Copenhagen Business School
Kandidatafhandling 2019
Afleveringsdato: 15. maj 2019

DEN DATAANSVARLIGES TILSYN MED DATABEHANDLERE

En undersøgelse af artikel 28 i GDPR med særligt fokus på inddragelse af en revisor

THE CONTROLLER'S SUPERVISION OF PROCESSORS

A study of article 28 in GDPR with a specific focus on the use of an auditor

Uddannelse: Cand.merc.aud
Fag: Revision

Udarbejdet af:
Henrik Tuyen, 32724
Martin Lusty Bøgelund Sørensen, 92407

Vejleder:
Ole Svenningsen

Antal anslag / sider:
271.763 / 120 sider

CBS

Institut for Regnskab

Executive summary

General Data Protection Regulation (EU) 2016/679 was adopted with the purpose of increasing the protection of the privacy of the individuals in the European Union. The consequences of not complying with GDPR can be severe, as this can result in fines up to 20 million euros or 4% of a company's global revenue. In article 28, it is set that a controller has a duty to supervise their processors. A controller can outsource their processing, but they can never outsource the responsibility of the processing. This thesis investigates the relationship between the controllers and the processors with regards to article 28. Using a qualitative approach 6 interviews has been carried out to examine the relationship between a controller and a processor. To assist the two parties in identifying their roles, a list of statements is presented. In order for a controller to supervise a processor, it is necessary to acknowledge the obligations of the processor as laid out in article 28 (3). The thesis furthermore analyses the obligations of a processor when a data processing agreement has been made. A supervision can be done in many ways, but generally there exists 2 approaches, either a written approach or a physical approach, which will depend on the associated risk. For each method the controller has to decide whether to conduct these themselves, or include an external part, e.g. an independent auditor in the circumstances when the controller doesn't possess the necessary abilities themselves to carry out the actions required, such as tests of controls. To assess the risk of a processing activity, the thesis has laid out criteria to assist the controller. To decide which supervisory methods and actions to be taken, the thesis sets up a matrix, which revolves around the laid-out criteria. In this matrix the controller can map their criteria to determine the supervisory actions based on a low, medium and high risk assessment. A controller must decide whether to include an external part. An external part can be an independent auditor, who can deliver an ISAE 3000 assurance report based on the agreed upon data processing agreement and whether or not the processor has fulfilled their obligations during a specific period. The thesis then continues with examining how a controller should respond to an independent auditor's ISAE 3000 assurance report. During a financial audit the company's external auditor must reflect on the possible effect of not complying with relevant regulation and law, where GDPR and the possible impact of a fine can be of material effect. To help the auditor evaluate the company's GDPR compliance, the thesis has laid out a list of questions that the auditor can ask the auditee. To illustrate all of the thesis' considerations and conclusions, a case is then presented. As GDPR is a relatively new regulation, the thesis concludes with a discussion and reflection of the usability of the presented results.

Indholdsfortegnelse

Oversigt over billeder:

Oversigt over figurer:

Oversigt over tabeller:

1. Indledning

Databeskyttelsesforordningen har været længe undervejs og er bl.a. blevet vedtaget på baggrund af den hastige teknologiske udvikling samt den øgede globalisering og digitalisering, som har skabt nye udfordringer i forbindelse med beskyttelsen af personoplysninger. Dertil er omfanget af indsamling og deling af personoplysninger også steget betydeligt hvilket har givet private selskaber såvel som offentlige myndigheder rig mulighed for at udnytte personoplysninger i et hidtil uset omfang. Heriblandt har personoplysninger fået øget portabilitet i et sådant omfang at data kan flyttes hurtigt, nemt og omkostningsfrit. Denne øgede portabilitet har skabt en forhøjet risiko hos det enkelte individ, da der hermed er flere indgangsvinkler for uvedkommende, samt flere muligheder for fejl end tidligere.

Navn, adresse, telefonnummer, arbejdssted, arbejdsstilling og uddannelse er en liste af eksempler på personoplysninger, men langt fra udtømmende, da personoplysninger er enhver form for information der kan knyttes om en identificeret eller identificerbar fysisk person. Individer afgiver på daglig basis personoplysninger om sig selv i stort omfang, eksempelvis i forbindelse med indkøb på internettet, ved brug af de sociale medier eller igennem arbejde. For den enkelte person gælder det ofte at personen ikke kun afgiver mange forskellige personoplysninger, men også at dette bliver afgivet til en bred vifte af modtagere, herunder virksomheder, styrelser, myndigheder osv. Dette har i stigende grad har medført et øget fokus på behandlingen af personoplysninger. I forbindelse med afgivelse af sine personoplysninger, afgiver man samtidig kontrol over sine oplysninger til organisationer, som ofte benytter sig af leverandører i forbindelse af outsourcing af funktioner eller opgaver.

I denne situation opstår ofte forholdet mellem dataansvarlig og databehandler. Ved outsourcing af behandlingen af personoplysninger er det den dataansvarlige der har det primære ansvar for at behandlingen sker i overensstemmelse med lovgivningen, på trods af den dataansvarlige ikke selv varetager den egentlige behandlingsaktivitet. Det er ikke unormalt at en dataansvarlig benytter sig af flere databehandlere, som igen kan benytte sig af underdatabehandlere, hvilket kan skabe en kompleks struktur for behandlingen af personoplysninger. Dette kan skabe indbyrdes afhængigheder, og der kan forekomme høj grad af udveksling af personoplysninger. Det skal fastslås at ansvaret altid er pålagt den dataansvarlige. Dette skaber dermed et behov og stiller krav til den dataansvarlige om at tilegne sig sikkerhed for at databehandlere foretager behandling af personoplysninger i overensstemmelse med

gældende lovgivning og de indgåede databehandleraftaler. Dataansvarlige skal føre kontrol med databehandlere og kan udføre dette på mange måder, heriblandt fysisk besøg hos databehandler, spørgeskemaer eller en revisorerklæring fra en uafhængig revisor som udtaler sig om et givent emne m.fl.

Behandling af personoplysninger har fundet sted længe, men det øgede fokus er opstået efter Databeskyttelsesforordningen, også kendt som GDPR, fra Den Europæiske Union, der har haft virkning fra den 25. maj 2018. Mange af forordningens begreber, principper og regler er allerede kendt fra Dansk lovgivning, men forordningen indeholder en række nyskabelser, som har til formål at styrke beskyttelsen af personoplysninger. Behandlingen af personoplysninger er en naturlig del af mange organisationers daglige drift, hvortil der fra lovgivers side er øget fokus herpå. Det enkelte individ afgiver som tidligere nævnt personoplysninger i mange sammenhænge, og kan ikke altid vide sig sikker på hvordan personoplysninger bliver brugt og hvor disse ender, hvilket kan skabe usikkerhed for det enkeltes individs rettigheder og frihedsrettigheder.

En af forordningens nyskabelser er en formalisering af forholdet mellem en dataansvarlig og en databehandler og tilhørende databehandleraftale. Forordningen stiller krav om at der kun må benyttes databehandlere, som kan stille de fornødne garantier, hvilket naturligvis stiller krav til den dataansvarliges dokumentation og proces for udvælgelse og løbende kontrol af databehandlere. Det er dette forhold og hvordan den dataansvarlige kan sikre sig den fornødne garanti som afhandlingen vil have sit fokus på og som henleder til problemformuleringen.

1.1 Problemformulering

Som allerede nævnt ligger ansvaret for behandling af personoplysninger altid hos den dataansvarlige, også ved brug af databehandlere. Organisationer som er omfattet GDPR, skal tilpasse sig den nye lovgivning. Hertil er GDPR stadig nyt ved udarbejdelse af afhandlingen, hvorfor der på området ikke er særlig erfaring i forhold til organisationer og deres dokumentering af efterlevelse af lovgivningen. Problemformuleringen tager afsæt i forholdet mellem dataansvarlig og databehandler og hvordan dataansvarlige benytter databehandlere, som kan stille de fornødne garantier for at behandling af personoplysninger opfylder kravene i forordningen og derved sikre beskyttelse af den registreredes rettigheder og frihedsrettigheder. Dette medfører at den dataansvarlige er forpligtet til at føre tilsyn med sine databehandlere, hvilket bl.a. kan udføres med hjælp fra en revisorerklæring og efterfølgende gennemgang

af denne. Undersøgelsesfeltet er som følge af det beskrevne forhold mellem en dataansvarlig og en databehandler, hvilket giver anledning til den udarbejdede problemformulering som afhandlingen skal besvares ud fra. Problemformulering er som følgende:

"Hvilke overvejelser indgår når en dataansvarlig outsourcer behandling af personoplysninger til en databehandler i henhold til GDPR og hvordan opnår en dataansvarlig sikkerhed for at en databehandler efterlever den indgåede databehandleraftale samt hvordan kan en revisor evt. inddrages i denne proces og hvordan bør den dataansvarliges eksterne revisor forholde sig til GDPR under en finansiel revision?"

For at understøtte problemformuleringen er der udarbejdet følgende underspørgsmål:

Underspørgsmål 1

Hvilke overvejelser har en dataansvarlig i forbindelse med outsourcing, herunder GDPR og databehandleraftaler?

Til at besvare problemformuleringen, er det relevant at undersøge hvilke overvejelser en organisation gør sig når denne vælger at outsource en aktivitet. Hertil vil GDPR og databehandleraftalerelaterede overvejelser blive undersøgt. Underspørgsmålet vil forsøge at skabe at grundlag for, hvornår en databehandlerkonstruktion opstår, hvilket er fundamentet for næste underspørgsmål. Dette underspørgsmål vil blive gennemgået i kapitel 7.

Underspørgsmål 2

Hvordan efterlever en databehandler den indgåede databehandleraftale?

For at besvare problemformuleringen er det nødvendigt at fastslå hvilke forpligtelser en databehandler har i henhold til en indgået databehandleraftale. Der bliver redegjort for hvilke forpligtelser en databehandler har i henhold til Datatilsynets standarddatabehandleraftale og hvilke foranstaltninger en databehandler skal iværksætte for at efterleve denne. Resultatet af dette spørgsmål skal bruges til næste underspørgsmål, da det er nødvendigt først at fastlægge hvad en databehandler skal efterleve, førend der kan konkluderes på hvordan en dataansvarlig sikrer at databehandleren efterlever dette. Dette underspørgsmål vil blive gennemgået i kapitel 8.

Underspørgsmål 3

Hvordan skal en dataansvarlig sikre sig at dennes databehandler efterlever den indgåede databehandleraftale?

Det er vigtigt at opnå en forståelse for hvilke krav en dataansvarlig, igennem en databehandleraftale, stiller til en databehandler. Det skal undersøges hvordan en dataansvarlig sikrer sig at databehandlere overholder de forpligtelser der er aftalt igennem et tilsyn, da den dataansvarlige er pålagt ansvaret for behandlingen af

personoplysninger. Analysen skal undersøge risici ved behandling af personoplysninger for de registrerede, og hvad man hertil bør gøre ved at benyttelse af databehandlere. Som led i udførelsen af et tilsyn vil der undersøges, hvornår en ekstern part, eksempelvis i form af en revisor, kan inddrages i denne proces. Da der i dette spørgsmål undersøges hvornår en revisor bør inddrages, vil der i næste underspørgsmål redegøres og vurderes på hvordan en dataansvarlig konkret skal forholde sig til revisors produkt. Dette underspørgsmål vil blive gennemgået i kapitel 9.

Underspørgsmål 4

Hvordan bør en ISAE 3000 erklæring om behandling af personoplysninger benyttes af en dataansvarlig?

I det forrige underspørgsmål bliver der redegjort for, hvornår en dataansvarlig kan benytte sig af revisors produkt. I henhold til GDPR vil dette produkt være en ISAE 3000 erklæring, hvorfor der i dette underspørgsmål vil undersøges og vurderes, hvordan en dataansvarlig skal forholde sig til en ISAE 3000 erklæring med udgangspunkt i FSR – Danske Revisorers erklæringsskabelon fra februar 2019, som tager udgangspunkt i Datatilsynets standarddatabehandleraftale. For at en revisors produkt kan benyttes til at skabe værdi for en dataansvarlig og som led i dennes tilsynsforpligtelse, er det nødvendigt at forstå, hvordan man skal forholde til en sådan erklæring. Dette underspørgsmål vil blive gennemgået i kapitel 10.

Underspørgsmål 5

Hvilke overvejelser til GDPR bør en revisor have under en finansiel revision?

I de forrige underspørgsmål bliver der undersøgt forholdet mellem en databehandler og en dataansvarlig, samt hvilke forpligtelser en databehandler er underlagt igennem en databehandleraftale. Herudover er der undersøgt hvordan en dataansvarlig skal sikre sig at denne aftale efterleves og hvordan en revisor kan inddrages i form af en ISAE 3000 erklæring. Den viden der er skabt igennem de spørgsmål, vil benyttes til at sætte GDPR spørgsmålet i perspektiv til den eksterne revisor når denne udfører en finansiel revision. Til underspørgsmålet vil der derfor blive udarbejdet en tjekliste, som den eksterne revisor kan benytte ved en finansiel revision, til at få en overbevisning om, hvorvidt øvrig regulering i form af GDPR bliver overholdt. Dette underspørgsmål vil blive gennemgået i kapitel 11.

I ovenstående er der opstillet underspørgsmål som har til formål at understøtte en besvarelse til problemformuleringen og en tilhørende konklusion. For at besvare problemformuleringen inddrages gældende lovgivning i form af relevante artikler i GDPR og revisionsteori. Udover de fem underspørgsmål vil der også opstilles en fiktiv case, som skal prøve at omfavne alle de overvejelser og konklusioner der udledes af underspørgsmålene. Casen vil have fokus på en situation mellem en dataansvarlig og databehandler, hvortil der vil ses på hvilke overvejelser en dataansvarlig gør sig både før, under og efter en

aftale indgås, hvori behandling af personoplysninger indgår. Da GDPR og revision er meget brede emner, er det nødvendigt at der foretages en afgrænsning af hvad der specifikt skal undersøges i afhandlingen.

1.2 Afgrænsning

Der er i afhandlingen foretaget en række afgrænsninger for at sikre at afhandlingen omhandler den egentlige problemstilling. Afhandlingen beskæftiger sig med love og regler i GDPR, som trådte i kraft d. 24. maj 2016, men fandt først anvendelse d. 25. maj 2018. Dette medfører at afhandlingen vil have en tidsmæssig afgrænsning, som tager udgangspunkt i hvordan regler forstås og anvendes i praksis efter d. 25. maj 2018. Grundet denne tidsmæssige afgræsning vil der ikke blive undersøgt hvordan reglerne inden for beskyttelse af personoplysninger blev fortolket og anvendt før d. 25. maj 2018. De tidligere regler var hovedsageligt reguleret i direktiv 95/46/EF og Lov om behandling af personoplysninger. Herudover skal det fastslås at GDPR er i fokus, hvorfor andre love og reguleringer ikke vil blive analyseret.

Inden for GDPR er der mange emner og problemstillinger der vil kunne undersøges. I afhandlingen afgrænses der til at blive undersøgt databehandlerkonstruktioner og en dataansvarliges tilsynsforpligtelse. Andre emner inden for GDPR, som de registreredes rettigheder og behandlingshjemler, vil dermed ikke blive belyst i særlige omfang. Det primære fokus i afhandlingen er på forholdet mellem en dataansvarlig og en databehandler, og ikke mellem en dataansvarlig og de registrerede. En databehandler handler efter instruks, hvorfor det antages at en dataansvarlig har hjemmel til at behandle de registreredes personoplysninger. Der afgrænses også for situationer når der ved outsourcing opstår andet end databehandlerkonstruktioner, som forholdet mellem fælles dataansvarlige. Yderligere kan der i databehandlerkonstruktioner være overførsler til tredjelande eller internationale organisationer, hvortil de overførselsgrundlag der findes, ikke bliver analyseret og vurderet, men kun benævnt. Sanktioner ved manglende overholdelse af GDPR vil ikke blive vurderet, udover at bødestørrelserne kan blive brugt som argument for hvorfor det er essentielt at overholde GDPR.

I afhandlingen bliver det undersøgt hvornår en revisor kan inddrages i en dataansvarliges tilsynsforpligtelse. Ved udførslen af revisionshandlinger bliver revisor gjort til dataansvarlig, hvortil der i afhandlingen ikke undersøges hvilke overvejelser og konsekvenser dette skaber for revisor under udførelsen af hans arbejde. Revisor agerer som offentlighedens tillidsrepræsentant, hvorfor der stilles krav til

uafhængighed, kvalitetskontrol, uddannelse, efteruddannelse, autorisation m.m. Kravet om uafhængighed vil blive belyst i afhandlingen. For de øvrige krav antages det at revisor er underlagt disse, uden at de benævnes yderligere.

GDPR er direkte gældende for alle EU-medlemslandende, men muliggør at medlemslandende kan implementere forskellige optioner i national lov. Afhandlingens gennemgang af GDPR og tilhørende revisorerklæring vil tage udgangspunkt i et dansk perspektiv, hvortil der fokuseres på forholdet for en dataansvarlig og en databehandler i Danmark. Dette betyder at der ikke vil blive inddraget GDPR lignende love og reguleringer fra andre lande eller områder. Dels fordi alle respondenterne sidder i danske organisationer og dels fordi der vil inddrages empiri fra Datatilsynet, den danske tilsynsmyndighed, og FSR – Danske Revisorer. Dette betyder endvidere at der ikke vil blive analyseret på de hjemmelsmuligheder der findes i forbindelse med overførsel til tredjelande og internationale organisationer.

Yderligere vil der i afhandlingen blive inddraget revisors arbejde i form af en ISAE 3000 erklæring, herunder FSR – Danske Revisorers skabelon til en ISAE 3000 om behandling af personoplysninger, hvorfor andre erklæringer som ISAE 3402 og SOC 1, 2 og 3 ikke vil blive analyseret. I afhandlingen analyseres hvordan og hvornår en ISAE 3000 erklæring kan benyttes af de dataansvarlige. Der afgrænses hertil for beskrivelser og vurdering af tilstrækkeligheden af de revisionshandlinger som indgår heri. Det antages derfor at de revisionshandlinger FSR – Danske Revisorers skabelon lægger op til er tilstrækkelige.

I ovenstående er gennemgået de overvejelser og afgrænsninger som gælder for hele afhandlingen, hertil må det fastlås at der løbende i afhandlingen også vil forekomme afgrænsninger når dette findes relevant.

1.3 Afhandlingens struktur og opbygning

Følgende afsnit vil kort redegøre for afhandlingens struktur og opbygning, og vil samtidig fungere som en læsevejledning. Overordnet er afhandlingen delt op i 15 kapitler som er opdelt i 5 faser. De fem faser er følgende: Introduktion og metode, teoretisk ramme, fra teori til empiri, tilsynsforpligtelsen og anvendelse i den eksterne revision og afsluttende del.

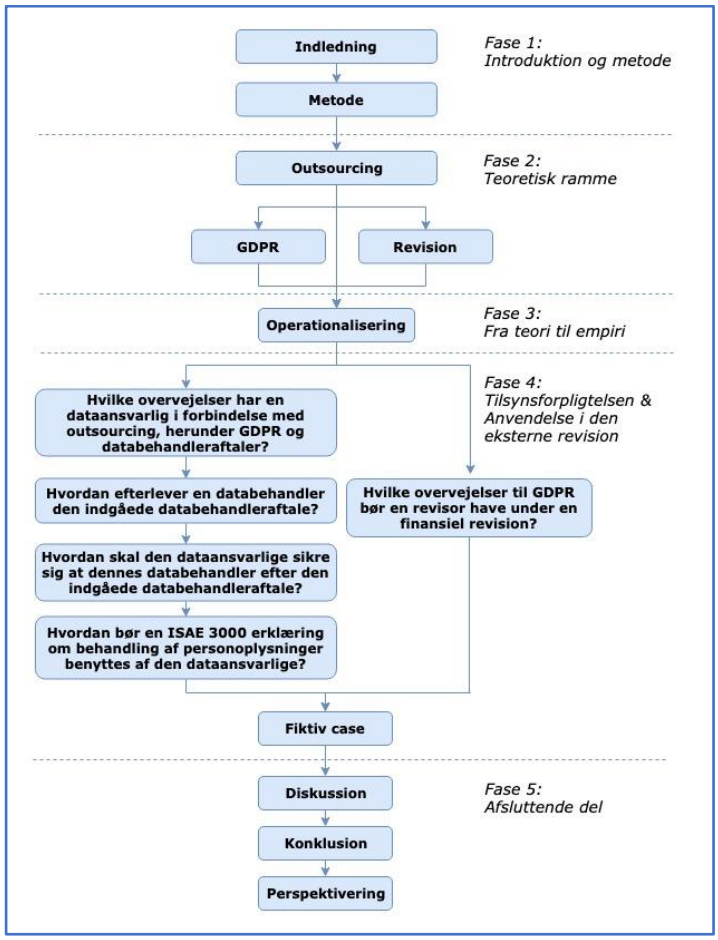
1. fase, introduktion og metode: Denne fase består af kapitel 1-2 som er indledning og metode. I indledningen fremgår problemstillingen og den tilhørende problemformulering. Derudover fremgår understøttende underspørgsmål samt en afgrænsning af emner og problemstillinger, som ikke vil blive belyst i afhandlingen. I metoden fastlægges den videnskabelige fremgangsmåde og de antagelser forfatterne har gjort sig om den måde data indsamles og fortolkes. Hertil bliver der gennemgået hvilke dataindsamlingsmetoder der vil blive benyttet og præsentation af de respondenter der indgår i afhandlingen.

2. fase, teoretisk ramme: Denne fase består af kapitel 3-5 som er gennemgang af den teori som skal danne fundamentet for analysen. I fasen indgår teori om outsourcing, GDPR og revision. Der bliver først redegjort for outsourcing, da dette skaber anledning til overvejelser inden for både GDPR og revision. GDPR og revision skal ses som to parallelle kapitler, da disse to kapitler kan læses uafhængigt af hinanden og ikke bygger videre på den indbyrdes teori. Det skal gøres klart at dele af den teori der fremlægges, er forudsætninger som læseren skal bære med over til den videre analyse, selvom nogle af begreberne ikke eksplicit vil fremgå i analysen.

3. fase, fra teori til empiri: Denne fase består af kapitel 6, som er et kapitel hvor der redegøres for hvordan den beskrevne teori operationaliseres. I kapitlet fremlægges interviewguides og kildekritik af de enkelte respondenter, som er med til at skabe fundamentet for analysen.

4. fase, tilsynsforpligtelsen & anvendelse i den eksterne revision: Denne fase består af kapitlerne 7-12 som er en analyse af de fremlagte underspørgsmål, hvortil de samlede delkonklusionerne har til formål at svare på problemformuleringen. Kapitel 7-10 er de fire første underspørgsmål, hvortil det gøres klart at disse er opbygget som afhængige kapitler, hvorfor de konklusioner der drages i et underspørgsmål tages videre til næste underspørgsmål. Kapitel 11 kan derimod anskues uafhængigt fra de andre, da kapitlet fungerer som en anden vinkel på GDPR og hvordan den eksterne revisor kan forholde sig hertil. Denne fase afsluttes med en fiktiv case i kapitel 12, som vil benytte de fremlagte konklusioner med en praktisk tilgang. Formålet med casen er at vise hvordan et virkelighedseksempel med tilsyn, risikovurdering, brug af revisor og erklæringer kan se ud.

