GDPR compliant måde, end de selv gør. Så min indgangsvinkel har faktisk været at ligge ansvaret ud til dem i højere grad, og så i højere grad at få dem til at forstå principperne. Fordi selvom GDPR er så lang og kompleks og fyldt med undtagelser og modifikationer og forskellig nationallovgivning, så er selve de 7-8 grundlæggende databeskyttelsesprincipper jo nemme at forstå. Og det kan alle forstå, hvis de vil. Så jeg har egnetlig prøvet, når jeg har snakket med folk, at bruge en del tid på at sætte dem ind i kernen i lovgivningen og hvilke hensyn vi forsøger at varetage, og så sige til dem: "I forhold til det I gør nu, hvordan kan vi gøre det bedre, for ligesom at tage hensyn til de databeskyttelsesprincipper, som er i lovgivningen?" Og så ligesom sige: "GDPR det er en stor ramme, men inde i den ramme, der er der plads til, at I kan lave og tilrettelægge en proces, som også passer for jer." Min teori er, at hvis det bare kommer ovenfra og ned, så er der mindre sandsynlighed for, at medarbejderne følger det, end hvis de selv er med i beslutningsprocessen, med i udviklingen, altså policy-arbejdet, med i afregningen af hvor man kan få mest value for den ændring, som man nu ligger for dagen. Hvilke relativt små ændringer, som ikke betyder så meget for dem, kan man hurtigt implementere, og hvilke steder kan det virkelig være besværligt for medarbejderen at lave om. Så hele den her baggrundsforståelse, det er det primære. Så det bliver ikke bare taget ud af hænderne på dem. Jeg giver dem en opgave, og det er noget jeg har fundet ud af hen af vejen, at det er den eneste måde, at jeg har kunnet gøre det på. De skal have ejerskab i processen, og den eneste måde, at man kan få folk til at få ejerskab, det er hvis de forstår vigtighed og hensynene og at de også forstår, at det også er en interesse for virksomheden som sådan, og at det faktisk bliver prioriteret af deres managers. Så det er den konklusion, jeg ligesom er nået frem til. Konsekvensen for at kunne gøre det, så er det klart, at mine GAP-analyser de er ikke bare tre sider, de er enormt lange. Manageren for en konkret afdeling bliver sat ind i tingene og får den opgave at sætte medarbejderne ind i det, så processen er allerede i gang, når legal kommer ind i billedet. Så det er egentlig afdelingerne selv der går ind og arbejder med det, og så kommer legal på som rådgiver bagefter.

7. ***F/J:*** *Hvordan er du kommet på det her? Er det bare fordi, at du fandt ud af, at det ikke virkede at trække noget ned over hovedet på dem?*

X: Ja, det tror jeg. Altså, jeg bestilte en bog fra en jurist som har en baggrund i psykologi, "Forandringsledelse uden forandring", Jeg var til et oplæg med hende, og det var simpelthen så pisse godt, og stemte overens med de tanker jeg selv havde gjort mig, og det underbyggede bare, at det var den rigtige måde at gribe det an på, ved at gå mere i detaljen fra starten. Det at jeg har valgt den her fremgangsmåde har jo gjort, at vi er bagud i forhold til policy-arbejdet. Der er en masse ting, som vi står nu og skal have færdigt inden d. 25. maj – dokumentation osv. Det har der ikke været tid til at få udarbejdet, fordi GAP-analyserne har været lange og det har taget lang tid at få folk til at forstå de her grundlæggende ting – så det kommer så nu. Men det har været vurderingen, at det her godt har kunnet betale sig på den lange bane. Har I set den årsrapport fra Datatilsynet, hvor de laver sådan en liste over hvor mange henvendelser de har fået? Jeg tror, den er fra 2017. Der er sket en stigning i antallet af henvendelser på 40 % til datatilsynet fra private personer, som har enten en klage eller en forespørgsel til datatilsynet. Så det for mig indikerer jo, at der hvor man skal være "bange" for at blive ramt som dataansvarlig og som virksomhed, det er ikke om datatilsynet står herude d. 26. maj og banker på, det er at nogle af vores egne medarbejdere problematiserer den måde vi behandler deres oplysninger på fordi der er større fokus på

det den vej rundt – og ikke så meget fra kontrol. Folk bliver opmærksom på, at de har den ret. Så jeg forudser, at vi får langt flere henvendelser fra fagforeninger og andre interesseorganisationer som repræsenterer datasubjekter – lønmodtagere – og som vil bruge det her som reparation på samme måde, som man ville gøre i alle andre situationer, som man ville gøre, hvis der skulle opstå en eller anden form for disciplinærsag, som gør, at medarbejderen har en eller anden interesse i at ramme vores virksomhed hårdt på en eller anden måde.

8. ***F/J:*** *Hvordan har medarbejderne så modtaget alt det her? At de har fået den her medbestemmelse?*

X: Det er noget, der er kommet lidt hen ad vejen. Til at starte med så var det sådan lidt: ”Hov, så det er ikke bare noget legal laver? Vi får ikke bare af vide hvad vi skal gøre – nå!” Det har heller ikke været sådan lige let. Da jeg startede, der blev det arrangeret, at jeg skulle rapportere ind til en stirring committee, som består af de chefer, hvis område har størst relevans i forhold til projektet. Dvs. Min egen chef som er head of legal og HR-chefen, chefen for vores finansafdeling og så chefen for vores IT-afdeling. Jeg har aftalt med dem, at jeg skulle lave nogle møder med cheferne i alle andre afdelinger. Det gjorde jeg dels for at sætte dem ind i vigtigheden af det, dels for at få dem til at pege de vigtige medarbejdere ud, som jeg skulle snakke med! Det har haft en effekt, at når jeg så har haft interviews eller workshops, så har de medarbejdere jeg har talt med, de har også hørt det fra deres nære chef. Det tror jeg, har en betydning. At dem som bestemmer, hvordan man skal disponere sin tid, at det er dem der siger, det her det skal du prioritere. Det tænker jeg har gjort en forskel. Ikke dermed sagt, at det har været problemfrit, men det har været med til at gøre det lidt lettere. Det har været et projekt, der har været fokus på, og det har været et projekt, der har været omtalt af ledelsen flere gange. På vores kvartalsmøder har det været nævnt og jeg har også forsøgt at komme med artikler på vores intranet, så på den måde synes jeg egentligt, at der har været ok opbakning til det, men der er sindssygt travlt her – sindssygt travlt – så på den måde kommer det bag i køen. Men jeg tror helt klart, at det har gjort en forskel, at det kommer fra deres egen leder også.

9. ***F/J:*** *Har I fået nogle resultater fra jeres GAP-analyser? Når de i mål, med det du gerne vil?*

X: Efter de har fået afleveret GAP-analyser, skriver jeg en generel mail til chefen om, at det er her der er blevet fundet i din afdeling ud fra de interviews, der er blevet lavet med dine medarbejdere. Og jeg har faktisk også lavet et referat fra alle mine datamapningssceancer/workshops, sådan at lederen selv kan gå ind og se, det er det her mine medarbejdere har gået ind og fortalt. Så beder jeg chefen om at bekræfte det, af hensyn til at dække mig selv af, hvis nu der er noget, der er misset, eller jeg har lavet en forkert vurdering, eller at de ikke har fortalt mig alt. Når de så har fået GAP-analysen, er cheferne blevet bedt om at lave en action-plan. Så i forhold til hver enkel finding er de blevet bedt om at tage stilling til: ”Hvem har ansvaret for det her?” Og: ”Hvornår regner vi med, at det kan være færdigt?” Er der noget, som vi ikke kan nå inden d. 25. maj, så skal vi vide det. Så skal vi tage stilling til, om det er den rigtige rækkefølge, vi prioriterer tingene i. Det har taget noget tid. Men ikke desto mindre, så tror jeg, at i kræft af GAP-analysen har været relativt detaljeret og