5. fase, afsluttende del: Denne fase består af kapitlerne 13-15 som er diskussion, konklusion og perspektivering. I diskussionen bliver der diskuteret emner som kan være af betydning for de fremlagte delkonklusioner. I konklusionen bliver alle delkonklusionerne sammenlagt, hvortil den fremlagte problemformulering vil blive besvaret. Afslutningsvis i afhandlingen er der en perspektivering som redegør for anvendeligheden af de fremlagte resultater. Disse 5 faser kan illustreres i følgende figur:



Figur 1: Opgavestruktur.
Kilde: Egen tilvirkning

1.4 Opsummering af indledning

Der er indledningsvis i kapitlet blevet fremlagt motivation for afhandlingen i form af kort baggrund for GDPR. Der er fremlagt en problemformulering med tilhørende fem underspørgsmål, som skal danne grundlag for det videre arbejde. Herudover er der foretaget en afgrænsning af beslægtede emner og områder, som ikke vil blive analyseret i afhandlingen. Afslutningsvis er der fremlagt en læsevejledning i form af gennemgang af struktur og opbygning af afhandlingen. Dette leder hen til metoden, hvor der vil blive gennemgået de videnskabsteoretiske og metodiske overvejelser som forfatterene har gjort sig.

2. Metode

Grundlæggende for afhandlingen, er det vigtigt at fastlægge de metodiske overvejelser, der indgår i hele processen, som danner grundlag for det endelige output. Metoden er en beskrivelse af det redskab, som anvendes til at besvare problemformuleringen. Dette omfatter i hovedtræk videnskabsteori og undersøgelsesdesign og er relevant at fastlægge og gøre sig overvejelser til, da det beskriver måden hvorpå der interageres med den kontekst som bliver undersøgt. Metoden er den måde der fremskaffes og analyseres empiri på, og dermed lægger metoden fundamentet for afhandlingens konklusion. I dette kapitel vil der blive redegjort for hvilket paradigme afhandlingen tager afsæt i og dernæst et undersøgelsesdesign som følge heraf. For at fastlægge et paradigme vil det være nødvendigt at gøre sig bevidst om hvilken ontologi, epistemologi og metodologi som bliver anvendt i afhandlingen.

2.1 Videnskabsteori

Skabelse af ny viden styres af paradigmer, da paradigmer bl.a. fastlægger udgangspunktet for hvordan data skal analyseres og hvordan menneskers synpunkter skal fortolkes. Guba definerer et paradigme som *"Et basalt sæt af værdier som styrer vores handlinger – både hverdagshandlinger og handlinger forbundet med disciplinerede undersøgelser"*[1]. Forklaret på en anden måde er et paradigme et spørgsmål om hvordan virkeligheden er og bliver opfattet, samt hvordan viden skabes. Der findes mange paradigmer, og da et paradigme er en beskrivelse af hvordan en person opfatter ting, er der principielt set ligeså mange paradigmer, som der er forskellige menneskers opfattelser af virkeligheden. Når et paradigme benyttes, har det konsekvenser for den måde hvorpå viden skabes. I henhold til Voxted er de 3 grundlæggende konsekvenser: en ontologisk, epistemologisk og metodologisk konsekvens. Disse er skematiseret i følgende:

	Definition	Konsekvens
Ontologi	Læren om det værendes væsen	Fremtvinger en bestemt virkelighedsopfattelse, som har konsekvenser for, hvordan man arbejder epistemologisk og metodologisk
Epistemologi	Erkendelsesteoretisk og filosofisk studie af erkendelse og viden	Fremtvinger bestemte antagelser om, hvordan man opnår viden om det værende, som har konsekvenser for, hvordan man arbejder metodologisk
Metodologi	Læren om videnskabelige metoder	Fremtvinger bestemte antagelser om fremgangsmåder ved videnskabelse, som har konsekvenser for forskerens håndværk som analytiker.

Tabel 1: Paradigmers konsekvenser for videnskabelse.
Kilde: Voxted, S. (2006), s. 54

[1] Voxted, S. (2006), s. 53

Som det kan aflæses af Tabel 1, er ontologien en af de tre konsekvenser for et paradigme og er læren om det værendes væsen. Ontologien er dermed læren om hvad det man undersøger er, samt den virkelighedsopfattelse og forståelse man har af verden. Hertil mener Voxted at ontologien og den måde mennesker opfatter virkeligheden på kan ændre sig over tid, som følge af eksempelvis en oplevelse eller hændelse[2].

Denne afhandling omhandler GDPR og den dataansvarliges tilsynsforpligtelse over for en databehandler, samt hvordan revisor kan inddrages i denne proces. Da afhandlingen dermed omhandler lovgivning, vil dette pege i retning af en realistisk ontologi, da der normalt vil være en sandhed i lovgivningen. Det må dog vurderes at fordi at afhandlingen inddrager flere respondenter og deres fortolkninger af artikel 28 i GDPR, vil dette pege hen imod en relativistisk ontologi. Grunden til at den relativistiske ontologi er aktuel, er fordi virkeligheden vil afhænge direkte af den måde hvorpå loven bliver fortolket og dens øvrige kontekst. GDPR stiller sjældent absolutte krav, hvorfor den efterlader meget rum til fortolkning, eksempelvis nævnes "fornødne garantier" i artikel 28. Det er subjektivt hvordan "fornødne garantier" skal fortolkes, hvorfor ordene kun eksisterer igennem deres fortolkning. Dette fastslås endvidere i kraft af at GDPR er nyligt implementeret i EU-retten, hvorfor den i høj grad bygger på fortolkninger frem for sædvane og retspraksis. Dette medfører at der ikke er en eksisterende sandhed omkring fænomenet. De involverede parters forskellige opfattelser af lovgivningen betyder, at afhandlingen hovedsageligt vil bygge på en relativistisk ontologi. I henhold til Voxted[3] er ontologien det dybest liggende niveau i paradigmet, hvorfor ontologien vil påvirke de epistemologiske og metodologiske konsekvenser.

Ifølge Voxted omhandler de epistemologiske konsekvenser hvordan man opnår viden omkring et fænomen, og er derfor afgørende for hvordan man kan og skal tilrettelægge sine undersøgelser og studier. Afhandlingen vil tage afsæt i en subjektiv epistemologi, fordi skabelse af ny viden og vurderingen og udformning af en dataansvarliges tilsynsforpligtelse i høj grad baseres på fortolkninger igennem interviews. Igennem afhandlingen vil der analyseres den dataansvarliges tilsynsforpligtelse ved fortolkninger, hvorfor dette falder inden for den subjektive epistemologi. Denne epistemologi er ikke kun omkring de personer der bliver interviewet, men i ligeså høj grad vedrørende de fortolkningerne, som forfatterne selv kommer frem til igennem interviews og interaktionsfeltet mellem det der bliver undersøgt og forfatterne. Både ontologien og epistemologien har betydning for den metodologi som bliver fastlagt.

[2] Voxted, S. 2006, s. 54
[3] Voxted, 2006, s. 55

Metodologien er ifølge Voxted den fremgangsmåde hvorpå der skabes viden. Det er måden og de værktøjer der anvendes til undersøgelsen. Da den ontologiske konsekvens til denne afhandling er fastlagt til relativistisk og den epistemologiske konsekvens er subjektiv, vil dette ifølge Guba [4] medføre at den metodologiske konsekvens vil være en hermeneutisk tilgang. I den hermeneutiske tilgang vil måden og de værktøjer der benyttes til undersøgelsen være fortolkninger af tilsynsforpligtelsen efter GDPR artikel 28, hvortil der vil benyttes en kvalitativ analysestrategi igennem interviews og respondenternes konstruktion og fortolkning af virkeligheden. Dette vil herefter blive omdannet til tekst, hvortil konstruktionerne fortolkes[5]. Når alle de førnævnte konsekvenser undersøges samlet, medfører dette at viden i denne afhandling vil blive skabt i det konstruktivistiske paradigme. Dette er grundet at virkeligheden og dannelse af viden i denne afhandling vil foregå igennem fortolkninger og individers holdninger, hvilket medfører en konstrueret virkelighed. Det konstruktivistiske paradigme ses endvidere via afhandlingens interviews, hvortil det er forskelligt hvordan respondenterne forholder sig til og fortolker tilsynsforpligtelsen i GDPR. Som det er redegjort for tidligere vil den viden der bliver skabt i afhandlingen, være påvirket af forfatterne, hvorfor interaktionen mellem netop forfatterne, respondenterne og undersøgelsen kan medføre at andre som benytter den samme empiri vil kunne komme frem til andre konklusioner om fænomenet og tilsynsforpligtelsen. Det gøres derfor klart, at afhandlingen skrives med udgangspunkt i subjektive holdninger og værdier, som er synliggjort igennem de forskellige respondenters vurdering af tilsynsforpligtelsen.

Afhandlingen foretages med udgangspunkt i interviews og data hertil vil dette være den induktive metode. Igennem afhandlingen vil der med udgangspunkt i den indsamlede empiri forsøges at drage konklusioner på hvordan en dataansvarlig skal forholde sig til sin tilsynsforpligtelse. Dette medfører at der ud fra den indsamlede empiri vil blive forsøgt at skabe ny viden om fænomenet. Ved den induktive metode forsøges der at blive skabt ny viden på baggrund af den kvalitative data[6]. Dette står i kontrast til den deduktive metode, hvor der anvendes eksisterende teorier til at teste hypoteser[7]. Med paradigmet og tilhørende konsekvenser fastlagt, er det relevant at gøre sig overvejelser omkring afhandlingens undersøgelsesdesign, som der bliver redegjort for i det kommende afsnit.

[4] Guba, 1990, s. 27
[5] Guba, 1990, s. 25-27
[6] Andersen, 2014, s. 266
[7] Andersen, 2014, s. 265

2.2 Undersøgelsesdesign

Undersøgelsesdesignet udgør den kombination af fremgangsmåde der benyttes ved indsamling, analyse og tolkning af data[8]. Ved at fastlægge sit undersøgelsesdesign inden man går i gang med analysen, skaber man rammerne for afhandlingens udformning. I undersøgelsesdesignet bliver det fastlagt hvordan data skal indsamles, hvem og hvad der skal indsamles data om, og hvordan denne data skal analyseres og fortolkes. Data skal først og fremmest indsamles og dernæst analyseres således at der kan konkluderes på den udarbejdede problemformulering.

Tilgangen til dataindsamlingen i afhandlingen vil primært være gennem en kvalitativ indsamlingsteknik. De kvalitative indsamlingsteknikker omfatter typisk fokusgrupper, åbne- eller semistrukturerede interviews. Problemformuleringen har fokus på den dataansvarliges kontrol af en databehandler, hvorpå forskellige dataansvarlige kontrollerer på forskellige måder og med forskellige virkemidler. Det er oplagt at kvalitative dataindsamlingsteknikker benyttes, for at skabe mulighed for at få en større indsigt i databehandlere og dataansvarliges overvejelser, end hvis der kun blev benyttet kvantitative data. GDPR stiller ikke krav til hvor tit eller hvordan databehandlere skal kontrolleres, men at der kun må benyttes de databehandlere, som kan stille de fornødne garantier. Ved at der ikke er absolutte begreber i GDPR betyder dette, at det er op til de enkelte dataansvarlige selv at vurdere, hvornår og hvordan de skal kontrollere deres databehandlere og dermed hvornår et tilsyn er tilstrækkeligt. Der er ikke meget historik i form af påbud fra Datatilsynet, hvorfor der heller ikke her er mulighed for at søge særlig meget inspiration til tilsynsopgaven. Dette betyder at vurderingen af kontrol af databehandlere ender i en subjektiv vurdering hos den dataansvarlige, hvorfor den kvalitative fremgangsmetode vurderes som være hensigtsmæssig, hvortil dataindsamlingsteknikken for den primære data vil være i form af interviews.

Det vurderes at semistruktuerede interviews vil være det oplagte virkemiddel, for at skabe mulighed for respondenterne til at komme bredt rundt omkring de adspurgte spørgsmål, uden at være låst i ja/nej spørgsmål. Det er vigtigt at fastslå hvem der skal interviewes og hvilke variabler der skal undersøges. Ved variabler menes hvilke egenskaber, der skal undersøges på undersøgelsesenhederne. Variablerne i afhandlingen vil være hvordan der føres tilsyn med databehandlere. Udover data der indsamles ved semistrukturerede interviews, vil der også blive anvendt sekundære data i form af GDPR, Datatilsynets

[8] Andersen, 2014, kapitel 5

standarddatabehandleraftale og FSR - Danske Revisorers skabelon til en ISAE 3000 erklæring der vedrører behandling af personoplysninger og andet som findes relevant for afhandlingens undersøgelse. Udover at fastlægge hvem der skal interviewes, er det relevant at fastlægge hvilken tidsfaktor afhandlingen vil undersøge. Ved tidsfaktor menes det perspektiv der undersøges, hvortil dette kan være statisk og dynamisk. Ved statisk er der tale om et øjebliksbillede og en situation på et enkelt tidspunkt, hvorimod der ved en dynamisk tidsfaktor ses på en længere periode, hvortil der har været en ændring af en form og der derefter ses på situationen før og efter denne ændring. I afhandlingen vil tidsperspektivet være statisk, da der undersøges hvordan tilsyn med databehandlere udføres i dag . Hvis denne afhandling skulle have være dynamisk, skulle der være foretaget dataindsamling og analyser både før og efter GDPR trådte i kraft.

I fastlæggelsen af undersøgelsesenhederne er det vigtigt at være kritisk overfor respondenterne, og at disse ikke repræsenterer alle. Tilsynsvurderingen er af subjektiv karakter, hvorfor det faktum at en dataansvarlig gør det på en given måde ikke er ensbetydende med at andre dataansvarlige gør det på samme måde. Dette gælder også for revisorer og databehandlere, som kan have forskellige definitioner af hvordan en erklæring fungerer og hvad et tilsyn omfatter. På trods af dette faktum, vurderes det stadig at det fremadrettede arbejde i afhandlingen vil være relevant, fordi afhandlingen vil prøve at skabe en forståelse af hvordan et tilsyn kan udføres og hvordan en revisor kan inddrages i denne proces. Dermed vil der, på trods af den lille empiri base, stadig være brugbare observationer og konklusioner som kan benyttes af andre dataansvarlige, databehandlere og revisorer som står i en lignende situation, hvor de skal vurdere hvordan de skal udføre et tilsyn og hvilke virkemidler de skal inddrage i processen. Respondenterne som indgår i afhandlingen er kort beskrevet nedenfor i anonymiseret form. Der vil senere i afhandlingen under kapitlet operationalisering blive gennemgået hvordan data fra respondenterne skal bearbejdes. Kildekritik af de enkelte respondenter vil indgå for at vurdere, hvad der skal være fokus på når deres svar skal inddrages i analysen. Forskellige organisationer og personer har forskellige mål og syn, hvorfor der kan forekomme bias i deres svar. Respondenterne som inddrages er følgende:

- Respondent A, advokat som bistår med rådgivning inden for GDPR og databehandleraftaler.
- Respondent B, dataansvarlig, DPO[9] og jurist ved en uddannelsesinstitution.

[9] Data Protection Officer (DPO) eller Databeskyttelsesrådgiver er beskrevet i GDPR artikel 37-39.

- Respondent C, databehandler, DPO og jurist i en organisation med varetagelse af bl.a. HR- og lønadministration.
- Respondent D, statsautoriseret revisor med fokus på rådgivning og afgivelse af erklæringer inden for informationssikkerhed og GDPR.
- Respondent E, statsautoriseret revisor med fokus på rådgivning og afgivelse af erklæringer inden for informationssikkerhed og GDPR.
- Respondent F, dataansvarlig, DPO og jurist i en finansiel virksomhed.

Det er i undersøgelsesdesignet fastlagt at dataindsamlingen primært baseres på semistrukturerede interviews. Det er essentielt at tilpasse interviewspørgsmålene til afhandlingens teoretiske ramme og de enkelte respondenter, således at disse forstår spørgsmålene og deres svar herefter kan anvendes i analysen. Det er derfor vigtigt at have operationalisering i fokus som bliver beskrevet senere i afhandlingen.

2.3 Opsummering af metode

Det er i afsnittet fastlagt at afhandlingen udarbejdes inden for rammerne af det konstruktivistiske paradigme. Hertil vil den ontologiske konsekvens være relativistisk, den epistemologiske konsekvens være subjektiv og den metodologiske konsekvens være hermeneutisk. Disse konsekvenser og tilhørende paradigme anses som aktuel, da der i afhandlingens undersøgelsesområde indgår høj grad af vurdering og kan variere fra person til person og deres opfattelse af verden. Dertil er undersøgelsesdesignet fastlagt, hvor det er vurderet at grundet en subjektiv tilgang igennem paradigmet, vil det også være nødvendigt at lade denne subjektivitet komme til live. Dette vil primært ske igennem semistrukturerede interviews, hvortil respondenterne har fri mulighed for at snakke bredt til de stillede spørgsmål. Det er i undersøgelsesdesignet bestemt at der skal anvendes semistrukturerede interviews, hvorfor det er vigtigt at tilpasse de stillede spørgsmål til afhandlingen teoretiske ramme.

Der er i dette kapitel redegjort for metodiske overvejelser som indgår i hele afhandlingens proces. Der vil i de næstkommende kapitler være en gennemgang af afhandlingens teoretiske ramme som har relevans til undersøgelsesområdet, hertil inddrages primært GDPR og revisionsteori samt forståelse for outsourcing. Forståelsen af den teoretiske ramme er relevant inden operationaliseringsfasen går i gang, da det skaber grundlag for dataindsamlingen.

3. Outsourcing

Afhandlingens undersøgelsesområde tager udgangspunkt i GDPR og forholdet mellem en dataansvarlig og databehandler. Dette kapitel handler om outsourcing da der selvsagt er tale om outsourcing når der benyttes en databehandler. Når en organisation outsourcer, betyder det at organisationen lader eksterne leverandører stå for aktiviteter, som organisationen selv tidligere har stået for. Der findes mange grunde til at outsource sine aktiviteter til eksterne leverandører, eksempelvis bliver aktiviteter ofte outsourcet pga. at organisationen kan reducere sine omkostninger.

Organisationer bliver oprettet med et formål om at løse en eller anden opgave eller udfylde en funktion[10]. Det er derfor relevant for organisationerne at overveje hvilke opgaver organisationen skal koncentrere sig om, hvad der ønskes at opnås engang i fremtiden, og hvordan man skal opnå det man ønsker. Organisationer opsætter nogle mål og har nogle kerneaktiviteter for at kunne opnå disse mål. Det er typisk ikke organisationens kerneaktiviteter der outsources, men derimod de sekundære aktiviteter. Der er en formodning om at en leverandør hvis kernekompetencer er netop inden for de outsourcede aktiviteter kan gøre dette stykke arbejde både billigere og bedre, således at organisationen kan fokusere på egne kerneaktiviteter. Disse nævnte forhold kan anses for at være fordele ved outsourcing. Eksempler på aktiviteter som typisk bliver outsourcet er støttefunktioner og -aktiviteter som finansbogholderi, rengøring, IT-drift, lønadministration og HR m.m. På trods af disse fordele der kan være forbundet med outsourcing, er der ulemper og udfordringer man skal have i overvejelserne når man vælger at outsource. Der kan bl.a. opstå udfordringer i aftaleindgåelsen, da der kan være mange forhold man skal tage stilling til herunder regulering, betingelser og retningslinjer, hvilket alt sammen tager tid at diskutere og gør det svært at komme frem til noget konkret. Derudover opstår der et afhængighedsforhold til leverandøren, hvortil manglende kommunikation mellem organisationen og leverandøren kan blive en udfordring. Ydermere skal man være opmærksom på at man ved outsourcing samtidig afgiver kontrol over en aktivitet idet der er en leverandør som overtager aktiviteten. Her skal man særligt være opmærksom på om sikkerheden er i orden, især hvis der arbejdes med fortrolige informationer.

Udfordringerne kan henledes til afhandlingens undersøgelsesområde, i det man som dataansvarlig skal være opmærksom på at man i anvendelsen af databehandlere afgiver kontrol af aktiviteter med behandling af personoplysninger som kan medføre store konsekvenser hvis ikke GDPR overholdes.

[10] Jacobsen & Thorsvik, 2014, s. 32-33

4. General Data Protection Regulation (GDPR)

GDPR, Databeskyttelsesforordningen også kendt som Persondataforordningen i daglig tale, er en forordning fra Den Europæiske Union (EU) som har til formål at styrke og harmonisere beskyttelsen af personoplysninger i EU[11]. Helt grundlæggende er det essentielt at forstå hvordan EU som instans forvalter lovgivning ud til medlemslandende, som enten kan udføres ved et direktiv eller en forordning.

Et direktiv er en retsakt hvor EU fastsætter et mål som alle medlemsstaterne skal opnå. Ved et direktiv skal de enkelte lande som hovedregel selv implementere dette ved lov eller administrative forskrifter. Et eksempel på dette er EU's direktiv om forbrugerrettigheder 2011/83/EU[12], hvor der i artikel 9, stk. 1 fremgår en fortrydelsesret på 14 dage ved fjernsalg, hvilket i dansk ret er implementeret i Forbrugeraftaleloven, §19, stk. 1[13]. En forordning er en almengyldig og bindende retsakt, som gælder i alle dens enkeltheder og umiddelbart i hver medlemsstat. Den gælder i Danmark på samme vis som enhver anden dansk lov. En fordel ved en forordning er at den skaber en identisk lovgivning på tværs af medlemslande hvilket sikrer større ensretning og retssikkerhed inden for EU. Udgangspunktet i en forordning er at ingen medlemslande kan eller må foretage ændringer til forordningen, ej heller må de igennem fortolkning begrænse eller ændre forordningens regler og formål. Dette er dog ikke en absolut sandhed, da der i nogle forordninger er indført muligheder for nationale ændringer og præciseringer. Databeskyttelsesforordningen er som navnet antyder en forordning, hvorfor den er gældende som beskrevet i sidstnævnte kategori. Baggrunden for forordningen, formålet, definitioner, relevante artikler mv. vil blive gennemgået i det følgende.

4.1 Baggrunden for beskyttelse af personoplysninger

Beskyttelse af personoplysninger er ikke et nyt emne. Personoplysninger har været på dagsordenen længe, da EU bl.a. i 1995 vedtog direktivet om databeskyttelse 95/46/EF[14]. Direktivet havde bl.a. til formål at sørge for at behandling af personoplysninger skete i overensstemmelse med de EU-borgernes grundlæggende rettigheder og frihedsrettigheder, uanset statsborgerborgerskab og bopæl, jf. direktivets betragtning (2). Danmark implementerede direktivet i dansk lovgivning igennem Persondataloven.

[11] Jf. betragtning (3) i Databeskyttelsesforordningen
[12] Direktivet 2011/83/EU: https://eur-lex.europa.eu/eli/dir/2011/83/oj
[13] Forbrugeraftaleloven, retsinformation: https://www.retsinformation.dk/forms/r0710.aspx?id=160666
[14] Direktivet om databeskyttelse, eur-lex: https://eur-lex.europa.eu/eli/dir/1995/46/oj

Udover det førnævnte direktiv har EU præciseret fortolkningen om individets rettigheder ved Charter om grundlæggende rettigheder[15]. Baggrunden for charteret er at bryde etablerede rettigheder fra forskellige tider og forskellige måder i det enkelte EU-medlemsland for at forståelsen af grundlæggende rettigheder er konsistent og ensrettet i EU-medlemslandende. I 2000 udstedte EU charter om grundlæggende rettigheder med det formål at fastlægge grundlæggende rettigheder for alle EU-borgere. Det er relevant at benævne charteret forbindelse med Databeskyttelsesforordningen, fordi en grundlæggende rettighed er at give alle EU-borgere ret til privatliv og beskyttelse af deres personoplysninger, jf. charterets artikel 7 og 8.

Databeskyttelsesforordningen blev vedtaget i EU-parlamentet den 14. april 2016. På trods af at forordningen blev vedtaget i 2016, blev der indført en "sunrise-periode" på 2 år, hvilket betød at selvom forordningen formelt trådte i kraft den 24. maj 2016 havde den først retsvirkning fra den 25. maj 2018. Den 2-årige periode betød at medlemslandende og de berørte organisationer fik tid til at tilpasse sig forordningen, da der var tale om store ændringer og betydelige sanktioner. Vedtagelsen satte punktum for 4 års lovarbejde under storpolitisk og pressemæssig opmærksomhed. Forordningen bygger i høj grad på allerede velkendte principper. Vedtagelsen af forordningen kan betragtes som en milepæl inden for EU- og persondataretten. Siden vedtagelsen af forordningen har der for både offentlige myndigheder og private virksomheder forelagt et stort arbejde i at sikre den nuværende og fremtidige behandling af personoplysninger sker i overensstemmelse med reglerne i forordningen.

Inden forordningen trådte i kraft, har Danmark allerede haft fokus på personoplysninger, hvilket kan ses i de gamle love som Persondataloven. Set fra et dansk perspektiv er det ikke drastiske ændringer, dog med forbehold da der stadig er meget nyt, bl.a. væsentlig større bødetakster end hidtil set, helt op til 20 millioner euro eller 4% af en organisations globale omsætning, samt højere krav til dokumentation. Forordningen sikrer en konsolidering af EU-persondataret og er med til at organisationer på tværs af grænser kan behandle personoplysninger ensartet. I henhold til forordningen er der stadig mange ubesvarede spørgsmål, som først vil blive besvaret i fremtiden når fremtidige domme fra EU-domstolen klarlægger disse. Der er i forordningen mulighed for at fastsætte nationale særregler på en række områder. I Dan-

[15] Charter om grundlæggende rettigheder, eur-lex: https://eur-lex.europa.eu/eli/treaty/char_2012/oj

mark er der for eksempel etableret et tværministerielt projekt under Justitsministeriets Databeskyttelseskontor med fokus på at vurdere konsekvenserne af forordningen for Dansk ret og behovet for danske særregler. Indenfor den seneste tid er der af Folketinget den 17. maj 2018 vedtaget Databeskyttelsesloven[16]. Et eksempel på en lempelse er i Databeskyttelseslovens §6 stk. 2, hvori der fastsættes en grænse for børns samtykke på 13 år, imod forordningens artikel 8, stk. 1, hvor grænsen er 16 år. I artikel 8 fremgår også at en medlemsstat frit kan sætte aldersgrænsen, så længe dette mindst er 13 år, hvilket Danmark altså har udnyttet.

Baggrunden og formålet med Databeskyttelsesforordningen, samt eksempler på særregler der findes, er nu blevet gennemgået. I det følgende afsnit vil der blive gennemgået relevante områder og artikler i forordningen i henhold til afhandlingens undersøgelsesområde.

4.2 Anvendelsesområde

Det er relevant at gennemgå forordningens anvendelsesområde, for at skabe forståelse for hvornår forordningen finder anvendelse. Der skelnes mellem organisatorisk afgrænsning og territorialt anvendelsesområde samt anvendelse uden for EU.

Organisatorisk afgrænsning: Ved den organisatoriske afgrænsning forstås hvem og hvilke enheder der er underlagt forordningen. Udgangspunktet er at forordningen finder anvendelse på alle, som foretager behandling af personoplysninger og omfatter både offentlige myndigheder og virksomheder.

Territorialt anvendelsesområde: I forordningens artikel 3 bliver det geografiske anvendelsesområde fastlagt. Heri fremgår adskillelse mellem dataansvarlige og databehandlere etableret inden for og uden for EU. Hertil er det den faktiske og effektive udøvelse af aktiviteter der er afgørende. Etableringens retlige form er uden betydning. Forordningen finder anvendelse på behandling af personoplysninger foretaget af en dataansvarlig eller databehandler etableret i EU, uagtet om selve behandlingen finder sted i EU eller ej. Dette kan eksempelvis være et dansk firma, som benytter sig af en amerikansk leverandør, her vil den amerikanske leverandør være underlagt bestemmelserne i forordningen. Et datterselskab eller en filial i EU vil blive anset som en etablering og være underlagt forordningen. Fra EU-Dom-

[16] Databeskyttelsesloven, retsinformation: https://www.retsinformation.dk/Forms/r0710.aspx?id=201319

stolens praksis omkring det tidligere direktiv 95/46/EF kan den blotte tilstedeværelse af en salgsrepræsentant inden for EU blive anset som etablering og dermed omfattet af GDPR. For yderligere læsning herom henvises til C-230/14, Weltimmo v NAIHC[17].

Anvendelse uden for EU: Udover at forordningen finder anvendelse på databehandlere og dataansvarlige etableret inden for EU jf. ovenstående, kan forordningen finde anvendelse uden for EU. Forordningen vil finde anvendelse uden for EU, hvis der bliver behandlet oplysninger om personer bosiddende i EU. Dette vil være tilfældet, hvis behandlingen vedrører udbud af varer eller tjenesteydelser til personer i EU eller ved overvågning af personer i EU. Ved den konkrete vurdering af hvorvidt der sker udbud af varer eller tjenesteydelser til EU-borgere skal der ses på hensigten. Her vil der være fokus på om udbuddet er målrettet kunder i et eller flere EU-lande og faktorer til denne vurdering kan være valuta, sprog på hjemmesiden, erfaringer, anmeldelser fra andre EU-kunder eller andre markedsføringstiltag tilknyttet EU. Såfremt dette er tilfældet, kan en virksomhed risikere at være underlagt forordningen. Dette var eksempelvis tilfældet i C-131/12[18], hvor Google Spain var underlagt det tidligere direktiv. Såfremt en dataansvarlig eller databehandler uden for EU anses som underlagt forordningen, vil denne være pålagt at udnævne en repræsentant som befinder sig inden for EU og som skal repræsentere denne i forhold til dennes forpligtelser under forordningen, jf. artikel 27. Hertil er lejlighedsvis behandling fritaget for kravet om repræsentant.

Den organisatoriske afgrænsning og territoriale anvendelsesområde samt behandling uden for EU er gennemgået i dette afsnit. Forordningen indeholder mange definitioner hvoraf de mest centrale for afhandlingen vil blive gennemgået.

4.3 Centrale definitioner

Relevante definitioner i afhandlingen omhandler bl.a. definition af personoplysninger, dataansvarlig og databehandler m.fl. og fremgår af forordningens artikel 4.

Definition	Uddybning
Personoplysninger	Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede). Ved en identificerbar fysisk person forstås en person der direkte eller indirekte kan identificeres ved

[17] Link til dommen: http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0230&lang1=en&type=TXT&ancre=
[18] Link til dommen: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A62012CJ0131

Definition	Uddybning
	en eller flere typer af oplysninger, jf. artikel 4, stk. 1. Forordningen inddeler personoplysninger i tre kategorier, hertil almindelige, særlige personoplysninger og straffedomme og lovovertrædelser. I artikel 9 fremgår en afgrænset liste af de særlige personoplysninger, og straffedomme og lovovertrædelser er nævnt i artikel 10. Dertil vil alle personoplysninger der ikke falder ind under artikel 9 eller 10 være almindelige personoplysninger. CPR-numre fremgår ikke af forordningen. I forordningen fremgår af artikel 87 at betingelser for behandling af nationale identifikationsnumre fastsættes af medlemsstaterne. CPR-numre er reguleret i dansk lovgivning jf. Databeskyttelsesloven §11.
Behandling	Enhver aktivitet eller række af aktiviteter med eller uden brug af automatisk behandling som personoplysninger eller en samling af personoplysninger gøres til genstand for, jf. artikel 4, stk. 2.
Dataansvarlig	En fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ der alene eller sammen med andre afgør til hvilket formål og hvilke hjælpemidler der må foretages behandling af personoplysninger, jf. artikel 4, stk. 7.
Databehandler	En fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandlinger personoplysninger på den dataansvarliges vegne, jf. artikel 4, stk. 8.
Databrud	Et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet, jf. artikel 4, stk. 12.
Tilsynsmyndighed	En uafhængig offentlig myndighed der er etableret i en medlemsstat i henhold til artikel 51, jf. artikel 4, stk. 21. I Danmark er tilsynsmyndigheden Datatilsynet[19]. På Datatilsynets hjemmeside fremgår vejledninger og skabeloner vedrørende behandling af personoplysninger.

Tabel 2: Centrale definitioner i GDPR.
Kilde: Egen tilvirkning

I Tabel 2 er der oplistet forordningens centrale definitioner der har relevans til afhandlingen. Der skal nu redegøres for forordningens grundlæggende principper for behandling af personoplysninger.

4.4 Grundlæggende principper

Forordningen opstiller en række grundlæggende principper om behandling af personoplysninger, jf. artikel 5, stk. 1, litra a-f, der skal overholdes ved enhver behandling, hvilket inkluderer både dataansvarlige og databehandlere. Det er dog vigtigt at fastslå at det helt overordnede ansvar for at de grundlæggende behandlingsregler bliver overholdt ligger hos den dataansvarlige. Dette betyder i praksis at den dataansvarlige ikke kun skal sikre sin egne behandlinger, men også sikre at eventuelle databehandlere også overholder reglerne på den dataansvarliges vegne. Et vigtigt tillæg hertil er at den dataansvarlige har

[19] Link til Datatilsynets hjemmeside: https://www.datatilsynet.dk/

pligt til at kontrollere om reglerne bliver overholdt. Udover at leve op til de grundlæggende behandlingsregler skal den dataansvarlige også sikre sig at behandlingsregler og principper dokumenteres. Ved at behandle personoplysninger i henhold artikel 5, stk. 1, litra a-f, opfylder man kriteriet for ansvarlighed, jf. artikel 5, stk. 2. De grundlæggende principper er specificeret i nedenstående tabel:

Artikel 5, stk. 1.	Grundlæggende princip	Fortolkning
Litra a	Lovlighed, rimelighed og gennemsigtighed	Personoplysninger skal behandles lovligt, rimeligt og gennemsigtigt i forhold til den registrerede
Litra b	Formålsbegrænsning	Personoplysninger skal indsamles og behandles i overensstemmelse med angivne og saglige formål. Andre formål må kun ske hvis disse er forenelige med de oprindelige formål, samtykke og lov.
Litra c	Dataminimering	Personoplysninger skal være tilstrækkelige, relevante og begrænset til det som er nødvendigt i forhold til de aftalte og saglige formål. Indsamling skal være nødvendigt og ikke kun belejligt.
Litra d	Rigtighed	Personoplysninger skal til enhver tid være opdateret og ajourført og rimelige skridt skal foretages for at berigtige eller slette forkerte oplysninger.
Litra e	Opbevaringsbegrænsning	Personoplysninger skal kun opbevares så længe det er nødvendigt for at overholde de saglige og aftalte formål som er nødvendige for behandlinger. Personoplysninger skal slettes eller anonymiseres når opbevaring ikke længere er nødvendigt til behandlingen.
Litra f	Integritet og fortrolig	Personoplysninger skal behandles på en sådan måde at der sikres integritet og fortrolighed, hvorfor der stilles krav til at forhindre bl.a. uautoriseret og ulovlig behandling.

Tabel 3: Grundlæggende principper.
Kilde: Egen tilvirkning pba. GDPR art. 5. stk. 1

Ved opfyldelse af principperne oplistet i Tabel 3 sikrer dataansvarlige og databehandlere at disse lever op til kravene om de grundlæggende principper og dermed er ansvarlige jf. artikel 5 stk. 2.

4.4.1 Hvornår må personoplysninger behandles?

Personoplysninger er defineret i Tabel 2 og som forklaret i ovenstående om grundlæggende principper skal personoplysninger behandles med lovlighed, hvilket betyder at personoplysninger kun må behandles når der foreligger hjemmel til behandling. Hjemlerne til behandling fremgår af artikel 6, 9 og 10, afhængig hvilken kategorier af personoplysninger der er tale om. Afhandlingen tager udgangspunkt i forholdet mellem dataansvarlig og databehandler, og hvordan der skabes sikkerhed for efterlevelse af en indgået aftale mellem de to parter.

Mellem dataansvarlige og databehandlere vil det være aftalt, som det også fremgår i Datatilsynets standarddatabehandleraftale[20], at det er den dataansvarlige der står med ansvaret for at der foreligger hjemmel til enhver databehandling som databehandler foretager, da databehandler arbejder efter instruks fra dataansvarlig. Dertil kan der være eventuelle retlige forpligtelser som en databehandler, kan have, hvortil der kan være hjemmel til at foretage dispositioner, som ellers ikke er aftalt mellem den dataansvarlige og databehandleren. Eksempelvis forpligtelser til at indberette A-skat, AM-bidrag eller indberette mistanke om hvidvask[21]. Det forhold som gør sig gældende i afhandlingen, som også fremgår af afgrænsningen, er forholdet mellem en dataansvarlig og en databehandler. Afhandlingen bliver udarbejdet med en forudsætning om at den dataansvarlige har hjemmel således at en databehandler må behandle personoplysninger på en dataansvarliges vegne.

4.4.2 Hvordan skal personoplysninger behandles?

Udover at lovligheden for behandlingen af personoplysninger skal være på plads, er der også en række andre forpligtelser som både dataansvarlig og databehandler skal følge for at efterleve de grundlæggende principper.

Rimelighed og gennemsigtighed: For en behandling af personoplysning gælder at den skal være rimelig. Ved rimelighed forstås at der på baggrund af en konkret vurdering skal vurderes om en behandling er rimelig i forhold til det formål der er fastlagt. Der er mulighed for at en tilsynsmyndighed på baggrund af almindelig samfundsopfattelse kan afvise en behandling som ellers kunne være anset for lovlig. Dertil gælder også at behandlingen skal være gennemsigtig. Ved gennemsigtig forstås at den registrerede som et klart udgangspunkt skal have kendskab til at der behandles personoplysninger om den pågældende. Derudover skal den registrerede på letforståelig vis have oplyst, hvilke personoplysninger der behandles og med hvilket formål samt hvilke rettigheder den registrerede har i forbindelse med behandlingen. Principperne om lovlig, rimelig og gennemsigtighed i forordningen svarer i høj grad til det der i den danske persondatalov er kendt som god databehandlingsskik. Selvom god databehandlingsskik ikke fremgår

[20] Findes som bilag D og link til Datatilsynets standarddatabehandleraftale: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2018/feb/ny-skabelon-skal-hjaelpe-virksomheder-og-myndigheder-med-at-blive-klar-til-databeskyttelsesforordningen/

[21] Se link til Erhvervsstyrelsens vejledning: "Sådan undgår du at medvirke til hvidvask": https://erhvervsstyrelsen.dk/sites/default/files/2019-02/saadan_undgaar_du_at_medvirke_til_hvidvask.pdf

ved ordlyd i forordningen, vil dette fortsat være et krav for danske virksomheder, jf. de danske tillægsregler.

Formålsbegrænsning: Ved princippet formålsbegrænsning forstås at personoplysninger alene må indsamles til udtrykkeligt angivne formål og at den behandling som personoplysningerne på et senere tidspunkt underlægges, ikke må være uforenelige med det oprindelige formål. Dette betyder at den dataansvarlige inden indsamlingen påbegyndes skal fastslå hvilke formål indsamlingen og behandlingen af personoplysningerne skal benyttes til. Af dette princip ligger også at behandlingen skal være udtrykkelig, hvilket betyder at formålet skal være veldefineret. I Persondataloven fremgår at formålet med behandlingen skal være sagligt, hvilket i høj grad svarer til princippet i forordningen.

Dataminimering: Forordningen stiller krav til at behandlede personoplysninger skal være tilstrækkelige, relevante og begrænset til det der er nødvendigt i forhold til formålet med behandlingen. Dette medfører at der ikke må behandles oplysninger som er unødvendige i forhold til formålet, og at behandlingen ikke sker på et ufuldstændigt grundlag. Der er tale om en proportionalitetsvurdering, hvortil det konkret skal vurderes om den indsamlede data er relevant og nødvendig for at opnå formålet.

Rigtighed: Den dataansvarlige er forpligtet til at tage ethvert rimeligt skridt til at slette eller rette personoplysninger som ikke er korrekte. Dertil skal den dataansvarlige sørge for at ajourføre de registrerede personoplysninger. Hvornår den dataansvarlige skal kontrollere om personoplysninger er korrekte eller forældede, afhænger af formålet med behandlingen, jo større betydning det har for den registrerede jo mere kontrol skal den dataansvarlige foretage. Den registrerede har ret til at kræve at få forkerte personoplysninger om sig selv rettet.

Opbevaringsbegrænsning: Den dataansvarlige må ikke opbevare personoplysninger i længere tid end det er nødvendigt for opfyldelse af det formål hvortil personoplysningerne behandles. Dette hænger i høj grad sammen med princippet om dataminimering. Det fastslås i dette princip, at data skal slettes eller evt. anonymiseres, når det har opfyldt formålet med behandlingen. Hvor lang tid der skal gå før personoplysninger skal slettes eller anonymiseres skal vurderes konkret på baggrund af formålet med den fortsatte opbevaring samt hvor indgribende denne opbevaring vil være. Et eksempel på dette er at kriminalitetsforebyggende videoovervågning skal slettes efter senest 30 dage jf. Lov om tv-overvågning

§4c, stk. 4. Det er beskrevet hvilke krav der stilles til at opfylde de grundlæggende principper i forordningen som skal overholdes af Dataansvarlige uagtet om denne selv behandler personoplysninger eller anvender en databehandler. Såfremt behandlingen er outsourcet aftales det i databehandleraftalen hvorledes ovenstående krav skal efterleves.

4.4.3 Hvad er passende sikkerhed og hvad gør man ved databrud?

Forordningen har som et af hovedformålene at styrke databeskyttelsen for individer, hvorfor etablering af sikkerhedsforanstaltninger til de behandlede personoplysninger er et centralt emne. Som nævnt tidligere er det et grundlæggende princip at personoplysninger behandles med integritet og fortrolighed, og i den forbindelse stilles der krav til sikkerheden for behandling af personoplysninger. Jf. artikel 5, stk. 1, litra f, skal personoplysninger behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende oplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse under anvendelse af passende tekniske eller organisatoriske foranstaltninger. I den dataansvarliges anvendelse af en databehandler er det derfor vigtigt at have sikkerhed i overvejelserne. Personoplysningssikkerhed er nærmere beskrevet i forordningens kapitel 4 om dataansvarlige og databehandlere, afdeling 2.

Behandlingssikkerhed – Artikel 32: Dataansvarlige og databehandlere skal foretage passende tekniske og organisatoriske handlinger for at sikre sikkerhedsniveauet i forhold til de gældende risici for de registrerede og værne om disses personoplysninger. Passende tekniske og organisatoriske tiltag, sikkerhedsniveauet, er ikke en absolut størrelse, men afhænger i høj grad af den enkelte organisation og hvilke typer af personoplysninger der besiddes og behandles. Det er med andre ord nødvendigt at foretage en afvejning og dette afgøres i den konkrete situation. Dertil er der listet en række krav til sikkerheden der kan være relevante, jf. artikel 32, stk. 1, litra a-d:

- Pseudonymisering og kryptering
- evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
- evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

- en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed

Pseudonymisering og kryptering er tekniske tiltag som foretages for at sikre sig mod udefrakommende trusler. Pseudonymisering betyder at direkte identificerbare parametre erstattes med pseudonymiserede koder[22]. Kryptering er processen hvor man koder en besked eller information på en sådan måde at det kun er godkendte parter, der kan få adgang til det og læse det. Begge disse tiltag er med til at sikre fortroligheden af data. Tilgængelighed og robusthed af data i behandlingssystemer skal sikres for at opfylde kravet om integritet. Derudover kan det også være et krav at der tages backup af data i tilfælde af nedbrud eller uvedkommende får adgang (uvedkommende kan have incitament til at låse eller slette data), hvilket er med til at sikre tilgængeligheden ved at adgangen kan genoprettes. Ydermere kan det være et krav at der er procedurer for regelmæssig afprøvning af alle aspekter af sikkerheden, eksempelvis i form af læsbarhedstest af backups og rettelser til adgange til diverse IT-systemer. Der kan også foregå løbende vurdering og evaluering af alle de tekniske og organisatoriske tiltag, som i det hele taget er med til at sikre behandlingssikkerheden. Som tidligere nævnt skal der altid foretages en vurdering af den konkrete situation, hvorfor de oplistede krav blot kan være relevante. For at sikre sig høj datakvalitet og plan ved databrud kan der udarbejdes en konsekvensanalyse.

Konsekvensanalyse, DPIA – Artikel 35: En Data Protection Impact Assesment (DPIA), også kaldt en konsekvensanalyse, er en kortlægning af beskyttelsen ved behandling af personoplysninger og er bygget op efter en risikoanalyse af behandlingen af personoplysninger og en handlingsplan i forhold til risikovurderingen. En konsekvensanalyse kan være kompleks og skal som minimum indeholde nedenstående 4 punkter:

- En systematisk beskrivelse af behandlingsaktiviteterne og formålene med denne behandling
- En vurdering af om behandlingsaktiviteterne er nødvendige og rimelige i forhold til formålet med behandlingen
- En vurdering af risici for de registreredes rettigheder og frihedsrettigheder
- Sikkerhedsforanstaltninger og mekanismer der påtænkes at blive opsat for at imødegå risici og som kan sikre beskyttelse af personoplysninger

[22] Definition af pseudonymisering fremgår af GDPR artikel 4, stk. 5.

Hvis en konsekvensanalyse viser høj risiko for de registrerede og denne risiko ikke begrænses eller kan begrænses med passende foranstaltninger er det et krav at underrette tilsynsmyndigheden. For de dataansvarlige og databehandlere stilles der krav om udarbejdelse af en konsekvensanalyse hvis en eller flere af nedenstående punkter er opfyldt:

- Der foretages en systematisk og omfattende vurdering af personlige forhold omkring fysiske personer, som er baseret på automatisk behandling og som lægger grund til afgørelse med retsvirkning
- Behandling i stort omfang af særlige kategorier af oplysninger, såsom straffedomme og lovovertrædelser
- Der foretages systematisk overvågning af et offentligt tilgængeligt område i et stort omfang

Derudover kan tilsynsmyndigheden udarbejde og offentliggøre lister som henholdsvis underlægger og fritager typer af behandlingsaktiviteter for en konsekvensanalyse. Selvom en konsekvensanalyse er udarbejdet og sikkerhedsforanstaltninger er opsat, kan databrud stadig forekomme. Underretning om databrud bliver behandlet i artikel 33 og 34.