inddelt i 1.000 forskellige underdele, så har det været lettere for folk at gå ind og sige: ”Nå, men det er Michael, der normalt sidder med den type aftaler. Det er ham der har den her action.” Og så ligesom dele det ud i deres egen afdeling. Og så er min tanke så, og det er jo så det vi er i gang med nu i implementeringsfasen, alle har fået en GAP-analyse, alle har udarbejdet en action-plan, tanken er så, at når folk så løber ind i nogle problemer, så kan de tage fat i mig, for de skal prøve selv først, for at få ejerskab. Så den der action-plan den spiller en ret central rolle i det.

10. ***F/J:*** *Og hvad tænker du så efter d. 25. maj? Er det så bare ren vedligeholdelse?*

X: Jeg regner med, at der stadig vil være en del ting. Dels vil der være noget vi simpelthen ikke når. Så vil der være det helt centrale, som er et stort problem for mig, det er, at der egentlig er ret mange medarbejdere, som gerne ville gøre deres arbejde godt, og som har forstået det, og som spørger mig helt specifikt: ”Lige nu sidder jeg med det hér, hvad skal jeg gøre?” Hvor jeg så kan sige til dem: ”Det ved jeg ikke endnu.” For vi er ikke færdige, og vi kan først ligesom starte træningsprocessen, når medarbejderne har fået udarbejdet alle de her instrukser selv, de er blevet tjekket af legal, og de ligesom er blevet offentliggjort i vores system. Så det som ligger efter d. 25. maj, som er det helt centrale, det er træningen af medarbejderne. En del af vores scope i projektet det er, at der skal være en plan for træningen, men at træningen først skal eksekveres efter d. 25. maj. Og så har vi jo en quality afdeling, som auditerer inden for alle vores forretningsområder. Der er jo en masse, ISO-standarter og sikkerhedsstandarter og standarter for hvordan man producerer produktet. Det gælder i hele forretningen. Hvis du kigger på Tyskland og hvis du kigger på England, og du kigger på andre europæiske lande, så har de jo langt højere bødeniveau også, og de har allerede ekstremt stor fokus på det her. Vi har en tysk advokat ansat her, han er helt blown away, når han hører, hvordan det er, tingene de foregår i Danmark. Han kunne aldrig nogensinde drømme om, når han går til frokost, ikke at låse sin computer inde. Eller du ved, da han blev ansat her og skulle have nemID, så spørger han mig: ”Kan det passe, at de skal have mine oplysninger? Er det her normalt?” Altså, han har en meget større skepsis. Det et det, jeg møder. Den dér store kulturforskel i andre lande. Og den kommer virkelig til udtryk, når man arbejder i en international koncern. Vi har også datterselskaber i andre EU-lande, og der er der bare en anden tilgang til det. Det har virkelig en stor betydning for det mindset som folk har, når de går ind til det. Fordi, hvis det er en del af ens kultur, eller ens forståelse til at starte med, så tror jeg, at det er nemmere.

11. ***F/J:*** *Så kulturen kan også godt have noget at sige?*

X: Ja, det tror jeg. Danskere tænker: ”Whatever, de må gerne få min mailadresse – det er jeg ligeglad med.” Eller jeg bliver også mødt med: ”Jamen det er jo ikke noget negativt”, ”vi gør det jo ikke af nogen ond vilje” eller ”vi gør det gør for at hjælpe folk.” Eller: ”Ham her, han har selv sagt, at han gerne vil være på den her liste.” Eller: ”Det har han sagt til mig, da vi spiste middag sammen i torsdags.” Jamen, det kan jeg ikke bruge til noget. Og det tror jeg er svært for danskere at forstå, fordi vi har jo ikke den der datahygiejne, som de har i andre lande. Det der med, at man lige tænker: ”Har jeg egentlig lyst til, at de skal have de her oplysninger om mig?” Det er i hvert fald mit indtryk, at det er der mange

mennesker, der slet ikke kan forstå problemet i, og som synes, at det her er totalt overgearet. Og at der går Bruxelles i den. Men det er et udtryk for, at vi går fra 0 til 100 i vores bevidsthed om databeskyttelse.