Underretning om databrud – Artikel 33 og 34: I artikel 32 fremgår det at man ved behandling af personoplysninger skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger, for at reducere risikoen for at der sker brud på persondatasikkerheden. I tilfælde af databrud har den dataansvarlige pligt til at underrette tilsynsmyndigheden og de registrerede i henhold til artikel 33 og 34.

Pligten hos den dataansvarlige til at underrette tilsynsmyndigheden opstår hvis der er et databrud, medmindre det er sandsynligt at bruddet ikke vil føre til en risiko for fysiske personers rettigheder og frihedsrettigheder, jf. artikel 33. Den dataansvarlige har bevisbyrden for at undtagelsen er til stede, da det er den dataansvarlige som bærer ansvaret for beskyttelsen af personoplysninger. Underretningen til tilsynsmyndigheden skal ske uden unødig forsinkelse og om muligt senest 72 timer efter at være bekendt med databruddet. "Uden unødig forsinkelse" vurderes særligt ud fra karakteren og alvoren af bristen, og ud fra konsekvenser og skadevirkninger for de registrerede. Dertil er der pligt til at begrunde hvis man går ud over 72 timer, men oplysninger kan gives i faser. Underretningen af databruddet skal bl.a. indeholde:

- Kategorierne og det omtrentlige antal af berørte registrerede, samt
- Kategorierne og det omtrentlige antal af berørte registreringer
- Navn på DPO eller kontaktperson for yderligere oplysninger
- Beskrivelse af de sandsynlige konsekvenser af bristen
- Beskrivelse af de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at behandle bristen, herunder, hvor det er passende, foranstaltninger til at mitigere mulige skadevirkninger

Der et krav om dokumentation som har til formål om at gøre tilsynsmyndigheden i stand til at kontrollere om bestemmelserne i artikel 33 er overholdt. Pligten til at underrette de registrerede fremgår af artikel 34. Det fremgår heraf at de registrerede kun skal underrettes, hvis databruddet sandsynligvis vil føre til en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Det er den dataansvarlige der har bevisbyrden for at betingelsen ikke er opfyldt. Underretningen skal ske uden unødig forsinkelse efter at være blevet bekendt med databruddet, og der er ikke nogen fastsat en frist som i artikel 33. "Uden unødig forsinkelse" fastlægges ud fra kriterier om behovet for de registrerede for at kende til databruddet, sådan at personen kan reagere.

Der er i dette afsnit gennemgået det relevante for hvad der skal forstås ved passende sikkerhed samt pligten til at underrette ved databrud. Hertil er der blevet redegjort for artikel 32 om behandlingssikkerhed, artikel 35 om konsekvensanalyse, artikel 33 og 34 om underretning ved databrud. Gennemgangen i afsnittet vil være relevant for en dataansvarlig at tage stilling til, både hvis denne selv udfører en behandling, men også hvis der benyttes en databehandler, hvorfor der i næste afsnit redegøres for forholdet mellem en dataansvarlig og en databehandler.

4.5 Dataansvarlig og databehandler

En databehandler er en organisation som varetager hele eller dele af en dataansvarliges behandling af personoplysninger. Eksempler herpå er outsourcing af IT-drift, hosting services, HR og lønadministration. I forordningen bliver databehandlere tildelt en aktiv rolle og forpligtelser i stil med dataansvarlige. Dette betyder i praksis at en databehandler kan ifalde erstatningsansvar for manglende overholdelse af den

indgåede databehandleraftale, som hertil også bør være i overensstemmelse med forordningen, jf. artikel 82 og de gennemgåede grundlæggende principper. Ved benyttelsen af databehandlere, må den dataansvarlige kun benytte sig af databehandlere som kan stille de fornødne garantier i form tekniske og organisatoriske foranstaltninger, således at den dataansvarlige opfylder sine forpligtelser i henhold til forordningen, jf. artikel 28, stk. 1.

Herudover skal dataansvarlige være opmærksom på at databehandlere kan benytte sig af underdatabehandlere, hvorfor en dataansvarlig skal have dette element med i overvejelser ved outsourcing af behandling af personoplysninger. I praksis betyder dette at den dataansvarlige ikke blot kan anvende hvilken som helst databehandler, men skal være opmærksom på anvendelse af underdatabehandlere ved outsourcing. Denne opmærksomhed kommer også i forbindelse med at den dataansvarlige som nævnt kan hæfte solidarisk med en eller flere databehandlere for databehandlerens manglende overholdelse af forordningen, jf. artikel 82, stk. 4.

Efter omstændighederne kan en dataansvarlig ifalde bøde for databehandlerens behandling af personoplysninger, hvis denne eksempelvis skyldes den dataansvarliges manglende eller mangelfulde kontrol med databehandleren, jf. artikel 83, stk. 4, litra a, hvilket er centralt at forholde sig til i forbindelse med undersøgelsesområdet. Dette betyder at den dataansvarlige aktivt skal spørge ind til og kontrollere hvordan databehandleren foretager behandlinger af personoplysninger på vegne af den dataansvarlige. Ansvaret for dette gælder både inden aftaleindgåelsen, men også løbende under aftalens levetid. Dertil har den dataansvarlige en forpligtelse til at udarbejde skriftlig dokumentation af sin behandling af personoplysninger, og såfremt behandlingen er outsourcet, skal dette indgå i den dataansvarliges dokumentationsproces.

4.5.1 Databehandleraftaler

Når en dataansvarlig outsourcer aktiviteter der vedrører behandling af personoplysninger, skal der indgås en databehandleraftale i form af en kontrakt eller andet retligt dokument, jf. artikel 28, stk. 3. Databehandleraftaler er ikke en ny opfindelse, da disse også har eksisteret før forordningen ikrafttrædelse. Forordningen stiller dog krav til både eksistensen og indholdet i en sådan aftale. I forbindelse med dataansvarliges pligt til at føre tilsyn, er der i forordningen stillet krav til at der i databehandleraftalen skal indgå et afsnit hvori der stilles krav til databehandleren om at denne skal stille alle oplysninger til rådighed til den dataansvarlige. Dette er nødvendigt for at påvise overholdelse af kravene i artikel 28, og disse

oplysninger skal give mulighed for og bidrage til revisioner og inspektioner som foretages af den dataansvarlige eller en anden revisor som er bemyndiget af den dataansvarlige, jf. artikel 28, stk. 3, litra h.

I artikel 28, stk. 3, litra a-h, er der opstillet krav til hvad databehandleraftaler som minimum skal indeholde. Datatilsynet har dertil udarbejdet en skabelon for en databehandleraftale, som opfylder minimumskravene og er i overensstemmelse med forordningen og findes i bilag D. Det er vigtigt at fastslå at en databehandleraftale er et tillæg til den oprindelige aftale, hvorfor denne ikke kan stå alene.

4.6 Opsummering af GDPR

I kapitlet er der blevet redegjort for relevante artikler og centrale begreber i GDPR som er nødvendige at have en forståelse for i det videre arbejde med afhandlingen. Problemformuleringen tager afsæt i forholdet mellem en dataansvarlig og en databehandler, hvor der dertil er beskrevet hvilke forpligtelser parterne er underlagt. De gennemgåede principper og regler er krav som både dataansvarlige og databehandlere er underlagt, og såfremt en dataansvarlig har outsourcet behandlingsaktiviteten vil begge parters forpligtelser blive behandlet i en databehandleraftale.

Det er vigtigt at fastslå at dataansvarlige altid vil bære det endegyldige ansvar over for de registrerede i forhold til behandlingen af deres personoplysninger, også når der er tilføjet et ekstra led i denne proces i form af en databehandler. Grundet dette må en dataansvarlig kun benytte sig af databehandlere som kan stille de fornødne garantier. For at en dataansvarlig kan få de fornødne garantier skal der udføres kontrol af databehandlere i form af et tilsyn. For et tilsyn gælder at eksterne parter kan inddrages til at hjælpe med denne proces. Heriblandt kan en revisor afgive en erklæring, som kan benyttes, hvorfor der i det næste kapitel vil redegøres for revisors virkemidler og forudsætninger for revisors produkt.

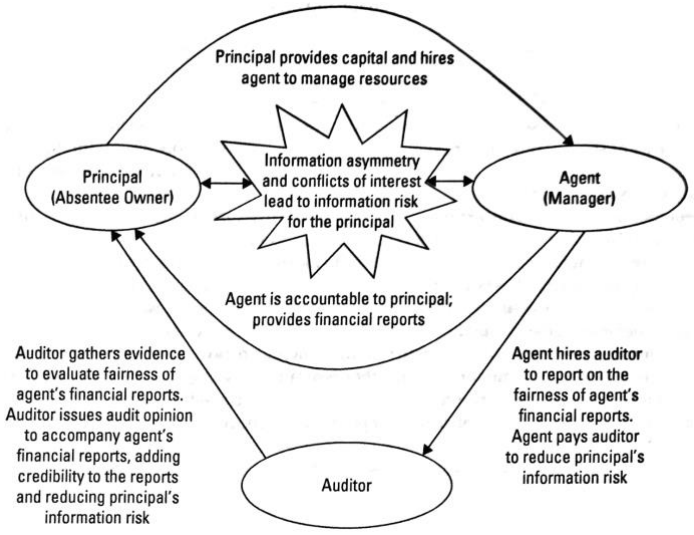
5. Revision

Som nævnt i det forrige kapitel er revisors arbejde en af flere mulige virkemidler som en dataansvarlig kan benytte som led i at føre tilsyn med en databehandler, og dermed overholde GDPR artikel 28. I dette kapitel vil der blive redegjort for hvad revision er og hvorfor der kan være et behov for dette. I forlængelse af kapitlet om GDPR vil der blive lagt fokus på revisorerklæringer, der kan benyttes til at opnå sikkerhed inden for behandling af personoplysninger hos en databehandler.

Revision forbindes ofte med at være et stykke arbejde udført af en revisor med det formål at lave en uvildig gennemgang og kontrol af en virksomheds regnskab. En revisor udtaler sig normalt om hvorvidt en virksomheds årsregnskab opfylder de lovmæssige krav, og om regnskabet som helhed giver et retvisende billede af virksomhedens aktiver, passiver, finansielle stilling samt resultat, hvilket bliver leveret i form af afgivelse af en revisorerklæring. I revision stilles der krav til revisors uafhængighed idet der er et behov for at have en uafhængig revisor til at forsyne en virksomheds årsrapport med en påtegning. Dette behov udspringer af, at regnskabets interessenter ikke selv har mulighed for at sikre sig, at de oplysninger, der fremgår af regnskabet, faktisk afspejler virkeligheden i virksomhedens økonomi. Sagt med andre ord er der behov for revision af en uvildig tredjepart, fordi der i mellem to parter vil være asymmetrisk information. Dette forhold kan beskrives med Principal-Agent teori.

5.1 Principal-Agent teorien

Teorien om Principal-Agent kan illustreres med nedenstående eksempel:



Figur 2: Principal-Agent forholdet.
Kilde: Eillifsen, A. et al. 2014, s. 7

Eksemplet i Figur 2 tager udgangspunkt i at en virksomhedsejer, principalen, har en manager, agenten, ansat. Hertil antages det at manageren hver måned skal sende månedsrapporter til virksomhedsejeren, hvorefter manageren så bliver honoreret efter de opnåede resultater. Dette kan skabe et incitament hos manageren til at overvurdere den forrige måneds præstation, for dermed at få et højere honorar. Dette er muligt fordi virksomhedsejeren ikke vil have nogen umiddelbar mulighed for selv at efterprøve de rapporter manageren leverer. Dette skaber det asymmetriske informationsforhold imellem de to parter. For at mitigere dette forhold kan principalen bede agenten om at inddrage en uafhængig tredjepart, eksempelvis en revisor, som skal vurdere de rapporter som manageren leverer til virksomhedsejeren. Ved at en revisor inddrages vil det medføre at virksomhedsejerens informationsrisiko bliver reduceret, fordi at revisoren kommer med sin vurdering af den afleverede rapport, der er tale om at revisor påtegner den afleverede rapport. I det tilfælde hvor manageren ikke har snydt med sine rapporter, vil denne påtegning også være i hans interesse. Dette skyldes at han ikke skal bekymre sig om at virksomhedsejeren har mistro til de rapporter han leverer og dermed frygte at hans honorar bliver påvirket, fordi virksomhedsejeren ikke vil honorere det fulde beløb.

Forholdet mellem en principal og agent opstår i mange sammenhænge og opstår i praksis bl.a. når en revisor påtegninger en årsrapport. I henhold til denne afhandlings undersøgelsesområde vil den oplagte situation være når en databehandler skal forsikre en dataansvarlig om at pågældende efterlever forpligtelserne i henhold til behandling af personoplysninger som bestemt i den indgåede databehandleraftale. Her vil det være muligt at benytte revisorerklæringen som en del af det tilsyn den dataansvarlige skal gennemføre i henhold til artikel 28. I situationen vil den dataansvarlige være principalen, som har uddelegeret noget ansvar til en databehandler, som vil agere som agenten. Databehandleren vil sagtens kunne fortælle og forsikre den dataansvarlige om at pågældende lever op til databehandleraftalen og vil overholde alle gældende krav, men igen opstår et forhold hvori der indgår asymmetrisk information, hvorfor den dataansvarlige ikke kan vide sig sikker. Dertil kan der opstå et incitament for databehandleren til at sige at pågældende lever op til forpligtelserne, men ikke lever op til forpligtelserne for eksempelvis at vinde en kontrakt eller spare tid og ressourcer selv. Som i det forrige tilfælde med virksomhedsejeren, så kan den dataansvarlige have begrænsede muligheder for selv at kontrollere om en databehandler taler sandt og rent faktisk overholder aftalen. En revisor kan derfor inddrages i denne situation og lave en påtegning om hvorvidt en databehandler faktisk lever op til de forpligtelser han er underlagt i henhold til databehandleraftalen. Slutresultatet bliver her det samme som i forrige situation,

når revisoren inddrages og laver en uafhængig påtegning, hvad end det er årsregnskaber, månedsrapporter eller overholdelse af en databehandleraftale, så vil informationskløften og den asymmetriske information blive reduceret til et sandsynligvis acceptabelt niveau.

Slutproduktet ved en revisor er en erklæring. Dette kan være inden for mange forskellige områder, såsom overholdelse af moms-, skat- og selskabslovgivning, årsregnskaber, rapporter, miljøregnskaber, CO2 kvoter, specifikke krav i GDPR eller en databehandleraftale. Fælles for alle disse erklæringer er at de kan komme i form af en erklæring med og uden sikkerhed, hvortil revisors handlinger og den tilhørende lovmæssige regulering er forskellig. Grundet dette vil de næste afsnit have fokus på hvad en uafhængig revisorerklæring er.

5.2 Revisors uafhængighed

Som forklaret i ovenstående er en erklæring en revisors slutprodukt. Disse erklæringer er primært reguleret i Revisorloven, Erklæringsbekendtgørelsen og andre bekendtgørelser udstedt på baggrund af Revisorloven. Som det er fastslået i forrige afsnit er det essentielle ved en revisorerklæring at den kommer fra en uafhængig og objektiv fagperson. For at erklæringen kan være objektiv og skabe værdi for andre, er det selvsagt et krav at revisor er uafhængig i forhold til både erklæringsemnet og tiltænkte brugere. Grundet dette stiller Revisorloven krav til revisors uafhængighed, som vil blive gennemgået herunder. Formålet med revisors arbejde, er som tidligere forklaret at afgive erklæringer med en høj grad af troværdighed i kraft af revisors rolle som offentlighedens tillidsrepræsentant, jf. Revisorloven §16, stk. 1. Det er en forudsætning hertil og krav for at denne troværdighed kan skabes at revisor er uafhængig af den person, virksomhed, myndighed eller lignende som revisor udtaler sig om.

Kravene om at revisor skal være uafhængig af genstanden for erklæringen og uafhængig af enhver form for erhvervsmæssig interesse, stammer tilbage fra loven omkring autoriserede revisorer fra 1909. Hvorvidt revisor nogensinde kan være 100% uafhængig er dog op til diskussion, som denne afhandling ikke vil gribe nærmere fat i. I dansk regulering var uafhængighed tidligere bygget op på at revisor ikke kun skal være konkret uafhængig, dvs. uafhængig for erklæringsemnet, men også skal være generel uafhængig, hvilket i praksis betyder at være udelukket fra at drive anden erhvervsmæssig virksomhed, herunder være privat eller offentligt ansat i andet end revisionsvirksomheder. For revisorer i dag gælder at

de kun er underlagt en konkret uafhængighed, og ikke længere den generelle uafhængighed. I Revisorloven §24 stk. 1. fremgår at revisor, revisionsvirksomheden og andre personer i revisionsvirksomheden, som er knyttet til eller kontrollerer udførelsen af en opgave med sikkerhed skal være uafhængig og må ikke være involveret i virksomhedens beslutningstagen. Denne uafhængighed gælder både i opgaveperioden og den periode som regnskabet eller hvad der erklæres om dækker. Den konkrete uafhængighed betyder at revisor skal være uafhængig når han udfører en erklæringsopgave med sikkerhed. Denne uafhængighed kan ifølge FSR – Danske Revisorers etiske regler nr. 290.6 opdeles i uafhængighed i opfattelse og fremtoning. Uafhængighed i opfattelse er at det skal være påviseligt, at revisor ikke er uafhængig. Uafhængighed i fremtoning er at revisor ikke er uafhængig, når der forelægger omstændigheder, der er egnet til at vække tvivl hos en velinformeret tredjemand. Disse typer af uafhængighed fremgår ikke direkte af loven, som i stedet for i Revisorloven §24 stk. 2. indeholder en oplistning af tilfælde, hvor revisor ikke er uafhængig, herunder direkte og indirekte økonomisk interesse. Derudover indeholder Revisorloven §24 stk. 3. en række trusler mod revisors uafhængighed, som hvis de ikke kan reduceres til et tilstrækkeligt niveau kan medføre, at revisor skal afstå opgaven. Grundprincipperne og reguleringen af revisors uafhængighed er nu gennemgået. En revisorerklæring indtræder i et tre-partsforhold, hvorfor det er essentielt at revisor er uafhængig, således at tredjemand kan stole på den erklæring der bliver fremlagt.

5.3 Hvilke erklæringstyper afgiver revisor?

Revisor kan afgive mange typer erklæringer, heriblandt er den mest gængse erklæringen ISA 700 udarbejdet af IAASB[23] som er revisors påtegning på årsregnskabet. Denne ISA gælder ved revision af et fuldstændigt regnskab med generelt formål[24]. For nogle virksomheder er denne påtegning et lovkrav[25] og for andre frivilligt. Udover denne ISA findes der en lang række af erklæringer som revisor kan udføre. Inden der bliver gennemgået andre erklæringer som revisor kan afgive, vil der først blive gennemgået regulering og andre forudsætninger for at kunne afgive en erklæring.

[23] IAASB har som formål at tjene offentlighedens interesser ved at fastsætte standarder af høj kvalitet for revision, andre erklæringsopgaver med sikkerhed og beslægtede opgaver samt ved at fremme ensretningen mellem internationale og nationale standarder for revision og andre erklæringer med sikkerhed, og derved øge kvaliteten og konsistens af global praksis samt styrke offentlighedens tillid på verdensplan til revisorprofessionen
[24] Jf. ISA 700.3
[25] For regnskabsklasse B, C og D er der revisionspligt, for klasse B kan udvidet gennemgang vælges, og for de mindste klasse B kan revision fravælges jf. Årsregnskabsloven §135.

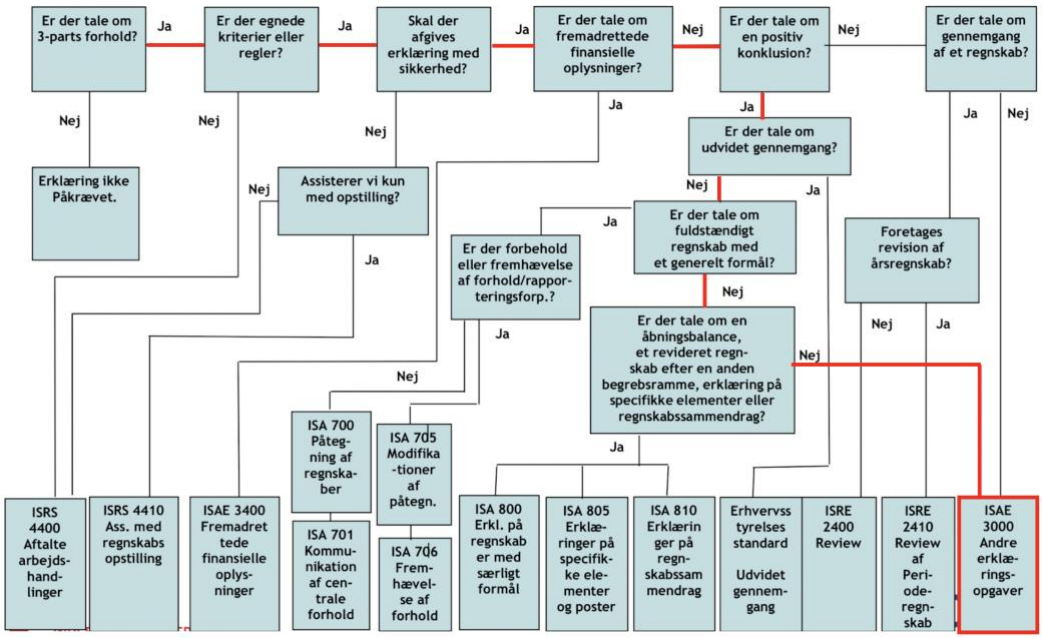
Afgivelse af erklæringer hører under deres respektive ISA, ISRE, ISAE eller ISRS standarder, som angiver de overordnede betragtninger i relation til revisors afgivelse af erklæringer med og uden sikkerhed. Erklæringerne findes med høj, begrænset eller ingen grad af sikkerhed. For erklæringer med sikkerhed finder Revisorloven §1, stk. 2. anvendelse samt Erklæringsbekendtgørelsen. For erklæringer uden sikkerhed finder Revisorloven §1, stk. 3. anvendelse. Herudover er forudsætningerne for afgivelse af erklæringer at der eksisterer et trepartsforhold, et erklæringsemne og egnede kriterier.

Et trepartsforhold omfatter en revisor, en ansvarlig part og en tiltænkt bruger. I forbindelse med fokusområdet for afhandlingen vil dette krav være opfyldt, idet der er tale om databehandler (ansvarlig part), dataansvarlig (tiltænkt bruger) og revisoren. I afhandlingens henseende vil erklæringsemnet være efterlevelse af databehandleraftalen, og de egnede kriterier vil være databehandleraftalen. For alle erklæringer som revisor afgiver, gælder at revisor jf. Revisorloven §16 skal udvise professionel kompetence og fornøden omhu. Dette betyder at hvis en revisor afgiver erklæringer i forbindelse med databehandleraftaler skal revisor have kendskab og indgående viden indenfor GDPR, og i de tilfælde hvor revisor ikke selv har det skal han sikre sig at relevante kompetencer inddrages i revisionen. I loven reguleres det at revisor ved erklæringer med sikkerhed skal være uafhængig jf. Revisorloven §24, stk. 1. og ved erklæringer uden sikkerhed skal det fremgå af påtegningen at han ikke er uafhængig jf. Revisorloven § 16 stk. 4, hvortil uafhængighed tidligere er gennemgået i afsnit 5.2. Revisor kan afgive mange typer af erklæringer, hvorfor disse oplistes i nedenstående tabel:

Standard	Navn på erklæring	Grad af sikkerhed
Bilag 1 til erklærings-bekendtgørelsen	Udvidet gennemgang	Begrænset
ISA 700	Udformning af en konklusion og afgivelse af erklæring om et regnskab	Høj
ISA 800	Særlige overvejelser - revision af regnskaber udarbejdet i overensstemmelse med begrebsrammer med særligt formål	Høj
ISA 805	Særlige overvejelser - revision af bestanddele af et regnskab samt specifikke elementer, konti eller poster, der indgår i et regnskab	Høj
ISA 810	Opgaver vedrørende afgivelse af erklæring om regnskabssammendrag	Høj
ISRE 2400	Opgaver om review af historiske regnskaber	Begrænset
ISRE 2410	Review af et perioderegnskab udført af selskabets uafhængige revisor og yderligere krav ifølge dansk revisorlovgivning	Begrænset
ISAE 3000	Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger	Begrænset eller høj
ISAE 3400	Undersøgelse af fremadrettede finansielle oplysninger (budgetter og fremskrivninger) og yderligere krav ifølge dansk revisorlovgivning	Begrænset eller høj
ISAE 3402	Erklæringsopgaver med sikkerhed om kontroller hos en serviceleverandør	Høj
ISRS 4000	Aftalte arbejdshandlinger vedrørende regnskabsmæssige oplysninger og yderligere krav ifølge dansk revisorlovgivning	Ingen
ISRS 4410	Opgaver om opstilling af finansielle oplysninger	Ingen

Tabel 4: Oversigt over erklæringsstandarder.
Kilde: Egen tilvirkning

Ovenstående erklæringer har forskellige formål, hvorfor det skal fastslås hvilken eller hvilke erklæringstyper, der vil kunne benyttes i forholdet mellem dataansvarlig og databehandler. For at afgrænse beskrivelser af erklæringstyper, vil nedenstående beslutningstræ anvendes, således at kun erklæringer, der er relevante for afhandlingen bliver gennemgået.



Figur 3: Beslutningstræ til valg af erklæringstype.
Kilde: Undervisningsslide slide 8, Karsten Andersen, BDO, Holdundervisning i Revision 2, CBS, d. 2.5.2018

Beslutningstræet i Figur 3 og de valg der efterfølgende bliver taget i forbindelse med forholdet mellem en dataansvarlig og en databehandler er tegnet med rød. Først og fremmest er der som tidligere beskrevet et trepartsforhold mellem revisor, dataansvarlig og databehandler. Hernæst vurderes der at der eksisterer egnede kriterier i form af hvorvidt en databehandleraftale bliver efterlevet. I vurderingen af om erklæringen skal være med eller uden sikkerhed, vurderes det at der skal vælges en erklæring med sikkerhed, da erklæringen skal benyttes i forbindelse med en tilsynsopgave i henhold til artikel 28. I forhold til fremadrettede finansielle oplysninger svares der nej, hvorfor der skal tages stilling til om der skal afgives en positiv konklusion eller ej, altså hvorvidt erklæringen skal være med høj eller lav grad af sikkerhed. Formålet er som beskrevet et led i en tilsynsopgave, hvorfor høj grad af sikkerhed vil være det oplagte valg. De næste tre spørgsmål om hvorvidt erklæringen omhandler regnskabsmæssige opstillinger, kan alle tre afkræftes og der kun en mulighed tilbage som fører til ISAE 3000. Da ISAE 3000 er valgt ud fra gennemgangen af ovenstående beslutningstræ, besluttes det at det er denne erklæring som vil blive gennemgået i det følgende.

5.4 ISAE 3000

ISAE 3000 omfatter erklæringer med både høj og begrænset grad af sikkerhed. I afhandlingen vil det primære fokus være på der hvor ISAE 3000 bliver afgivet med høj grad af sikkerhed, da det vurderes at handlingerne der udføres ved lav grad af sikkerhed, ikke er tilstrækkelige til at sikre databehandlerens efterlevelse af en databehandleraftale. Anvendelsesområdet for en ISAE 3000 erklæring er stort og kan bl.a. være med udgangspunkt i databehandleraftaler eller vedrørende interne kontroller. Formålet med at have en standard som ISAE 3000 er at skabe grundlæggende principper og relevante arbejdshandlinger som kan bruges til at afgive en erklæring med sikkerhed på andet end finansielle oplysninger. Samtidig giver standarden revisor vejledning om udførsel til denne slags opgaver. Målet med revisors arbejde efter en ISAE 3000 er at reducere opgaverisikoen til et niveau, som efter de konkrete omstændighederne er acceptabelt ved afgivelse af erklæringen. Erklæringer afgivet efter ISAE 3000 er underlagt Revisorloven §1, stk. 2. fordi der afgives en erklæring med sikkerhed og at udgangspunktet vil være til brug i et trepartsforhold. Dertil vil erklæringen også være underlagt Erklæringsbekendtgørelsen §16 til §19.

Formålet med ISAE 3000 er beskrevet i standardens afsnit 10-11. I afsnit 10 fremgår at det er revisors mål at opnå enten en høj grad af sikkerhed eller begrænset grad af sikkerhed, hvor det er relevant at sikre at emneindholdet ikke indeholder væsentlig fejlinformation. Dertil skal revisor udtrykke en konklusion om udfaldet af målingen eller vurdering af erklæringsemnet i en skriftlig rapport, som beskriver grundlaget for konklusionen. Revisor skal kommunikere yderligere information, som er krævet af ISAE 3000 og andre relevante ISAE'er. I afsnit 11 fremgår at revisor skal undlade at afgive en konklusion eller fratræde opgaven, hvor gældende lov eller øvrig regulering tillader dette, hvis der ikke kan opnås høj eller begrænset grad af sikkerhed og revisor ikke ser det tilstrækkeligt med en konklusion med forbehold. Som ved en hvilken som helst anden afgivelse af en erklæring, skal revisor inden han påbegynder arbejdet, have planlagt opgaven. I planlægningen skal revisor bl.a. tage stilling til arten af handlinger og den tidsmæssige placering jf. kravene i afsnit 40-47. Ved udførsel af erklæringsopgaven skal revisor udvise professionel skepsis og erkende at der kan være situationer, som medfører, at emneindholdet kan indeholde væsentlig fejlinformation. Derfor skal revisor være kritisk og stille spørgsmålstegn ved det opnåede revisionsbevis samt være opmærksom på revisionsbeviser, som strider imod den ansvarlige parts udsagn eller dokumenter. Dette gælder såfremt det opnåede revisionsbevis skaber usikkerhed i forhold til den ansvarlige parts udsagn eller dokumenter. Når revisor anvender specialister, skal revisor sikre sig at han sammen med specialisten har kompetencer til at han kan fastslå om det opnåede bevis

er tilstrækkeligt og egnet og danner grundlag for at udtrykke en konklusion. Revisor skal tillige indhente relevante skriftlige bekræftelser jf. ISAE 3000.56-60. Som det også er et krav ved andre standarder, skal revisor indhente dokumentation og arkivere dette. Da ISAE 3000 er en erklæring der kan afdække mange forskellige områder, vil dokumentationskravet grundet sagens natur være meget forskelligt afhængigt af hvad der erklæres om.

Overordnet skal erklæringen bygge på revisors konklusion på baggrund af det indsamlede revisionsbevis. Observationer og anbefalinger, herunder også eventuelle fremhævelser, skal holdes adskilt fra konklusionen og det skal være tydeligt af formuleringen at de ikke har påvirket konklusionen. Til udarbejdelsen af ISAE 3000 erklæringen fremgår krav oplistet i bilag A.

5.4.1 FSR – Danske Revisorers erklæringsskabeloner om persondata

En ISAE 3000 erklæring er som tidligere nævnt er en meget alsidig erklæring og kan benyttes til næsten alle erklæringsemner, hvorfor revisor skal tilpasse den til det enkelte behov. FSR - Danske Revisorer har af flere omgange udarbejdet ISAE 3000 erklæringsskabeloner vedrørende behandling af personoplysninger.

I 2017 udarbejdede Cybersikkerhedsudvalget under FSR – Danske Revisorer, ISAE 3000 erklæringsskabelonen *"Uafhængig revisors ISAE 3000- erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger"*[26]. Erklæringen forsøger at skabe den sikkerhed som en dataansvarlig jf. GDPR skal have. Erklæringen er beregnet til databehandlere, som vil give sikkerhed til deres kunder, de dataansvarlige, for at deres behandling, systemer og processer overholder de relevante krav i GDPR og andre danske lovkrav. Den dataansvarlige bærer altid har ansvaret for behandlingen af personoplysninger uagtet om denne foretager den egentlige behandling. Igennem erklæringen kan den dataansvarlige dermed få sikkerhed for at databehandleren har skriftlige og formelle procedurer for behandling af personoplysninger og overholdelse af GDPR.

Erklæringen skal som tidligere nævnt ses som en skabelon. Det er derfor nødvendigt, når erklæringen skal benyttes, at denne tilpasses til de relevante kontrolmål og omfang i forhold til den konkrete opgaves

[26] Link til FSR – Danske Revisorer artikel omkring ISAE 3000:
https://fsr.dk/Faglige_informationer/Om_revisor/Persondataforordningen/Erklaering%20om%20persondata_210917

omstændigheder og kompleksitet. Erklæringsskabelonen dækker meget bredt i forhold til kravene i GDPR, hvorfor man som dataansvarlig skal sikre sig at erklæringen bliver tilpasset de specifikke behov. Erklæringen er bygget op på at der er forslag til kontrolaktiviteter, som dækker mange af artiklerne i GDPR. Udfordringerne ved denne erklæringsskabelon er at den netop rammer meget bredt, og tager udgangspunkt i hele GDPR, hvortil der er flere af kontrolaktiviteterne der er lagt op til, som er den dataansvarliges ansvar. Dette gælder eksempelvis artikel 6 om gyldigt behandlingsgrundlag. Skabelonen lægger op til at det er databehandlerens ansvar at sikre at dette eksisterer, hvilket ikke er i overensstemmelse med GDPR. Databehandleren handler på instruks fra den dataansvarlige, hvorfor det altid vil være den dataansvarliges ansvar. Problemet er at erklæringen lægger op til at revisor skal erklære sig om hvorvidt databehandleren er compliant med GDPR på områder, som er den dataansvarliges ansvar.

Erklæringsskabelonen fra 2017 var udarbejdet før GDPR havde virkning, hvorfor FSR – Danske Revisorer har erkendt at denne ikke blev anvendt som forventet. Grundet dette har FSR – Danske Revisorer i februar 2019 udgivet endnu en erklæringsskabelon med fokus på behandling af personoplysninger. Til forskel fra den tidligere erklæringsskabelon tages der udgangspunkt i den indgåede databehandleraftale mellem en dataansvarlig og en databehandler.

Den seneste erklæringsskabelon fra FSR – Danske Revisorer er 'Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med [Dataansvarlig]"[27] og er den erklæringsskabelon som det fortsatte arbejde i afhandlingen vil tage afsæt i. Som navnet antyder og i modsætningen til erklæringsskabelonen fra 2017, tager den nye erklæringsskabelon udgangspunkt i den indgåede databehandleraftale. Dette skyldes at når man outsourcer sin databehandling, er det stadig den dataansvarliges ansvar at sikre, at personoplysninger bliver behandlet i overensstemmelse med GDPR.

Det ændrede fokus fra 2017 til 2019 kan bl.a. ses ved at der i den nye erklæringsskabelon ikke er lagt op til handlinger, der kontrollerer et fuldstændigt behandlingsgrundlag, da dette ikke er databehandlerens ansvar. Herudover er erklæringsskabelonen udarbejdet med udgangspunkt i Datatilsynets standard-

[27] ISAE 3000 Erklæringsskabelon findes i bilag E og Link til FSR – Danske Revisorer: https://fsr.dk/Faglige_informationer/Om_revisor/Persondataforordningen/FSR%20lancerer%20paa%20baggrund%20af%20samarbejde%20med%20Datatilsynet%20ny%20erklaering%20om%20persondata

databehandleraftale, hvorfor denne betragtning stemmer overens med databehandleraftalen. I Datatilsynets standarddatabehandleraftale punkt 3.3 fremgår at det alene er den dataansvarliges ansvar at der foreligger hjemmel til den behandling, som databehandleren instrueres i at foretage. Formålet med denne erklæringsskabelon er dermed, som det også var i erklæringsskabelonen fra 2017, at hjælpe de dataansvarlige med at sikre at deres databehandlere lever op til sine forpligtelser, og dermed gøre det muligt at benytte erklæringen som led i at føre et effektivt tilsyn i henhold til GDPR artikel 28. Det understreges dog at ISAE 3000 erklæringsskabelonen ikke vil være et tilsyn i sig selv, da dette kræver yderligere handlinger fra den dataansvarlige.

5.5 Opsummering af revision

I dette kapitel er der blevet redegjort for revisors uafhængighed og forpligtelser i revisors rolle som offentlighedens tillidsrepræsentant. Det er tidligere blevet forklaret at det er den dataansvarliges ansvar at behandling med personoplysninger sker i overensstemmelse med GDPR, hvorfor den dataansvarlige, når behandlingsaktiviteten outsources, er forpligtet til at føre tilsyn med sine databehandlere og dermed skabe sikkerhed. I den dataansvarliges tilsyn med databehandler kan en revisorerklæring inddrages.

Det er vigtigt at forstå revisors uafhængighed og dennes forpligtelser, da revisor er underlagt meget regulering, hvilket er med til at sikre troværdigheden og brugbarheden af en erklæring. Der findes mange typer af revisorerklæringer, hvortil det i afhandlingens henseende vil være oplagt at revisor afgiver en ISAE 3000 som led i den dataansvarliges tilsyn med databehandlere. ISAE 3000 er en meget alsidig erklæring som kræver tilpasning til det enkelte erklæringsemne. Hertil har FSR – Danske Revisorer i februar 2019 udarbejdet en ISAE 3000 erklæringsskabelon med udgangspunkt i en indgået databehandleraftale. Denne erklæringsskabelon har til formål at hjælpe med at sikre at en dataansvarlig har sikkerhed for at en databehandler har orden i procedurer og regler for beskyttelse af personoplysninger. I den fremadrettede undersøgelse vil der vurderes hvornår og hvordan en revisorerklæring kan og bør inddrages i den dataansvarliges tilsynsforpligtelse i henhold til GDPR.

6. Operationalisering

Videnskabsteori, undersøgelsesdesign, overvejelser omkring outsourcing, GDPR og revisionsteori er blevet redegjort for og fastlagt. Den næste del af afhandlingen omhandler hvordan teorien skal omdannes til empirisk målbare størrelser. Denne proces kaldes også for operationalisering[28]. Ved gennemførslen af dataindsamlingen igennem semistrukturerede interviews, er det vigtigt at have fastlagt reguleringer, teori og metode der skal undersøges. Når det er fastlagt hvad der skal undersøges, skal man være klar over at man sjældent kan gå direkte ud og spørge respondenten om dette. Inden der påbegyndes interviews, er det nødvendigt at omdanne den anvendte teori og regulering til håndgribelige spørgsmål som respondenten kan svare på.

Dataansvarlige og databehandlere kan være forskellige og have forskellige forudsætninger til at forstå spørgsmål inden for GDPR og anden regulering. Man er som interviewer derfor nødsaget til at klargøre hvem man spørger og tilpasse spørgsmålene til de enkelte grupper af respondenter. Er det eksempelvis ikke en juridisk anlagt respondent som interviewes, ville der være mulighed for at denne ikke ville kunne besvare fyldestgørende, hvis der blot blev spurgt ind til specifikke artikler i GDPR. Det er nødvendigt at tilpasse spørgsmålene som omhandler artiklerne på en måde, så respondenten eksempelvis får svaret på hvordan de fører tilsyn efter artikel 28, men uden konkret at spørge ind til artiklen. Hertil er det forskellige typer af respondenter som bliver interviewet, hvorfor det er forskellige interviewguides som udarbejdes og tilpasses til en bestemt faggruppe. Der kan ofte være mange forskellige metoder hvorpå man kan spørge ind til et givent emne, men i operationaliseringsprocessen gøres det klart, hvordan man som interviewer har tænkt sig at gøre det og hvilke tanker og antagelser der ligger til grund for de givne spørgsmål. Ved at have en formaliseret operationaliseringsfase bliver det muligt for læseren at stille sig kritisk overfor det materiale og den empiri der bliver fremlagt i afhandlingen.

Der indgår som tidligere nævnt semistrukturerede interviews, som består af åbne spørgsmål, hvilket sikrer at respondenterne ikke vil blive begrænset i sine svar. Hertil er udarbejdet et operationaliseringsskema, som fungerer som interviewguide. Disse interviewguides skal anvendes som rød tråd til interviews. Det skal dog gøres klart at respondenten ikke vil blive holdt tilbage i sine svar, også selvom dette ikke har umiddelbar tilknytning til det stillede spørgsmål, hvorfor spørgsmålene i interviewguides

[28]Andersen, 2014. s. 80-81

ikke nødvendigvis bliver stillet i rækkefølge. Nedenstående er udsnit af interviewguide som anvendes til Respondent C, databehandler:

Emneområde	Interviewspørgsmål	Forventet output
Introduktion	Vil du give en kort præsentation af jer	Introduktion til virksomhedens arbejdsopgaver, størrelse, historie osv.
Introduktion	Vil du kort præsentere dig selv og din baggrund	Hvem er respondenten og hvad er forudsætningerne og kendskab til at arbejde med GDPR
GDPR	Hvilke personoplysninger behandler i forbindelse med jeres lønadministration	Behandles der personoplysninger efter artikel 6,9 eller 10 i henhold til forordningen
GDPR	Hvor meget fylder GDPR i jeres daglige arbejde	Overvejer databehandler GDPR i den daglige drift
GDPR	Hvor meget fylder GDPR i den løbende dialog med jeres kunder	Er dataansvarlige interesserede i at få indsigt omkring GDPR fra deres databehandler
GDPR	Oplever du at kunderne er nervøse i fobindelse med jeres behandling af personoplysninger	Har dataansvarlige tiltro til deres databehandler
GDPR	Hvilke risici oplever i at der er forbundet med at behandle personoplysninger på vegne af kunder	Fylder ansvaret som databehandler noget i risikovurderingen
GDPR	Har jeres vurdering af risikobilledet af behandling af personoplysninger ændret sig efter at GDPR er trådt i kraft (25. maj 2018)?	Hvilken effekt har forordningen haft i riskovurderingen
GDPR	Hvilke udfordringer er der i forbindelse med aftaleindgåelsen i henhold til databehandleraftaler?	Hvor oplever databehandler problematikker i indgåelse af databehandleraftaler, jf. artikel 28.
GDPR/Revision	Hvad efterspørger kunderne for at få overbevisning om at i er compliant med databehandleraftalen	Hvad efterspørger dataansvarlig for at overholde artikel 28.
GDPR/Revision	Hvordan forsikrer i jeres kunder om at i er compliant med Databehandleraftalen?	Hvordan hjælper databehandler dataansvarlig med at overholde artikel 28
Revision	Får i lavet revisorerklæringer til hjælp af forrige spørgsmål	Bliver revisorerklæringer benyttet vedr. GDPR compliance

Billede 1: Udsnit fra interviewguide til databehandler.
Kilde: Egen tilvirkning, bilag B

Billede 1 er kun et udsnit af interviewguiden for databehandleren, hvortil de komplette interviewguides med alle respondenter kan findes i bilag B. Interviewguiden er opbygget i tre kolonner, hvortil det er fastlagt hvilket emne det stillede spørgsmål omhandler, og hvad interviewer forventer at få svar om. Formålet med at have "Forventet output" er at interviewer kan afstemme respondentens svar, så der sikres at interviewer indsamler den relevante empiri. Selve operationaliseringsfasen er ikke en nødvendighed, da det godt kan lade sig gøre at afholde interviews og herefter analysere på disse. Dette kan dog skabe uhensigtsmæssigheder fordi man kan ende ud i en situation, hvor man har gennemført en hel interviewfase og det herefter er klart at den indsamlede data ikke kan anvendes i analysedelen, fordi de spørgsmål der er stillet ikke kan kobles sammen med problemformuleringen og teorien. Dette scenarie kan selvsagt også opstå hvis man har gennemgået en operationaliseringsfase. Det vil alt andet lige skabe nogle gode forudsætninger for relevant og brugbart data at foretage en operationalisering. Ved at læse sine spørgsmål kritisk igennem i henhold til problemformuleringen, inden man bevæger sig ud i felten

og begynder at interviewe, skaber man gode forudsætninger for indsamling af data som kan benyttes i den videre analyse og dermed konklusion på problemformulering.

De semistrukturerede interviews vil blive gennemført inden for nogle forholdsvis åbne rammer som tillader en fokuseret og dialogbaseret tovejskommunikation. På denne vis ender man naturligvis med en stor mængde af informationer når interviews er afsluttet med respondenterne. Disse interviews skal herefter bearbejdes og benyttes til analyse, vurdering og diskussion. Alle interviews er blevet lydoptaget for at kunne bearbejde disse og findes som bilag C. Når dataindsamlingen er fuldent, er det nødvendigt at gøre sig overvejelser omkring hvordan den indsamlede data skal fortolkes og analyseres. Hertil skal det fastlægges om der er nogle bagvedliggende overvejelser som skal tages med når respondenters svar inddrages i undersøgelsen. Til dette er der udarbejdet kildekritik om de enkelte respondenter, for at klarlægge hvor der kan være bias.

6.1 Kildekritik

For intervieweren er det en forudsætning at være kritisk overfor de svar som respondenterne giver for at opnå validitet og troværdighed og dermed høj kvalitet af data. Alt afhængig af hvem respondenten er, må det antages at dennes svar kan være påvirket af bias. Grundet dette vil der i nedenstående være en gennemgang af forhold interviewer skal være opmærksom på og være kritisk overfor når der stilles spørgsmål til den enkelte type af respondenter.

Respondent A, Advokat: Advokater kan have forskellige roller og arbejdsopgaver i forholdet mellem dataansvarlige og databehandlere. Advokater er en faggruppe som kan være behjælpelige i dataansvarliges tilsyn, og grundet dette, kan revisorer og advokater være i konkurrence med hinanden, hvorfor der kan være en tendens til at advokaten vil tale erklæringer ned, og sine egne ydelser op.