12. ***F/J:*** *Hvor mange ansatte har i? Hvor meget data har du med at gøre?*

X: Vi har ca. under 3000 ansatte. Det er det det primære for os, men det der så er særlig i den her industri, er at der er enormt store dokumentationskrav til hvilke færdigheder du skal have for at arbejde med produktet, da den har så høj værdi som den har. Den bliver monoturet og holdt øje med på alle tænkelige måder. Der for er der også enormt store dokumentationskrav til vores kunder og over for certificeringsorganer, som er nødvendige at have for at kunne udføre arbejdet. Og så har vi selvfølgelig også en masse kunde oplysninger, som enhver anden salgsorganisation. Vi har så bare ikke kundeoplysninger på privatpersoner, vi har kunde oplysninger på andre virksomheder. Så det er lidt nemmere at komme om med end hvis det var sådan noget forbrugeradfærd man gik ind og monitorerede. Det lettere trods alt noget at det er et B2B set-up omvendt så gør B2B set-uppet også at vi ikke rigtig kan brande os på at være GDPR compliant. Hvor du kan egentlig sige at: ”du er certificeret inden for det og det”. ”Og kan sige at vi passer på dine oplysninger.” ”Vi overholder alle de regler vi skal.” Det kan vi ikke rigtig bruge som motivation her, da folk her ikke føler det skaber nogen form for værdi.

13. ***F/J:*** *Og så havde i også jeres egen interne rekruttering?*

X: Ja det har vi. Og vi lejer også andre medarbejder og bruger også eksterne konsulenter. Så det er ikke bare sådan regulære HR-data, som hvis du gik hos købmand Jensen og så på de 10 ansatte han har og så på hans personalemappe. Det er væsentligt bredere end det og forskellige kategorier. Men ja primært oplysninger om medarbejder og oplysninger om kunder.

14. ***F/J:*** *Har du sådan hele processen igen haft fuld support fra ledelsen? Altså har de stået bag dig i alt hvad du har foretaget dig eller har de også stillet spørgsmålstegn til hvorfor det skal implementeres det her?*

X: Øhm. Jeg tror nogen af dem, nu snakker jeg om den der stearing komiteen som jeg rapporterer indtil, som er vores C level managers. De har nogen, fordi det er stor en opgave og fordi de har så meget andet, nedprioriteret det. Og måske givet udtryk for at så længe vi har en plan den 25. så er det okay. Hvor at det nogle gange er frustrerende og nogle gange gør mit arbejde mere besværligt. Jeg vil ikke sige at jeg har fuld blowen support, hvor de har sagt at vi bare skulle gå i krig med det samme. Der har helt klart været skepsis til det. Jeg ved ikke rigtigt, hvordan jeg skal forklare. Der er ikke rigtig andre der ved noget om det end mig, så jeg tror det at der er en advokat der har siddet med det, før jeg blev ansat, som så ikke haft kapacitet til at sidde med den fulde tid. Men ham har jeg selvfølgelig kunne spare meget med. Men det er mere og mere blevet mit område. Jeg vil dog sige at min egen afdeling har der været opbakning, men på den måde at det er fordi de ved hvor

vigtigt det er og kan ikke stille spørgsmålstegn ved det jeg gør, da de ved det er nødvendigt, men de har ikke kunne stille spørgsmålstegn ved det jeg har gjort i forhold til om det er det rigtige at gøre, simpelthen fordi min chef ikke ved noget om databeskyttelse, så det er også sådan lidt underligt konstellation, da en chef normal tjekke at de ting man gør er rigtige, hvor at der har min chef bare valgt at det kan han ikke sætte sig ind i, det bruger han mig til.