Respondent B og F, Dataansvarlig: Når der stilles spørgsmål til en dataansvarlig vedrørende dennes tilsynsforpligtelse, vil man muligvis kunne forvente svar hvor egne evner til at føre tilsyn effektivt overvurderes, da en dataansvarlig højst sandsynligt ikke vil se svagt på sig selv og dermed fremstå med at være i uoverensstemmelse med GDPR.

Respondent C, Databehandler: I interviewet med databehandler er det vigtigt at have for øje at pågældende virksomhed lever af at behandle data på vegne af kunder. Der kan være en formodning om at de selv mener at de lever op til alle deres forpligtelser. Herudover er det relevant at erklæringer ikke er gratis, hvorfor der kan være incitament som databehandler, til at fravælge dette grundet ressourcemæssige overvejelser. Derfor kan nogle svar tale imod erklæringer selvom der måske er et reelt behov for dette.

Respondent D og E, Revisorer: Revisorer kan i deres svar være påvirket af at deres daglige arbejde i høj grad er præget af at udarbejde og afgive erklæringer, hvorfor det som interviewer er vigtigt at have for øje at revisor kan være stærk tilhænger af erklæringer og vil muligvis argumentere for et større behov for erklæringer end der reelt er behov for.

6.2 Opsummering af operationalisering

I dette kapitel er der redegjort for hvordan data skal indsamles, og hvordan man går fra teori til praksis og til empiri. Det er vigtigt med en operationaliseringsfase, således at de interviews der skal foretages, vil være på et fuldstændigt grundlag og være nyttige til den videre undersøgelse. Til dette er der udarbejdet interviewguides som er baseret på den teoretiske ramme, og fungerer som rød tråd til interviews. Derudover er der belyst hvordan man som interviewer skal forholde sig til respondenter i henhold til forskellige bias. Alt der er gennemgået i de tidligere kapitler er med til at danne grundlag, for den analyse som foretages, og som skal forsøge at besvare den udarbejdede problemformulering som fremgår af afsnit 1.1. Der vil i de kommende kapitler være en gennemgang af de underspørgsmål der er fremlagt i afsnit 1.1, der har til formål at understøtte og udarbejde en konklusion til problemformuleringen.

7. Outsourcing og databehandlerkonstruktioner

Dette kapitel skal besvare Underspørgsmål 1: 'Hvilke overvejelser har en dataansvarlig i forbindelse med outsourcing, herunder GDPR og databehandleraftaler?', som har til formål at analysere og fastslå hvilke overvejelser en organisation har både i forbindelse med outsourcing generelt, og hvilke overvejelser outsourcing skaber i henhold til GDPR, databehandleraftaler og tilhørende forpligtelser. I kapitlet vil der blive redegjort for forholdet mellem en organisation og en leverandør. Inden der analyseres på forholdet mellem disse og overvejelser hertil, vil der undersøges generelle overvejelser til outsourcing. Når en organisation vælger at benytte sig af en leverandør er det hovedsageligt ikke pga. GDPR, men fordi organisationen typisk har et behov som en leverandør kan løse. Der kan være mange grunde til at en organisation vælger at outsource aktiviteter, hvortil der også er mange forskellige aktiviteter som kan outsources.

Der vil blive taget udgangspunkt i eksempler vedrørende en uddannelsesinstitution, hvortil Respondent B vil inddrages. Respondenten fortæller at det for en uddannelsesinstitution gælder at deres primære formål er at formidle undervisning og forskning, hvortil de i den forbindelse skal administrere studerende, undervisere, ansøgere og andre interne eller eksterne personer. Fælles for alle disse grupper af personer, er at der indgår mange forskellige personoplysninger omkring dem i de behandlingsaktiviteter, som foregår på en uddannelsesinstitution. På en uddannelsesinstitution vil der typisk være mange led i en administrationsproces, hvortil der kan indgå mange forskellige systemer med vidt forskellige formål. Dette kan være studieadministrative systemer, systemer til at foretage lønudbetalinger og systemer til at koordinere lokaler m.fl. For disse systemer skal en organisation overveje hvorvidt den selv vil varetage udviklingen og driften af disse, eller om der skal benyttes en leverandør. Når nogle organisationer vælger at outsource, skyldes dette typisk, som det er beskrevet i kapitel 3, at det er vurderet at en ekstern part vil kunne varetage en given funktion hurtigere, bedre og billigere end organisationen selv, hvilket også bekræftes af Respondent F:

Respondent F [12:29]
"Før vi begyndte at outsource alting gjorde vi alting selv, og det var meget dyrt og meget besværligt. Bl.a. havde vi en pensionskasse, hvor alle medarbejdere så fik oprettet en konto og vi så styrede tingene selv, det gjorde man i gamle dage i de finansielle virksomheder (…) og det administreres i dag af ham der Person A"

Citatboks 1

Respondenten kommer i Citatboks 1 ind på hvordan de grundet for høje omkostninger og besværlig administration har valgt at outsource deres pensionskasse. De områder der typisk outsources vil være områder som ikke ligger inden for organisationens egne kernekompetencer. For en uddannelsesinstitution vil det derfor ikke være oplagt at outsource undervisningen eller forskningen, men derimod at outsource udviklingen og driften af IT-systemer, da dette typisk vil være sekundære aktiviteter, som kun eksisterer for at understøtte det primære fokus på uddannelse og forskning. Når en organisation vælger at outsource er det typisk ikke GDPR som er det første organisationen overvejer. Respondent F forklarer hvordan medarbejdere i organisationen køber programmer efter behov, uden at indtænke behandling af personoplysninger:

Respondent F [23:18]

"Men nogle gange så er folk hurtige, de køber alt det der Surveymonkey og Mailchimp osv. når de skal sende et eller andet ud, og det duer jo ikke, det er jo sådan nogle amerikansk baseret firmaer, den ene af dem, jeg mener nok det er Mailchimp, de har sådan en Safe Harbor ordning[29], og så kan vi jo så acceptere det men ellers duer det jo ikke og så må de jo lukke det ned igen"

Citatboks 2

For organisationer og leverandører gælder også at den ydelse eller service der leveres ikke er behandling af personoplysninger, men at dette indgår som en del af ydelsen eller servicen som det også forklares af Respondent A:

Respondent A [27:19]

"Indtil 25. maj sidste år, så var behandling af personoplysninger bare sådan noget man gjorde, og det betød egentligt ikke noget. Det er de færreste virksomheder der handler om behandling af personoplysninger, langt de fleste virksomheder skal sælge nogle biler eller sko eller et eller andet noget og det er det der bekymrer dem. Og så har de nogle personoplysninger, det er rigtig rart, så kan de analysere på folk så de kan sælge noget mere. Det var slet ikke et issue, fordi det værste der kunne ske var at tilsynet kunne offentliggøre på hjemmesiden at man var utilfreds med et eller andet, så hvis man var rigtig uheldig fik man en bøde på 5.000 kr."

Citatboks 3

[29] Safe Harbor: Ordning for amerikanske virksomheder, som tillod at overførsler af ikke-følsomme personoplysninger kunne ske uden tilladelse. Ordningen er erklæret ugyldig af EU-domstolen i oktober 2015, jf. C-362/14, Schrems. Afløseren til Safe Harbor er Privacy Shield som er vedtaget juli 2016.

Ifølge respondentens udtalelse i Citatboks 3 har behandling af personoplysninger ikke fyldt meget hos organisationer før d. 25. maj 2018, da dette blot er en tilhørende del af deres hovedformål om at sælge biler eller sko. Dertil var bødestørrelserne også meget små, hvorfor det ikke gav anledning til store overvejelser til behandling af personoplysninger. Det må dog vurderes at grundet GDPR's ikrafttrædelse er behandling af personoplysninger noget der skal overvejes når der indgås en aftale med en leverandør.

7.1 Hvornår er man databehandler?

Når en organisation vælger at outsource noget, hvad end det er drift og udvikling af IT-systemer eller en receptionsfunktion, kan der opstå overvejelser til GDPR. En organisation vil være dataansvarlig jf. artikel 4, pkt. 7 for organisationens registrerede. Dette skyldes at organisationen bestemmer formålet med behandlingen af personoplysninger, samt hvilke hjælpemidler, der skal understøtte denne behandling. Dertil vil en leverandør ofte blive gjort til databehandler jf. artikel 4, pkt. 8, da databehandleren handler på instruks fra den dataansvarlige. I få tilfælde kan en leverandør dog blive fælles dataansvarlig. I henhold til GDPR skal den dataansvarlige ved enhver behandling af personoplysninger behandle disse i overensstemmelse med princippet om ansvarlighed jf. artikel 5, stk. 2. Hertil vil en dataansvarlig skulle sikre sig at eventuelle databehandlere opfylder dette princip når de behandler personoplysninger på vegne af dem. Dette krav henledes til artikel 28, stk. 3, hvortil databehandleren skal bistå den dataansvarlige med at overholde sine forpligtelser. Det skal dog fastslås hertil, at ved benyttelse af en databehandler vil den dataansvarlige ikke outsource ansvaret for behandlingen, men kun selv behandlingsaktiviteten.

Outsourcing giver anledning til at organisationen afgiver kontrol til en leverandør. Dette medfører at en dataansvarlig skal overveje om der indgår personoplysninger i den outsourcede aktivitet og i så fald hvad risikoen er for de registreredes rettigheder og frihedsrettigheder. Ved benyttelsen af leverandører kan der opstå en databehandlerkonstruktion. For at vurdere om der opstår en databehandlerkonstruktion skal der overordnet vurderes om ydelsen eller en del af den ydelse der leveres, omfatter behandling af personoplysninger efter instruks fra og på vegne af en anden part. Den levererede ydelse eller service skal klart dreje sig om behandling af personoplysninger. En kommunes brug af et rengøringsfirma, på trods af denne bl.a. vil inkludere navn og adresse på personen der skal rengøres hos, vil som udgangspunkt ikke vil skabe en databehandlerkonstruktion. For at der opstår en databehandlerkonstruktion vil dette kræve at der skal være en databehandler og en dataansvarlig, hvorfor der for at konkludere om

der er en databehandlerkonstruktion, skal vurderes om der både er en databehandler og en dataansvarlig i henhold til den ydelse der leveres af en leverandør. For at blive identificeret som en databehandler er der flere forhold man kan lægge vægt på. Der lægges vægt på om personoplysninger bliver behandlet efter instruks, hvis ikke dette er tilfældet kan man ikke være databehandler. Dertil bestemmer en databehandler ikke selv formålet med behandlingen og bliver instrueret i hvilke hjælpemidler der må tages i brug til behandlingen. For at blive databehandler kræves det dermed at man handler efter instruks og at den anden part bestemmer formål og hjælpemidler. For at identificere om man er dataansvarlig kan vejledningen om dataansvarlige og databehandlere fra Datatilsynet inddrages[30]. Denne opstiller en række udsagn hvortil et "ja" til de følgende udsagn taler for at man er dataansvarlig ved behandling af personoplysninger. Omvendt vil et "nej" tale for at man ikke er dataansvarlig, og dermed er databehandler.

#	Udsagn
1.	Oplysningerne behandles kun til dine formål
2.	Den anden part behandler alene oplysninger på dine vegne.
3.	Du har ved lov eller lignende fået pålagt en opgave, som vedrører behandling af personoplysninger (f.eks. hvis du som kommune skal behandle ansøgninger om kontanthjælp).
4.	Aftalen eller en del af aftalen mellem dig og en anden part indeholder en direkte eller indirekte instruks om behandling af personoplysninger (modsat en aftale som alene retter sig mod levering af en anden ydelse).
5.	Den anden part skal varetage en opgave, som i princippet kunne have været udført af dig selv (modsat en ydelse, som kun lovligt kan foretages af den anden part).
6.	Du har instrueret den anden part i, hvordan oplysningerne skal behandles.
7.	Den anden part kan lovligt følge en instruks fra dig.
8.	Det er alene dig, der træffer afgørelse om formål og væsentlige hjælpemidler, herunder behandlingsskridt som indsamling, videregivelse, sletning og anvendelse af underdatabehandlere.
9.	Den anden part udfører ingen af ovenstående behandlingsskridt, medmindre det er aftalt med eller godkendt af dig.
10.	Du fører kontrol med, at den anden part behandler oplysningerne som aftalt.
11.	De personer, der behandles oplysninger om, har en klar forventning om, at du er ansvarlig for behandlingen.
12.	Du kan kræve oplysningerne tilbageleveret eller slettet hos den anden part, hvis du ikke længere ønsker, at den anden part skal behandle oplysningerne.

Tabel 5: Udsagn ved vurdering af, om en organisation er dataansvarlig eller databehandler.
Kilde: Datatilsynets vejledning om dataansvarlige og databehandlere s. 11-12

Nogle udsagn i Tabel 5 vægter dog mere end andre i vurderingen af om man er dataansvarlig eller ej. Eksempelvis vil et "ja" til nr. 3 eller 8 betyde at man er dataansvarlig, mens et "ja" til nr. 10 ikke nødvendigvis vil betyde at man bliver dataansvarlig. Dette kan også blive gjort, hvis man som

[30] Link til Datatilsynets vejledninger, herunder "Dataansvarlige og databehandlere":
https://www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger-og-skabeloner/

databehandler, fører kontrol med en underdatabehandler. Hvis det vurderes at der er en databehandlerkonstruktion med en leverandør, er der krav til at der udarbejdes en databehandleraftale jf. GDPR artikel 28, stk. 3, hvori der er oplistet minimumskrav til indholdet af en sådan aftale. Databehandleraftalen regulerer hvilke forpligtelser hver part i aftalen har ved behandling af personoplysninger. Forholdene som aftalen regulerer, har til formål at den dataansvarlige kan opfylde sin forpligtelse om ansvarlighed. Da man ved outsourcing afgiver kontrol, er det nødvendigt for den dataansvarlige at kontrollere sin databehandler for om de handler i overensstemmelse med det aftalte, så ansvarligheden kan opretholdes.

7.2 Delkonklusion

Der er i dette kapitel redegjort for hvordan en databehandlerkonstruktion opstår, og hvad der skal indgå af overvejelser såfremt en organisation vælger at outsource aktiviteter. Typisk er det primære formål med outsourcing ikke behandling af personoplysninger, men kommer ofte som følge af den aktivitet som bliver outsourcet, hvortil at en organisation skal have dette med i sine overvejelser ved indgåelse af en aftale med en leverandør. Ved at outsource en aktivitet afgives samtidig kontrol, hvorfor det er nødvendigt at følge op på det outsourcede.

I de efterfølgende kapitler vil der blive undersøgt nærmere hvilke forpligtelser en databehandler har når der bliver indgået en databehandleraftale, samt hvordan en dataansvarlig skal kontrollere at databehandleren overholder det aftalte.

8. Efterlevelse af en databehandleraftale

I det forrige kapitel er der gennemgået hvilke overvejelser der opstår ved outsourcing. Til dette kapitel vil Underspørgsmål 2: 'Hvordan efterlever en databehandler den indgåede databehandleraftale?' blive besvaret. Det skal undersøges hvordan en databehandler efterlever den indgåede databehandleraftale for at imødekomme overvejelser og bekymringer den dataansvarlige måtte have i forbindelse med outsourcing. Databehandlerens forpligtelser vil blive analyseret med udgangspunkt i Datatilsynets standarddatabehandleraftale[31]. Det er vigtigt at klarlægge de forpligtelser og det ansvar en databehandler har i forbindelse med indgåelse af en databehandleraftale, førend der kan fastslås hvad et tilsyn skal indeholde som bliver gennemgået i kapitel 9.

8.1 Databehandleraftalen

Det er et krav at der skal foreligge en databehandleraftale såfremt der ved outsourcing indgår behandling af personoplysninger jf. GDPR artikel 28, stk. 3. Til at analysere databehandlerens ansvar vil der både blive inddraget relevante artikler fra GDPR og Datatilsynets standarddatabehandleraftale. Datatilsynets standarddatabehandleraftale benyttes til analysen fordi den kommer fra tilsynsmyndigheden i Danmark, hvorfor det må antages at have en bred benyttelse i samfundet. Respondent A bliver ligeledes spurgt ind til om denne bliver benyttet:

Respondent A [53:53]
"Ja jeg ser den, rundt omkring, minder meget om vores egen, men selvfølgelig når de store leverandører skal ud med det så har det taget sådan en som denne her og pillet lidt i det (…) Den er dækkende, kan man sige, den kommer jo hele vejen rundt."

Citatboks 4

I Citatboks 4 fortæller Respondent A, at Datatilsynets standarddatabehandleraftale bliver brugt og forklarer at den minder meget om de databehandleraftaler de selv bistår med, hvorfor det vurderes at der er bred benyttelse af Datatilsynets version. Det må dog fastslås at det ikke er et krav at benytte Datatilsynets standarddatabehandleraftale. Kravet til en databehandleraftale er at den foreligger skriftligt, herunder elektronisk og opfylder kravene i henhold til GDPR artikel 28, stk. 3. Ansvaret for behandling

[31] Datatilsynets standarddatabehandleraftale fremgår af bilag D.

af personoplysninger er altid hos den dataansvarlige, men databehandleren har også forpligtelser i henhold til behandlingen, hvor disse primært er reguleret i en databehandleraftale. I en databehandleraftale skal fremgå en række krav og forpligtelser som hver part henholdsvis er ansvarlig for.

8.1.1 Opbygning af Datatilsynets standard databehandleraftale

Datatilsynets standarddatabehandleraftale er bygget op med først en generel del fra side 1 til 11, som udover navnene på parterne og hovedaftalen ikke bør tilrettes, da dette skal ses som en standardtekst, som ikke være nødvendigt at ændre fra aftaleforhold til aftaleforhold. Efterfølgende indeholder side 12 til 20 den specifikke del og bilag, som skal udfyldes særskilt for hvert aftaleforhold og ydelse der leveres. Denne del af aftalen skal indeholde nærmere beskrivelser om behandlingen, behandlingssikkerheden, og evt. underdatabehandlere samt aftale om procedurer for tilsyn. Der er hertil også mulighed for at tilpasse enhver anden aftaleretlig regulering som parterne finder relevant, eksempelvis regres[32] og ansvarsbegrænsning. I standarddatabehandleraftalen er noget af teksten markeret fed, hvilket er tekst, som efter Datatilsynets opfattelse er afgørende for databehandleraftalens gyldighed og opnåelse af minimumskravene i henhold til GDPR artikel 28, stk. 3[33]. Denne tekst bør kun slettes hvis den erstattes af en anden ordlyd med samme materielle indhold. Derudover er noget tekst markeret med gult, hvilket kræver udfyldelse førend aftalen er gyldig. Skabelonen har behov for at blive tilpasset til den enkelte aftale og det specifikke formål og databehandling som outsources. Dertil er der den resterende tekst som hverken er fed eller gul. Dette er tekst, som efter Datatilsynets opfattelse ikke er nødvendigt at have med i aftalen, men kan hjælpe med at dokumentere overholdelsen af andre bestemmelser i GDPR.

8.1.2 Databehandlerens forpligtelser i henhold til aftalen

De forpligtelser som databehandleren bliver underlagt igennem Datatilsynets standarddatabehandleraftale (herefter "aftalen") bliver herunder gennemgået og analyseret. Forpligtelserne som databehandleren er underlagt ifølge aftalen er oplistet herunder:

- Handle efter instruks
- Sikre fortrolighed
- Sikre behandlingssikkerhed
- Betingelser for anvendelse af underdatabehandlere

[32] Regres er et betalingskrav som fremsættes af en skyldner eller kautionist over for en eller flere andre personer.
[33] Jf. følgetekst til Datatilsynets standard databehandleraftalen side 2.
https://www.datatilsynet.dk/media/6812/databehandleraftale_-_foelgetekst.pdf

- Overførsel af oplysninger til tredjelande eller internationale organisationer
- Bistand til den dataansvarlige
- Underretning om databrud
- Sletning og tilbagelevering af oplysninger
- Tilsyn og revision

Handle efter instruks

Databehandlerens opgave er som beskrevet at varetage en eller flere behandlingsaktiviteter på vegne af en dataansvarlig. Hjemlen til denne behandling ligger hos den dataansvarlige jf. aftalens afsnit 3, stk. 3. Hertil er der i aftalens afsnit 4, stk. 1, reguleret at en databehandler udelukkende handlinger efter instruks. Databehandleren er forpligtet til at informere den dataansvarlige, hvis de mener at en instruks kan være i strid med GDPR eller andre relevante databeskyttelsesbestemmelser jf. afsnit 4, stk. 2. Disse punkter i aftalen stemmer overens med GDPR artikel 28 stk. 3, litra a. Førend en databehandler kan efterleve afsnit 4 i aftalen kræves der, at denne sikrer sig at der foreligger en dokumenteret instruks fra den dataansvarlige der omfatter de enkelte behandlingsaktiviteter. At handle efter instruks som databehandler bliver forklaret af Respondent C, som kommer ind på hvordan deres organisation, som databehandler, normalt ikke benytter sig af USB-stik til udveksling af oplysninger. Grundet et krav fra en kunde, den dataansvarlige, gjorde organisationen det alligevel, fordi de handlede efter instruks. Respondenten udtaler:

Respondent C [24:31]
"*Vi handler jo på instruks fra vores kunder, så hvis vi har en kunde der siger det vil jeg skide på, i skal sende mig et usb stik så gør vi det, så noterer vi det i det vi kalder exception*."

Citatboks 5

I situationen i Citatboks 5 er det vurderet internt i Respondent C's organisation, at USB-stik som udgangspunkt ikke benyttes af sikkerhedsmæssige årsager. Grunden til at organisationen alligevel kan acceptere dette, er fordi der i GDPR ikke stilles absolutte krav til sikkerhed, hvorfor det er op til en dataansvarliges egen risikovurdering om USB-stik kan eller skal benyttes.

Sikre fortrolighed

Fortrolighed er reguleret i aftalens afsnit 5. Der fremgår krav om at databehandleren skal sikre at de personer, som er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, er underlagt en lovbestemt tavshedspligt, som stemmer overens til GDPR artikel 28, stk. 3, litra b. Efter almen

praksis indarbejdes en sådan tavshedspligt ofte i medarbejderes ansættelseskontrakter, og selv i de tilfælde, hvor dette ikke indgår i en ansættelseskontrakt, vil en medarbejder stadig være pålagt en sådan tavshedspligt[34]. Fortrolighed er et bredt begreb og dækker ikke kun information ud af organisation, men skal også sikres internt i organisationen hvortil kun de medarbejdere som har et legitimt og arbejdsbetinget behov med behandling af personoplysninger har adgang til disse oplysninger.

For at leve op til forpligtelsen om at sikre fortroligheden kan en databehandler indføre flere forskellige tiltag. En databehandler kan bl.a. indføre adgangsstyring, både til de fysiske lokaler og tekniske blokeringer i IT-systemerne, for at sikre at kun relevante medarbejdere har adgang. Herudover kan der også indføres politikker omkring generel adfærd for medarbejdere. Disse politikker kan omhandle at medarbejderne skal låse eller slukke deres computere når de forlader den, have et rent skrivebord når dagen er slut samt at medarbejdere skal overveje hvad der bliver sagt når man er ude i det offentlige rum og benytte privacy filtre. Disse politikker skal være nedskrevet i databehandlerens persondatapolitik og derudover bør personalehåndbogen for alle medarbejdere indeholde en henvisning til persondatapolitikken. Disse tiltag vil kun være effektive såfremt medarbejderne er bevidste om at de findes, som eksempelvis kan ske igennem intern undervisning. En måde hvorpå databehandleren kan skabe opmærksomhed på de interne politikker er gennem obligatoriske e-learnings forløb. Respondent C nævner i det følgende at medarbejdere i deres organisation får differentieret undervisning, for at sikre at de er klar over indvirkningen af deres specifikke arbejdsopgaver i henhold til bl.a. fortrolighed:

Respondent C [26:30]
"Vi har awareness (...) for nye medarbejdere (...) vores udviklere skal jo have en anden uddannelse end vores sælgere(...) vores kundekonsulenter som sidder med fingrene nede i folks data skal have en anden uddannelse end vores bogholderi som kun arbejder med kundeoplysninger (...) en differentieret uddannelse."

Citatboks 6

Af Citatboks 6 fremgår det at databehandleren sørger for at de relevante medarbejdergrupper får den uddannelse der passer til deres arbejdsopgaver, for at sikre behandlingen af personoplysninger. De gennemgåede tiltag hjælper både enkeltvis og sammen til at skabe fortrolighed og integritet, som er krævet i henhold til aftalen og de GDPR's grundlæggende principper om fortrolighed og integritet.

[34]HK om tavshedspligt: https://www.hk.dk/aktuelt/temaer/du-har-altid-loyalitets-og-tavshedspligt-paa-job

Behandlingssikkerhed

I aftalens afsnit 6 er det reguleret at databehandleren skal iværksætte foranstaltninger som kræves i henhold til GDPR artikel 32. Denne artikel er tidligere redegjort for i afhandlingens afsnit 4.4.3 og omhandler bl.a. pseudonymisering, kryptering, tilgængelighed og løbende test af disse. Databehandlere er forskellige og foretager varierende typer af behandling af personoplysninger, hvorfor det altid vil være op til en konkret risikovurdering hvor gennemgribende et sikkerhedsniveau en databehandler skal have. Er der eksempelvis tale om lagring og behandling af straffeoplysninger i henhold til GDPR artikel 10, vil der være krav om et højt sikkerhedsniveau. I det tilfælde hvor der udelukkende er tale om behandling af e-mailadresser for folketingsmedlemmer, som i forvejen ligger offentligt, vil være tilstrækkeligt med et lavere sikkerhedsniveau. Førend en databehandler kan efterleve dette afsnit i aftalen, er det nødvendigt at identificere hvilke mulige trusler der kan ramme organisationen og hvordan disse bedst muligt kan mitigeres. Trusler kan eksempelvis være hackere, ransomware[35] eller social engineering[36]. Respondent C nævner hvordan de tidligere har været ramt af ransomware og pga. dette ikke tillader medarbejdere at benytte deres egne enheder:

Respondent C [20:51]

"*Så derfor har vi også nogle særlige foranstaltninger, i forhold til vores pc'er, altså herinde er der ikke noget der hedder bring your own device, altså vi vil ikke have folks egne devices knyttet op på vores systemer*."

Citatboks 7

Som beskrevet i Citatboks 7 om at nægte medarbejderes egne enheder på arbejdspladsen, er dette blot en af flere tiltag som en databehandler kan implementere for at imødekomme kravet om behandlingssikkerhed. Ved at nægte medarbejdernes egne enheder øger det kontrollen hos databehandleren, og er med til at sikre at uønskede programmer som kan være kompromitterede ikke installeres på databehandlerens netværk. Mellem en databehandler og en dataansvarlig vil der ofte blive udvekslet meget data, hvorfor der kan være et behov for en sikker måde at sende dette på som eksempelvis kan være krypterede e-mails eller lukkede portalløsninger. Respondent C fortæller:

[35] Ransomware: En form for ondsindet software, som er designet til at låse eller nægte adgang til en computer indtil en løsesum (ransom) er betalt.
[36] Social engineering: Brugen af bedrag og udnyttelse af menneskelige tiltro og til at manipulere individer til at oplyse fortrolig information eller personlig information som kan bruges til kriminelle formål.

Respondent C [24:51]

"Der har vi jo et krypteret område hos os hvor kunderne kan logge ind og så kan de selv hente data derinde fra."

Citatboks 8

Til udveksling af data har de i Respondent C's organisation jf. Citatboks 8 implementeret en løsning med en krypteret dataudvekslingsportal for at sikre integriteten af personoplysninger. Yderligere kan en databehandler følge med i markedet og se hvilke trusler som også kan være menneskelige fejl, der opstår, som det også forklares af respondenten:

Respondent C [25:10]

"Hvor tidligere var vi måske lidt mere fleksible med at sende det på et eller andet device men vi lærer jo også af andres erfaringer, vi kigger jo efter så når en cd-rom med helbredsoplysninger pludselig er hos den kinesiske ambassade, eller hvor det nu var."

Citatboks 9

Respondent C henviser i Citatboks 9 til en sag fra 2016, hvor ukrypterede CD-rommer med helbredsoplysninger[37] (følsomme personoplysninger jf. GDPR artikel 9) fra Statens Serum Institut ved en fejl blev leveret til en kinesisk virksomhed[38]. Efterfølgende har databehandleren som udgangspunkt stoppet med at udveksle data med USB-stik af frygt for at ende i samme situation som Statens Serum Institut. Der er mange tiltag der kan implementeres for at sikre behandlingssikkerheden, men i sidste ende skal der altid foretages en risikovurdering af de registreredes rettigheder og frihedsrettigheder.

Betingelser for anvendelse af underdatabehandlere

Ved brug af underdatabehandlere er udgangspunktet at disse ikke må benyttes uden forudgående godkendelse fra den dataansvarlige jf. aftalens afsnit 7, stk. 2. I praksis betyder dette at der i aftalen skal indgå et bilag over de på forhånd godkendte underdatabehandlere, da det er de færreste databehandlere, som ikke benytter sig af underdatabehandlere. For at en databehandler kan leve op til forpligtelserne i aftalens afsnit 7 kræves der som nævnt at databehandleren har fået skriftlig godkendelse fra den dataansvarlige, samt at denne lever op til forpligtelserne i henhold til GDPR artikel 28 stk. 2. og

[37] Helbredsoplysninger: Personoplysninger, der vedrører en fysisk persons fysiske eller mentale helbred, herunder levering af sundhedsydelser, og som giver information om vedkommendes helbredstilstand, jf. GDPR artikel 4, stk. 15.
[38] Link til artikel om sagen: https://www.dr.dk/nyheder/viden/tech/eksperter-om-cpr-laek-amatoeragtig-omgang-med-data

4, som pålægger en underdatabehandler de samme forpligtelser som databehandleren selv er pålagt over for den dataansvarlige.

I Datatilsynets standarddatabehandleraftale vil betingelser for brug og eventuelle underdatabehandlere være aftalt i bilag B. Hvis den dataansvarlige ikke accepterer de underdatabehandlere som en databehandler mener er nødvendige, kan konsekvensen være at en aftale bliver forkastet, eller at en aftale leveres med manglende funktionalitet. Et eksempel på anvendelse af underdatabehandlere og tilhørende funktionalitet kan ses i Danløns databehandleraftale[39], hvoraf det af Appendiks 2 fremgår at Danløn samarbejder med Post Danmark A/S, som muliggør udsendelse af lønsedler via E-boks. Det vigtige for dette afsnit i aftalen er dermed at den dataansvarlige godkender de underdatabehandlere som databehandleren vil benytte.

Overførsel af oplysninger til tredjelande eller internationale organisationer

I forlængelse af brug af underdatabehandlere er det vigtigt at være opmærksom på, at hvis en databehandler ønsker at overføre oplysninger til tredjelande eller internationale organisationer, så skal dette være aftalt med den dataansvarlige. I aftalens afsnit 8, stk. 1 er udgangspunktet at overførsler til tredjelande ikke er tilladt, medmindre det er påkrævet af EU eller national ret, hvortil databehandleren skal informere den dataansvarlige, hvis dette er tilfældet. I alle andre tilfælde skal det være aftalt i bilag C hvilke overførsler til tredjelande der er godkendt af den dataansvarlige. Det er dog stadig vigtigt at have for øje at førend en databehandler kan overføre personoplysninger til et tredjeland, skal der udover den dataansvarliges godkendelse også sikres at modtageren i tredjelandet kan stille den fornødne sikkerhed i overensstemmelse med GDPR.

I GDPR skelnes mellem sikre og ikke sikre tredjelande. EU-kommissionen fastlægger hvilke lande der betragtes som sikre[40]. For de sikre lande vil der ikke være et særskilt krav om godkendelse af overførsler, udover at disse skal godkendes som underdatabehandler, hvorfor udgangspunktet er, at den fornødne sikkerhed er tilstede. For de usikre tredjelande kræves særskilt hjemmel førend der må overføres personoplysninger. Behandlingshjemlerne omfatter bl.a. EU's standardkontraktbestemmelser (også

[39] Link til Danløns databehandleraftale https://www.danlon.dk/databehandleraftale/
[40] EU-kommissionens liste over sikre tredjelande forefindes på følgende hjemmeside: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

kendt som "EU's modelklausuler") og Privacy Shield[41]. EU's modelklausuler findes i tre udgaver, hvoraf to af disse udgaver vedrører overførsler fra dataansvarlig til dataansvarlig og den sidste udgave vedrører dataansvarlig til databehandler. Klausulerne forpligter parterne til at handle i overensstemmelse med GDPR. EU's modelklausuler kan og vil ofte indgå som en del af en drift- eller outsourcing kontrakt. Hvis man som databehandler overfører personoplysninger til et usikkert tredjeland, skal den sidstnævnte EU modelklausul benyttes[42]. Privacy Shield er en selvcertificeringsordning som amerikanske virksomheder kan tilslutte sig. Ordningen kræver at virksomhederne skal overholde regler der sikrer en passende beskyttelse af personoplysninger fra EU/EØS. Krav til at blive certificeret omfatter bl.a. en række principper om gennemsigtighed, sikkerhed, formålsbegrænsning og beskyttelse af de registreredes rettigheder samt en række supplerende principper om eksempelvis følsomme personoplysninger. De stillede krav til Privacy Shield certificeringen antages at være i overensstemmelse med de grundlæggende principper i GDPR. Ved benyttelse af EU's modelklausul, eller en underdatabehandler som er certificeret via Privacy Shield, kan en databehandler sikre sig at en overførsel til et tredjeland ikke er i strid med GDPR og at underdatabehandleren er underlagt de samme forpligtelser som databehandleren selv og dermed sikrer den fornødne sikkerhed. Det antages for begge metoder at disse sikrer tilstrækkelig sikkerhed for de registrerede, i kraft af at de er godkendt af EU som gyldige overførselsgrundlag, hvorfor der ikke vil foretages en analyse af deres tilstrækkelighed.

Visma e-conomic[43] benytter sig bl.a. af disse metoder, hvortil de har en udspecificeret liste af deres underleverandører og deres funktion[44]. Det fremgår at Visma e-conomic benytter Privacy Shield i forbindelse med AskNicely fra New Zealand og USA, som er underleverandør i forbindelse med spørgeskemaer. Derudover benytter de sig af EU's modelklausul til Ciklum fra Ukraine, som er en underleverandør der benyttes til udvikling. For at sikre sig at overførsler til tredjelande eller internationale organisationer sker i overensstemmelse med GDPR skal databehandleren undersøge om modtageren er omfattet af Privacy Shield, eller alternativt benytte sig af EU's modelklausul.

[41] Link til Privacy Shield: https://www.privacyshield.gov/welcome
[42] Link til EU's modelklausul til dataansvarlig og databehandler: http://data.europa.eu/eli/dec/2010/87/oj
[43] Visma e-conomic er leverandør af det online regnskabssystem e-conomic.
[44] Link til Visma e-conomic liste over underdatabehandlere:
https://www.e-conomic.dk/sikkerhed/persondata/underleverandoerer

Bistand til den dataansvarlige

Afsnit 9 i aftalen omhandler databehandlerens forpligtelse til at bistå den dataansvarlige med at imødekomme sine forpligtelser i forhold til de registrerede. De registreredes rettigheder fremgår af kapitel 3 i GDPR som bl.a. omfatter indsigtsret, berigtigelsesret m.m. Databehandlerens forpligtelse er med til at sikre at de grundlæggende principper bliver overholdt af den dataansvarlige. En dataansvarlig som benytter sig af databehandlere vil højst sandsynligt ikke ville kunne imødekomme de registreredes rettigheder uden bistand fra deres databehandlere, da disse ligger inde med data om de registrerede.

Bistand til den dataansvarlige omfatter også tilfælde af databrud, hvor databehandleren skal assistere den dataansvarlige med dennes forpligtelser i henhold til GDPR artikel 32-36. Dette omfatter behandlingssikkerhed, underretningspligt, konsekvensanalyse og forudgående høring. I aftalens afsnit 10 er der udarbejdet et særskilt afsnit om underretning om brud på persondatasikkerheden, selvom dette allerede indgår i artikel 33 og 34, og derfor allerede er omtalt i aftalens afsnit 9.

Underretning om brud på persondatasikkerheden

Den dataansvarliges pligt til at underrette tilsynsmyndigheden og de registrerede i tilfælde af databrud er beskrevet i afhandlingens afsnit 4.4.3. I henhold til databrud har databehandleren en forpligtelse til at bistå hvis der opstår et databrud. I afsnit 10 er der reguleret hvordan en databehandler skal agere i en situation hvor der opstår et databrud med hensyn til underretning til både tilsynsmyndigheden, jf. GDPR artikel 33, og de registrerede, jf. GDPR artikel 34. Det er i dette afsnit aftalt hvor lang tid databehandleren har til at underrette den dataansvarlige om et databrud. Hvorvidt et databrud skal underrettes til Datatilsynet er op til den dataansvarlige, da de bærer ansvaret for behandlingen og databehandleren kun arbejder efter instruks. Respondent C forklarer deres procedure for håndtering af databrud:

Respondent C [23:51]

"Det vi gør, hvis vi finder ud af at der er et læk, vi har sådan en privacy incident procedure, og det første vi gør det er jo at orientere kunder, nu skal i høre den her har fået den her og så er det jo kunderne der skal vurdere om det er noget man vil fortælle Datatilsynet, det er jo ikke os. Altså vi har forpligtelsen til at lynhurtigt og orientere om at der er sket en eller anden form for incident og så arbejde videre sammen med kunderne og lad det være op til dem at lave vurderingerne."

Citatboks 10

Det forklares i Citatboks 10 at databehandleren har pligt til at underrette den dataansvarlige, men fastslår samtidig at det er den dataansvarlige, som skal foretage en vurdering om hvorvidt disse databrud skal indberettes til Datatilsynet. Et eksempel på dette forklares af Respondent F, da de som dataansvarlige i deres organisation oplevede et databrud hos en databehandler. Respondent F fortæller:

Respondent F [25:56]

"Leverandør xx havde på et tidspunkt et problem, hvor de i forbindelse med en opdatering, kom de til at give forkerte adgange, sådan så alle fik alle adgange. Så skrev de så ud til mig at nu skulle jeg være opmærksom på at dem inden hos os der havde begrænset adgang, de havde fået fuld adgang i en periode, jeg mener det var 2 måneder, det undskyldte de så osv. og de havde anmeldt det til Datatilsynet og vi skulle måske det samme, de aner ikke hvad vi foretager os, det er et lukket system for dem, og så gik vi ind og undersøgte det og så viste det sig at alle, vi har kun 2 medarbejdere som bruger den løsning, de havde begge 2 fuld adgang i forvejen."

Citatboks 11

Databehandleren fulgte sin forpligtelse om at underrette den dataansvarlige, som forklaret i Citatboks 11 vurderede at bruddet ikke havde betydning for de registrerede, hvorfor der ikke blev foretaget yderligere. For at en databehandler kan efterleve dette afsnit i aftalen stilles der krav til at det bliver indberettet til den dataansvarlige uden unødig forsinkelse, hvortil der aftales et konkret timeantal. Såfremt den dataansvarlige indberetter databrud til tilsynsmyndigheden, skal databehandleren bistå den dataansvarlige i dennes forpligtelser med rapporteringen og videregive de nødvendige oplysninger efter GDPR artikel 33, stk. 3.

<u>Sletning og tilbagelevering ved tjenesternes ophør</u>

I afsnit 11 i aftalen fastlægges hvilke forpligtelser databehandleren har til at slette og tilbagelevere oplysninger til den dataansvarlige når aftalen ophører.

<u>Tilsyn og revision</u>

I aftalens afsnit 12 fremgår det at databehandleren har pligt til at bistå den dataansvarlige i dennes tilsynsforpligtelse efter GDPR artikel 28. I praksis kan tilsynsforpligtelsen være at den dataansvarlige selv kommer ud og kontrollerer databehandleren, hvortil der findes alternativer som at databehandleren får udarbejdet revisorerklæringer som herefter udleveres til den dataansvarlige. Det er i afhandlingens fo-

kus hvordan den dataansvarlige skal sikre sig at databehandleren efterlever den indgåede databehandleraftale. Dette sker i forbindelse med tilsyn hos databehandleren, hvilket vil blive analyseret dybdegående i det næste underspørgsmål.

Parternes aftaler om andre forhold og ikrafttræden og ophører

Afsnit 13 i aftalen indeholder en henvisning til bilag D, som er alle andre forhold som den dataansvarlige og databehandleren kan have indgået. Hertil indeholder aftalens afsnit 14 regulering om ikrafttræden og ophør af aftalen.

8.2 Delkonklusion

I dette kapitel er der gennemgået hvilke forpligtelser en databehandler har ud fra Datatilsynets standarddatabehandleraftale. Det er relevant at bemærke at databehandleren handler efter instruks, hvorfor ansvaret for behandlingen af personoplysninger er hos den dataansvarlige. Dertil er databehandleren forpligtet til at bistå den dataansvarlige med at sikre fortrolighed, behandlingssikkerhed og generelt bistå med den dataansvarliges forpligtelser til de registreredes rettigheder og frihedsrettigheder samt at de grundlæggende principper bliver efterlevet. Hertil skal databehandleren bistå i den dataansvarliges forpligtelser overfor tilsynsmyndigheden, herunder i tilfælde af et databrud. Kravet om at databehandleren skal stille de fornødne garantier overfor en dataansvarlig medfører at databehandleren skal implementere organisatoriske og tekniske tiltag, hvoraf disse bl.a. kan være uddannelse i behandling af personoplysninger, adgangsstyring og tekniske foranstaltninger som kryptering af dataudveksling. Disse tiltag er med til at sikre de grundlæggende principper om integriteten og fortroligheden af personoplysninger. For benyttelse af underdatabehandlere og overførsel til tredjelande og internationale organisationer gælder samme hjemmel, at den dataansvarlige skal have godkendt dette. Hertil kan metoder som Privacy Shield og EU's modelklausul benyttes til at sikre overførsler til tredjelande og internationale organisationer. Afslutningsvis er det i aftalen reguleret at data skal slettes og tilbageleveres når brugen af tjenesterne ophører, samt at databehandleren skal bistå den dataansvarlige i dennes tilsynsforpligtelse.

I analysen er der taget udgangspunkt i Datatilsynets standarddatabehandleraftale. Hertil skal det bemærkes at aftalen er en skabelon, hvorfor der altid skal foretages en vurdering om hvilke afsnit, der skal tilpasses. Bilagene skal også udfyldes for de enkelte aktiviteter, hvor konkrete forhold som det ønskede sikkerhedsniveau og underdatabehandlere reguleres.

Dette henleder til det næste kapitel hvortil der undersøges hvordan en dataansvarlig kan sikre sig at en databehandler efterlever den indgåede databehandleraftale, hvorfor det har været relevant at redegøre for hvilke forpligtelser databehandleren er underlagt. Dette skyldes at det ikke er muligt at vurdere om en part efterlever en aftale, hvis det ikke først er klart hvad denne aftale indebærer og dermed hvad der skal efterleves.

9. Den dataansvarliges tilsynsforpligtelse

Dette kapitel skal besvare Underspørgsmål 3: 'Hvordan skal en dataansvarlig sikre sig at dennes databehandler efterlever den indgåede databehandleraftale?'. Som det er beskrevet i afhandlingens afsnit 4.5, skal en dataansvarlig ved anvendelse af en databehandler sikre sig at databehandleren kan stille de fornødne garantier. Dette gælder ikke blot ved aftaleindgåelsen, men også under hele aftalens levetid, hvorfor det er nødvendigt at den dataansvarlige foretager opfølgning af dens databehandlere jf. GDPR artikel 28. Når der bliver indgået aftaler vil der opstå et principal-agent forhold, som beskrevet i afhandlingens afsnit 5.1. Forholdet opstår fordi principalen har en opgave, som denne ikke selv kan eller vil varetage og derfor uddelegerer det til agenten, som agerer på vegne af principalen. Dette er tilfældet når en databehandler handler efter instruks fra en dataansvarlig, som har uddelegeret en eller flere behandlingsaktiviteter. I en databehandlerkonstruktion mellem den dataansvarlige (principalen) og databehandleren (agenten) vil der mellem disse parter opstå asymmetrisk information og de kan have modstridende interesser og forskellige incitamenter. Der opstår derfor et behov for at få bekræftet at behandlingen sker i overensstemmelse med databehandleraftalen. Hertil har den dataansvarlige et behov for at mitigere informationsrisikoen og reducere den til et acceptabelt niveau. Det er nødvendigt at de dataansvarlige tager stilling til hvem i organisationen der er ansvarlige for at der bliver fulgt på databehandlere. Respondent F forklarer hvordan de i organisationen prøver på at gøre medarbejdere ansvarlige for at sikre, at der bliver taget stilling til hvilke risici der kan være ved at benytte en databehandler og om der bliver reageret på ændringer hertil.

Respondent F [21:21]

"Bare dem der sidder i forretningen og er ansvarlig for aftalen har en kontraktejer (...). Man kan jo aldrig outsource et ansvar prøver jeg at sige til folk. (…) Altså enten skal man vedgå sig at man flytter ud til leverandøren og holder øje med leverandøren eller må man finde ud af hvordan man kan sikre det internt og det kan man jo så gøre via nogle kontroller(…) der er jo så udpeget en persondataambassadør i alle afdelingerne, som har overblik over hvad de foretager sig og typisk er der jo ikke ændret noget, og nogle gange, en sjælden gang må de jo så sige, nå ja vi har jo så købt et eller andet."

Citatboks 12

Derudover forklarer Respondent F i Citatboks 12 at de også på den ene eller anden måde skal holde øje med leverandøren. Derudover er det i forbindelse med interviewet med Respondent B blevet konstateret, at nogle dataansvarlige ikke har faste procedurer for at føre tilsyn, men at disse bliver udført ad hoc.

Respondent B [40:56]
"Vi har ikke fået de første rapporteringer endnu og vi har ikke begyndt systematisk at føre kontrol endnu. Så der er også noget med at, få det løbet i gang, (…) så har det været fordi man har nogle oplevelser med en leverandør, så har vi gjort det sådan mere ad hoc."