15. ***F/J:*** *Ja okay det bliver opgaven så heller ikke mindre af også fordi det er meget du skal nå igennem. Nu ved jeg ikke hvor længe du har arbejdet med det?*

X: Ja præcis. Og nej ikke særlig længe, jeg blev ansat i september sidste år.

16. ***F/J:*** *Men da du så blev ansat i september, var det så fra day one at du var 100 procent på GDPR?*

X: Ja, det var simpelthen det de søgte. Jeg har så også lavet andet løbende, men det har været 90 procent af min tid.

17. ***F/J:*** *Og det regner du også med fortsætter med efter 25 maj?*

X: Ja det regner jeg med. Altså det er faktisk en projektansættelse jeg har, men det er en løbende dialog med min chef.

18. ***F/J:*** *Så det er egentlig først fra september af at du har fundet på din geniale ide?*

X: Ja og det var ikke engang dér jeg fandt på den. Jeg ved ikke, om det er, men synes det er flot, at du kalder den genial. Nej det fandt jeg først ud af, den gang jeg startede og så, at det her er fandme en stor opgave. Og det var ligeså meget en erkendelse af at "jeg kan ikke nå det her selv". Og så dengang jeg fandt ud af, hvor stor en betydning det havde at involvere medarbejderne, og hvor meget jeg kunne se at det betød, at de havde en medbestemmelse. Jo mere bekræftede det mig i, at så må jeg forsætte med at lave et godt benarbejde i forhold til at sætte dem ind i det, og så må jeg skubbe noget væk fra mig selv bagefter. Også fordi der er det der tidspres, da vi er kommet relativt sent i gang, eller altså de har været i gang lidt før mig, men der var mange ting, vi skulle samle op på. Når der så kommer en ny projektmanager ind og skal redefinere hele scoopet på projektet, og jeg kendte heller ikke noget til industrien og organisationen, så det skulle jeg også lige forstå, hvordan en virksomhed er bygget op. Det er en forudsætning for at kunne gøre det. Ellers forstår du slet ikke hvor dataflow i virksomheden er, hvorfor de er, som de er, hvis du ikke forstår, hvordan hele supply chain fungerer, og de forskellige afdelinger understøtter hinanden. Jeg kommer fra Cand. Jur., så jeg har ingen erhvervsmæssig erfaring.

19. ***F/J:*** *Der har været meget ved siden også at skulle sætte sig ind i det først.*

    X: Ja lige præcis. Det har været intenst. Men i forhold til artikel 25, har jeg særlig kigget på vores IT-systemer. Rent historisk er IT-systemer for det meste sat op til, at skulle gemme så meget som muligt i så lang tid som mulig. Så det konflikter enormt meget med privacy by design. Det har bare været en kæmpe udfordring. For hvilket system skal man så egentlig bruge, hvis vi skal opfylde det krav? Fordi, nu ved jeg ikke, om I kender SharePoint og Microsofts løsninger, for de er netop baseret på deling. Så bare det at skulle vælge den platform, man bruger til at ligge sine oplysninger i og have styr på sine rettigheder.

20. ***F/J:*** *Så I har ikke været ude og skifte IT system, I har bibeholdt det I havde?*

    X: Ja, også fordi der var en enorm arv, i forhold til hvad bruger folk egentlig. Vi har dog for nyligt lige implementeret et nyt ERP-system, hvor vi bruger AX, og det har slet ikke været på dagsorden at lave ændringer i det, fordi det har taget sindssygt lang tid bare at få det implementeret, og det kæmper vi stadig med, at nu har vi valgt det, så skal vi også kunne netop stå på mål for Privacy by design bestemmelsen, og netop have styr på at det kun er de relevante personer, der har adgang ind i det system. Så nej, ikke udskiftning - men justeringer i eksisterende IT-systemer.

21. ***F/J:*** *Og hvad med den generelle medarbejders IT, altså deres computere og fysiske papir. Har du været inde over det?*

    X: Øhh, jeg har været inde over det i forhold til retningslinjer om, hvor du gemmer ting. At du ikke gemmer lokalt. Øhm, og det er planen, at der skal være en plan for data på iPhone og mobilen, at det skal være. Men det tror jeg bliver en del af vores IT-sikkerhedspolitik. Vi har faktisk for nyligt indgået en aftale med Atea, om at du skal håndtere vores computere og sådan noget, hvor de skal sørge for rense computer og telefoner, når de skal gå i arv til en ny eller smides ud. Så jo, det en del af det, men ikke noget vi er så langt med endnu. Man kan sige, at vi nok mest har lagt vægt på den organisatoriske inddeling, i kraft af at vi ikke som sådan har investeret i nogle nye IT-systemer. Vi har den der Microsoft pakke med forskellige funktioner, som man kan trække ned over sine IT-systemer, og det er egentlig planen og bruge den, men vi har bare ikke rigtigt kunne få det i værks, før vi har det fulde overblik, for det kræver bare, at hele forarbejdet skal laves først. Men i forhold til politikker og det arbejde, har det klart været den organisatoriske del, vi har lagt vægt på.

22. ***F/J:*** *Hvad så i forhold til når der kommer en medarbejder, om det så er en sur eller glad medarbejder. De er jo blevet meget mere opmærksom på deres rettigheder, og hvad de må og ikke må. Hvis de så kommer og siger, at de vil slettes eller overføres. Det er jo ligeså meget det der ligger i og kunne gå det i hele organisationen. Kan du på nuværende tidspunkt håndtere det?*

X: Altså, for at være helt ærlig, så er det noget, der vil være svært for os i kraft af, at vi ikke har haft faste processer defineret fra start. Så medarbejderdata kan principalt ligge mange forskellige steder, men det er noget af det, vi har forsøgt at rette op på, ved at lave klare processer for hvor data egentlig skal være. Man kan sige, at alle den registreres rettigheder forudsætter, at du kan identificere oplysningerne, hvor de ligger henne. Det er første step. For at kunne slette dem skal du vide, hvor de er og for at kunne give indsigt, jamen der skal du også vide, hvor de er. Så det har været mit overordnet mål i forhold til hvor medarbejderdata må opbevares henne, og så har vi lavet en politik for, hvordan vi vil forhold os, hvis vi får en henvendelse. Og på nuværende tidspunkt vil vi ikke bare kunne trykke på en knap og så får vi det hele ud. Det ved jeg, at Microsoft arbejder på, at man kan inden den 25. maj. Så det er jeg spændt på at se. Vi kan ikke automatisere det, men processen må være, at man må spørge datasubjektet, om hvor deres data er. Hvilke afdelinger har du været i kontakt med, og så må man tage den internt - tage den i afdelingerne. Men det er selvfølgelig ikke en 100 procent sikker fremgangsmåde til at få alt med, så det er en kæmpe udfordring. Men i forhold til det jeg har prøvet at få skabt i forhold til medbestemmelse, så har jeg hørt, at mange medarbejder har sagt, at de i hvert fald ikke vil være skyld i en bøde. Altså en form for stolthed i form af, at de i hvert fald vil gøre deres for, ikke at det er her, bøden kommer. Og det synes jeg egentlig også indikerer det her ejerskab lidt.

23. ***F/J:*** *Men det er så også fordi, du har været god til at lave hele den her awareness omkring GDPR.*

X: Ja, og det kan man så sige, at det der har været mit problem, hvis jeg skal være lidt kritisk, at jeg har kun snakket med enkelte medarbejdere. Men det er ikke muligt at snakke med 3000 mennesker. Så jeg har været nødsaget til at snakke med nogle medarbejder, der har haft en bestemt funktion og så få en af hver af dem til at fortælle, hvad de gør, og så er det ligesom tanken, at de skal sørge for at udbrede budskabet internt i deres afdeling. Og det at det kommer til at tage længere tid, og det bliver langsommere, og folk ved ikke det hele fra starten, men det er så den risiko, vi løber ved at gøre det her.

24. ***F/J:*** *Ja, men man kan sige, at selvom du taler med alle medarbejdere, så vil der også være medarbejdere, som eventuelt kunne glemme nogle procedurer, hvor det også var relevant, og så er det svært.*

X: Ja, jeg tror efterhånden, at de fleste ved, at vi har det her projekt, og det kører, og også hvordan det kører, fordi jeg er også sådan lidt en showstopper rundt omkring, når folk skal til at dele et eller andet, så bliver de nød til at spørge mig, og så på den måde rammer folk ikke ind i mig, fordi jeg har snakket med dem i et interview, men så rammer de ind i mig, fordi de vil gøre et eller andet med persondata, og så får jeg igen mulighed for at fortælle, at det her er en del af et større hele i din egen afdeling, hvor den her person har været med, og de sidder i øjeblikket nu og finder ud af, hvordan vi skal gøre det her fremover. Så jeg kan ikke svare dig nu, men det er faktisk dem, der sidder og arbejder på hvordan, det skal være. Så på den måde tror jeg, det er blevet spredt. Og de allerede har vendt den tanke om at gå til mig, så er man noget et godt stykke vej. Jeg kan i hvert fald mærke det i min

indbakke, at min synlighed er blevet større og større. Folk har så mange forskellige kompetencer, så det er vigtigt, at man ikke taler ned til dem. Det er så sindssygt meget psykologi i det. Jeg har gjort sindssygt meget ud af det, når jeg har talt med folk og anlægge en positiv vinkel i det. Det er en mulighed for at optimere og får smidt de ting ud, vi ikke bruger mere og få effektiviseret de arbejdsprocesser, vi har. Det her projekt har rent faktisk medført, at vi har kunne barbere en masse væk fra medarbejdere. Så sådan nogle ting har haft en stor betydning. Det kan lette folks hverdag, og det er noget, de kan sætte sig ind i. Det kan hjælpe dig med at få mindre travlt, det har været noget, der har hjulpet meget. Man bliver nød til at anerkende, at det kan være svært for en medarbejder at komme ud af sin skal og sin daglige rutine. Så jeg tror på, at det gør meget, at man anerkender det hos medarbejderen og gør opmærksom på, at man godt ved, at det er en svær ting. Så det at man indikerer, at man har stor respekt for det de laver, og at man vil prøve at lave de bedste løsninger for alle. Dermed er der også en større tilbøjelighed til, at de hjælper.

25. ***F/J:*** *Jeg kom til at tænke på, hvordan er uddannelsesniveauet. Er det sådan ca. ens?*

X: Nej, det er meget bredt.

26. ***F/J:*** *For du nogen fornemmelse for, om der er en forskel på forståelsen af GDPR og den uddannelse man har?*

X: I udgangspunktet ja, da der er en tendens til, at folk med en højere uddannelse forstår, at det ikke bare er noget, vi har fundet på, og at det er et EU-krav. Men jeg synes egentlig, hvis man formår at få folk til at forstå betydningen gennem principperne, så kan langt de fleste uanset uddannelsesniveau egentlig forstå, at det er vigtigt, og det er et problem. Det er egentlig ikke fordi, jeg har oplevet, at der har været større opbakning i dele af organisationerne, der har højere uddannelse. Men jeg har ikke som udgangspunkt kunne mærke en forskel i uddannelse og implementeringen af GDPR.

27. ***F/J:*** *Men det tror jeg også er i qua af den måde, du har håndteret dette projekt.*

X: Ja, det er det måske. Det er erkendelsen af, hvad den enkelte medarbejder sidder med. OG gøre det klart, at det ikke er alt, der skal ændres, men nogen ting, og det er kun måske lidt, der skal laves om. Så man fjerner skrammescenariet, for så kan langt de fleste være med.

Bilag 3 – Fortroligt