Citatboks 13

Ud fra Citatboks 13 er der et behov for at fastslå hvordan de dataansvarlige skal vurdere, hvordan de skal sikre at deres databehandlere efterlever de indgåede databehandleraftaler. Det fremgår ikke med ordlyd i GDPR at en dataansvarlig skal føre et tilsyn med sine databehandlere. Dog må der kun benyttes databehandlere der kan stille de fornødne garantier, samt at de dataansvarlige skal leve op til det grundlæggende princip om ansvarlighed. Det må vurderes at en dataansvarlig ikke kan leve op til kravet om ansvarlighed, hvis der ikke føres tilsyn, som sikrer at den indgåede databehandleraftale overholdes og at de aftalte organisatoriske og tekniske sikkerhedsforanstaltninger efterleves af databehandleren. Tilsynet kan være af større eller mindre omfang afhængig af den konkrete databehandleraftale, og hvilke behandlingsaktiviteter der er outsourcet. Forskellige metoder at føre tilsyn på vil blive gennemgået i dette kapitel. Der vil herudover også blive undersøgt hvordan en dataansvarlig skematisk kan vurdere risici forbundet med den outsourcede behandlingsaktivitet. Risikovurderingen er individuel fra dataansvarlig til dataansvarlig, og skal baseres på hvad der outsources, kategorier af personoplysninger der behandles og mængden af personoplysninger der bliver behandlet på vegne af de registrerede m.m. Den dataansvarlige skal skabe sig et overblik og kan opstille en oversigt hvortil det gøres klart hvilke databehandlere der benyttes, hvilke risici der er vurderet hertil og hvilke tilsynshandlinger der skal foretages.

9.1 Tilsynsformer

Før udførelsen af et tilsyn er det nødvendigt at klargøre at et tilsyn kan komme i forskellige former og størrelser, afhængigt af hvor kompleks en databehandleraftale der er indgået, og hvor stor en risiko der er for de registrerede. Ved benyttelse af en databehandler er vurderingen op til den dataansvarlige.

Af Datatilsynets vejledning om tilsyn med databehandlere fremgår det at et tilsyn kan komme i to former[45]. Tilsynet kan både være i form af skriftlig informationsindsamling, hvor der eksempelvis sendes spørgsmål, der følger op på den outsourcede behandlingsaktivitet som sendes til databehandlere. Derudover kan tilsynet også være et fysisk besøg, hvor den dataansvarlige selv kommer på besøg hos databehandleren og påser behandlingssikkerheden ved inspektioner og eventuelle tests. Omfanget af disse metoder og kombinationen heraf vil afhænge af den dataansvarliges konkrete vurdering af risikoen for de registrerede. Hvis den dataansvarlige eksempelvis fastlægger en meget høj risiko, vil der både skulle udføres skriftlige informationsindsamlinger og fysiske besøg, det ene udelukker ikke det andet og skal i dette tilfælde være en kombination af begge former.

For de skriftlige informationsindsamlinger vil tilsynshandlinger typisk bestå af spørgeskemaer om de aftalte sikkerhedsforanstaltninger, løbende rapportering, dokumentation for overførselsgrundlag, dokumentation af databehandlerens tilsyn med underdatabehandlere m.m. Der er tale om næsten alt som kan indfanges i et skriftligt medie. Fordelene ved at udføre skriftlige informationsindsamlinger er at disse typisk vil være tidseffektive, da det kan udføres fra skrivebordet og at spørgeskemaer typisk ikke tager lang tid at besvare. Ulemperne er at der kan være en risiko for at man ikke identificerer nye risici, fordi man typisk vil tage udgangspunkt i de risici man allerede har identificeret. Derudover opnås der heller ikke meget troværdighed, da udsagn fra databehandlere typisk ikke kan eller vil blive kontrolleret for om de rent faktisk har hold i virkeligheden. Yderligere kan der også være risici som ikke kan mitigeres ved skriftlige bekræftelser fra databehandleren. Dette kan være ved behandling af følsomme personoplysninger eller meget komplekse databehandleraftaler, som involverer mange behandlingsaktiviteter, overførsler og underdatabehandlere. Den dataansvarlige har typisk ikke har kontakten til underdatabehandlerne, hvorfor det som udgangspunkt ikke vil være tilstrækkeligt med skriftlige informationsindsamlinger i disse tilfælde.

For de fysiske besøg kan der udføres tilsynshandlinger som består af dokumenterede opfølgningsmøder med databehandleren af varierende hyppighed. Dertil kan der foretages besigtigelse og stikprøver af kontroller som omfatter inspektion, efterprøvelse, observationer og test af områder, som den dataansvarlige vurderer relevant for den outsourcede behandlingsaktivitet. Eksempelvis hvis den dataansvarlige mener at sikkerhedsforanstaltninger som tilgængelighed og kryptering er det vigtigste for de

[45] Link til Datatilsynets vejledning om tilsyn: https://www.datatilsynet.dk/media/6865/vejledende-tekst-om-tilsyn-med-databehandlere-og-underdatabehandlere.pdf

registrerede, hvorefter dette testes for om det fungerer effektivt. Fordelene ved at udføre fysiske besøg er, at den dataansvarlige kan få en overbevisning om, at det databehandleren påstår også har hold i virkeligheden. Såfremt der ikke er væsentlige afvigelser, vil den dataansvarlige kunne konkludere på at databehandleren efterlever den indgåede databehandleraftale og de aftalte sikkerhedsforanstaltninger. Ulemperne ved de fysiske besøg er at de er meget tidskrævende og at det samtidig ikke er unormalt at den dataansvarlige anvender en række af databehandlere. Det er hertil ikke forudsat at den dataansvarlige har kompetencerne til at udføre de nævnte tests og vurdere hvornår der er testet i et tilstrækkeligt omfang. At vurdere om en kryptering er stærk nok, eller om backup procedurer er tilstrækkelige, vil ofte kræve en vis mængde af IT-kompetencer som ikke nødvendigvis besiddes internt i den dataansvarliges organisation. Selv i de tilfælde hvor den dataansvarlige besidder kompetencerne til at vurdere de nævnte områder, kan det være svært at vurdere hvornår man har testet nok og hvornår man har taget nok stikprøver. Den dataansvarlige skal derfor foretage en vurdering af om de selv besidder kompetencerne til de specifikke handlinger og samtidig vurdere om de selv skal udføre handlingerne eller benytte en ekstern part.

9.1.1 Inddragelse af en ekstern part

For begge disse tilsynsformer gælder at de både kan udføres af den dataansvarlige selv, eller at den dataansvarlige kan få en ekstern part, som en revisor, advokat, IT-ekspert eller lignende til at udføre det på vegne af den dataansvarlige. Førend benyttelse af en ekstern part vil være en tilsynshandling der lever op til GDPR artikel 28, kræves det at den dataansvarlige tager stilling til det produkt der leveres af den eksterne part. Selve arbejdet der udføres af revisoren er i sig selv ikke en tilsynshandling. Ud af de mange muligheder med anvendelse af eksterne parter som led i tilsynsforpligtelsen, er brug af en revisorerklæring et værktøj som stiller høj sikkerhed, da revisorer er underlagt regulering, som bl.a. revisors uafhængighed jf. afhandlingens afsnit 5.2 som er med til at sikre troværdighed. Respondent F forklarer at der benyttes erklæringer for at opnå sikkerhed for leverandører:

Respondent F [13:19]
"Der er jo nogle som er dækket af erklæringer (...) Der er en masse ting der er dækket af en erklæring og jeg vil gætte på den næste store erklæring kommer fra Leverandør XY, de styrer jo så alle de her systemer for os"

Citatboks 14

Som redegjort for i afhandlingens afsnit 5.3, er en revisors slutprodukt at afgive erklæringer. I samme afsnit er det konstateret at der skal anvendes en ISAE 3000 erklæring til databehandleraftaler. Den dataansvarlige skal vurdere hvordan en erklæring skal udformes og hvad den skal tage udgangspunkt i. Der kan eksempelvis udarbejdes en ISAE 3000 erklæring som omhandler en databehandler og dennes databehandleraftale i forhold til en ydelse som lønadministration. Førend den dataansvarlige fører en tilstrækkelig tilsynshandling ved brug af en ISAE 3000 erklæring, skal den dataansvarlige dokumentere at en modtaget erklæring er gennemgået og vurderet i henhold den dataansvarliges vurdering af risiko for de registrerede. Fordelen ved at benytte at benytte sig af en erklæring, er at revisor har de rette kompetencer til at vurdere hvorvidt en given aktivitet og kontrol udføres i overensstemmelse med det aftalte i databehandleraftalen. Ulempen ved en erklæring er, at processen for revisionen kan være administrativ- og omkostningstung, især for de mindre databehandlere. Dette forhold forklares af Respondent A, som sidder på begge sider af forhandlingsbordet når forskellige databehandleraftaler bliver indgået.

Respondent A [35:21]
"*Vi får ikke leverandøren til at lave erklæringer, det kan man jo godt forstå, det er en relativt lille leverandør, ganske få kunder, de vil aldrig nogensinde, prisen vil stige til det firedobbelte eller sådan noget, hvis de skulle tage prisen for en erklæring og vælte det over på de der få kunder de havde, det kommer ikke til at ske, det er en alt for stor opgave for dem*"

Citatboks 15

Respondent A forklarer i Citatboks 15 at små leverandører ikke har ressourcerne til at få udarbejdet en erklæring. Dette er en erkendelse som de dataansvarlige også har gjort sig, som det forklares af Respondent B:

Respondent B [34:15]
"Hvis vi har nogle lidt mindre systemer, som egentlig ikke har særlig mange personoplysninger i sig, men stadig har personoplysninger i sig, om vi skulle kræve revisionsrapporteringer, eller om det mere skulle være et spørgsmål om det de ligesom har kunne fortælle os de gør, både teknisk og organisatorisk, at de skal kunne dokumentere at det gør de rent faktisk stadig. Det er igen noget med, hvis det er en lille enkeltmandsvirksomhed, som har et system der ligger i skyen, et eller andet sted, altså hans forretning kan slet ikke bære at gøre det, men vi er ret betryggende i det han, kan levere dokumentation for hvad har han gjort både teknisk og organisatorisk, så er det i højere grad et spørgsmål om skal kunne løbende dokumentere det."

Citatboks 16

Respondent B forklarer i Citatboks 16 omkring de tilfælde hvor de ikke modtager en erklæring. I disse tilfælde skal de som dataansvarlige, i stedet modtage tilsvarende dokumentation for at de kan sikre at tilsynsforpligtelsen overholdes. I forlængelse af Citatboks 16 forklarer Respondent A, at når der ikke leveres en erklæring, kan dette skabe udfordringer i de tilfælde hvor de dataansvarlige ikke selv har kompetencerne til at foretage fysiske tilsynshandlinger, hvorfor disse dataansvarlige vil kræve en erklæring.

Respondent A [35:48]

"(...) så må i jo bare få den dokumentation i har behov for og gennemgå det, det kan de jo heller ikke forholde sig til fordi, de ikke har revisorhåndværket, de har ikke den der, der kan tygge oplysninger og sige det der ser faktisk fornuftigt ud, de aner ikke hvordan man tager en stikprøve, de aner ikke hvordan man tester en kontrol, de aner ikke hvilke kontroller de bør teste og hvornår de har testet dem nok, de rigtige kontrolmål og hvornår de har testet dem nok. og derfor tør de ikke påtage sig denne her opgave og derfor fisker de efter en der tør skrive under på at tingene er i orden"

Citatboks 17

I Citatboks 17 forklarer Respondent A, at nogle dataansvarlige mangler kompetencerne til at vurdere hvorvidt en given kontrol er tilstrækkelig, hvilket kan skabe en udfordrende situation når den dataansvarlige skal føre sit tilsyn. En løsning hertil kan være at den dataansvarlige selv betaler for en erklæring, eller inddrager ekstern hjælp til at foretage de fysiske tilsynshandlinger. Derudover mener Respondent A også at erklæringer er den mest effektive løsning for begge parter i en databehandleraftale til at hjælpe den dataansvarlige med sin tilsynsforpligtelse i henhold til GDPR artikel 28.

Respondent A [44:11]

"Jeg mener at den mest effektive måde for begge parter det faktisk er en erklæring for databehandleren, fordi et, han skal kun have et hold mennesker rendende til at kigge over ham. To han kan rimeligvis forvente at de rent faktisk ved hvad de taler om, de har prøvet at lave sådan noget her før. (...) de forstår formentligt også det meste af det de render og spørger ind til, hvorimod en virksomhed som kommer rendende, altså hvis der kommer 50 af dem og de aner ikke hvad de spørger til (...) Set fra dataansvarliges side er det jo det samme, de aner ikke hvad de skal spørge om derude (...) Så jeg mener helt klart det er nødvendigt med et eller andet lag, som skaber forbindelse mellem parterne."

Citatboks 18

Opfattelsen af at en erklæring er et effektivt virkemiddel som led i et tilsyn som forklaret i Citatboks 18 deles af Respondent E:

Respondent E [3:22]

"Fordi det er den bedste og mest effektive måde at få en høj grad af overbevisning om at databehandleren overholder de aftaler man har indgået i forhold til håndtering af data, og givet kritikaliteten af det her, givet det samfundsmæssige fokus der er kommet på det, så synes jeg ikke man kan negligere den opgave man har med at holde tilsyn med sine databehandlere og så er det en meget effektiv måde fordi de fleste setups vi ser er jo at databehandleren får lavet en erklæringer der kan dække i forhold til flere dataansvarlige."

Citatboks 19

Respondent A og E mener begge at brugen af erklæringer er den mest effektive måde for en dataansvarlig at føre et tilsyn med sine databehandlere og opnå en overbevisning om hvorvidt de aftalte forhold bliver overholdt. Opfattelsen med at opnå overbevisning igennem en erklæring udtrykkes også af Respondent B, da denne bliver spurgt ind til hvordan de udfører fysisk besøg.

Respondent B [41:42]

"Så man kan sige den mere fysiske del af et tilsyn (…) det er svært at vurdere hvor meget vi nødvendigvis kommer til at gøre det fordi at vi jo nok i vidt omfang kommer til at bero os på, dybest set IT-revisorer, der jo er ude og føre kontrol med at de rent faktisk lever op til det vi har aftalt."

Citatboks 20

Respondent B forklarer i Citatboks 20 hvordan de ikke selv udfører de fysiske besøg, da denne har vurderet at det er mere effektivt at benytte en ekstern part i form af en revisor til at udføre dette på sine vegne. Respondent A mener, udover at de dataansvarlige kan mangle de relevante kompetencer, også at ved få udarbejdet en erklæring, så undgår databehandlere at have en masse dataansvarlige på besøg. Dette argument fra Citatboks 18 bekræftes af Respondent C, da denne bliver spurgt ind til udfordringer med at indgå databehandleraftaler.

Respondent C [33:44]

"De reagerer på, at vi siger at vi har faktisk skrevet at hvis det kontrolformål de har er dækket af en erklæring fx ISAE 3402 eller lignende, så kan de ikke komme og lave fysisk kontrol. Det er jo ikke det samme som at man ikke kan komme og lave fysisk kontrol hvis man har et andet kontrolpunkt, men hvis vi kan komme med en erklæring og sige se her, det i vil kontrollere det har revisoren faktisk kontrolleret. Så ønsker vi jo ikke 60.000 kunder inde og, det kan vi jo slet ikke overskue."

Citatboks 21

Respondenten bekræfter i Citatboks 21 dermed advokatens tese om at databehandlere ikke ønsker at have samtlige kunder på kontrol, hvorfor de foretrækker at lade en revisor foretage dette, hvorefter dette produkt så videregives til kunderne. Hertil erkender respondenten dog, at der kan være særlige dataansvarlige med særlige krav, som ikke er dækket af en erklæring, hvorfor de har lov til at udføre deres egne tests. Som det er forklaret af respondenterne, mener disse at brugen af en erklæring mellem dataansvarlige og databehandlere er et effektivt værktøj som led i et tilsyn. Dels sikrer det et produkt, hvortil de revisorer der udarbejder erklæringen, har ekspertisen og kompetencerne inden for GDPR og revision. Dertil sikrer det også at de stikprøver og kontroller, der bliver testet, er meningsfyldte og relevante i forhold til den indgåede databehandleraftale og at databehandleren ikke skal have massevis af dataansvarlige på besøg for at foretage de samme test. På baggrund heraf må det derfor vurderes at benyttelsen af en revisorerklæring som led i et tilsyn er et effektivt værktøj.

På trods af at revisorerklæringer umiddelbart og ud fra ovenstående gennemgang vurderes som den mest effektive metode, er det stadig vigtigt at have for øje at det ikke er ved alle databehandleraftaler at det er oplagt at inddrage en erklæring. Dette er forklaret af Respondent B, som nævner at det altid er op til en risikovurdering i forhold til de registrerede om hvorvidt en revisorerklæring skal inddrages, hvortil respondenten forklarer:

Respondent B [35:01]

"Ja det er igen lidt tilbage, hvor ligger vi, hvor kritisk er systemet og hvor risikabelt er det for dem der registreres oplysninger om."

Citatboks 22

Såfremt en outsourcet behandlingsaktivitet vurderes klart uvæsentlig og uden særlig risici for de registrerede, kan det være for omfattende at få udarbejdet en ISAE 3000 erklæring i henhold til det omkostningsmæssige perspektiv set i forhold til den vurderede risiko. Her kan en skriftlig bekræftelse fra en databehandler ofte være tilstrækkelig. Da det er fastlagt hvilke tilsynsformer og tilsynshandlinger en dataansvarlig kan foretage samt hvordan en ekstern part kan inddrages, skal det nu fastlægges hvordan en dataansvarlig skal vurdere risikoen for de registrerede.

9.2 Kriterier til vurdering af risici for de registrerede

Det er i afhandlingens afsnit 9.1 beskrevet at et tilsyn foregå gennem fysiske besøg eller skriftlige informationsindsamlinger. En dataansvarlig kan vælge selv at udføre tilsynshandlingerne, eller at få hjælp fra en ekstern part. Grundet de forskellige muligheder der findes, er det nødvendigt for en dataansvarlig at opstille kriterier som danner grundlag for en risikovurdering og hvilke tilsynshandlinger der skal benyttes. Relevante kriterier som en dataansvarlig kan benytte til at vurdere risikoen forbundet med behandling af personoplysninger er oplistet i nedenstående tabel, hvortil kriteriet er uddybet og vurderet hvilke risikoovervejelser de enkelte kriterier giver anledning til.

Kriterie	Uddybning	Risikoovervejelser
Hvilke personoplysninger behandles?	Behandles der kun almindelige personoplysninger, eller behandles der også særlige personoplysninger efter artikel 9 og 10 eller CPR-numre.	Hvis der behandles personoplysninger efter artikel 9, 10 eller CPR-numre, vil udgangspunktet være at der er højere risiko for den registrerede.
Hvor mange kategorier af almindelige personoplysninger behandles?	Hvor mange typer af personoplysninger efter artikel 4 stk. 1 behandles. Eksempelvis navn, adresse, telefonnr. m.m.	Hvis der behandles mange kategorier af almindelige personoplysninger, taler dette for en højere risiko for den registrerede.
Hvor stor en mængde af almindelige personoplysninger behandles?	Hvor mange registreres personoplysninger behandles.	Hvis der behandles personoplysninger om en stor mængde af registrerede, taler dette for en højere risiko for de registrerede.
Hvor mange kategorier af særlige personoplysninger behandles?	Hvor mange typer af personoplysninger efter artikel 9 og 10 behandles. Eksempelvis fagforeningsmæssige forhold, seksuelle præferencer m.m.	Hvis der behandles og i så fald mange kategorier af særlige personoplysninger, taler dette for en højere risiko for den registrerede.
Hvor stor en mængde af særlige personoplysninger behandles?	Hvor mange registreres personoplysninger efter artikel 9 og 10 behandles.	Hvis der behandles særlige personoplysninger om en stor mængde af registrerede, taler dette for en højere risiko for de registrerede
Hvor kompleks er databehandlerkonstruktionen?	Indgår der mange underdatabehandlere i databehandlerkonstruktionen og er der hyppige overførsler imellem disse.	Såfremt der benyttes mange underdatabehandlere og der hyppigt overføres personoplysninger imellem disse, vil det tale for en højere risiko for den registrerede.
Bliver personoplysninger overført til et tredjeland eller en international organisation?	Bliver personoplysninger overført til et tredjeland eller en international organisation	Hvis personoplysninger bliver overført til et tredjeland eller en international organisation, vil der være en øget risiko for den registrerede.

Tabel 6: Kriterier til risikovurdering.
Kilde: Egen tilvirkning

Vurdering af risikoen for de registrerede skal foretages af den dataansvarlige, og skal være på baggrund af den enkelte databehandleraftale. Respondent F forklarer i det følgende hvordan de vurderer risikoen for deres registrerede:

Respondent F [14:37]

"Det er jo sådan en helhedsvurdering, vi gør jo det, at hvis det er en databehandling som medfører risici, så udfører vi en konsekvensvurdering, og den gennemfører vi principielt også ved alle store projekter selvom der ikke er noget kritisk i det (…) og for alle projekter hvor det lugter af HR. Der kører sådan en del af facility management, altså dem der styrer huset, de styrer samarbejdsaftaler med leverandører. Der er også forholdsvist kritiske data, de har også forsikringsaftaler, hvor vi har forsikret en masse ting bl.a. direktørbilerne, og der vil kunne være skader og alle mulige sager hvor de behandler personoplysninger, altså CPR-numre osv. Så sådan lidt ud fra gruppen, antallet af registrerede det er ikke så aktuelt for typisk er det alle medarbejdere, så det er det samme antal, stortset medmindre det fx er kreditregistret eller andet projekt hvor vi kører noget data der vedrører nogle eksterne, det har selvfølgelig også noget som betyder fx på kreditregisteret hvor vi kører låneoplysninger på 3 mio. mennesker, det er selvfølgelig høj kritisk."

Citatboks 23

Som det forklares af Respondent F i Citatboks 23, er det nødvendigt med en helhedsvurdering når risikoen for de registrerede skal vurderes, da en dataansvarliges tid og ressourcer er begrænsede. Derfor skal det prioriteres ud fra den vurderede risiko hvor omfattende tilsynshandlinger der skal udføres. Det er relevant at gennemgå alle kriterierne i Tabel 6 som led i denne helhedsvurdering, hvortil de samlede svar kan tale for enten lav, mellem og høj risiko. Risikovurderingen og virkemidler til tilsyn afhænger af den konkrete risiko, som det forklares i det følgende af Respondent E:

Respondent E [4:27]

"Altså databehandleren skal lave risikovurdering, eller dataansvarlig af sine databehandlere, der vil man jo typisk, hvis man går struktureret til det sige det falder i fem forskellige kasser afhængig af hvad det er, i den ene der mener vi det er meget irrelevant at gøre noget ekstra, der behøver man slet ikke lave noget tilsyn. (…) Og så hvis man skal have den fulde sikkerhed jamen så får man lavet en erklæring, der står på mål for at den databehandleraftale man har indgået, rent faktisk er efterlevet i en given periode, så der er et helt katalog af hvad man bør gøre."

Citatboks 24

Respondenten mener i Citatboks 24 at man som dataansvarlig bør opdele sine databehandlere i forskellige kategorier alt afhængig af hvilken risici der er vurderet. Dertil skal man ud fra kategorierne fastlægge, hvilke virkemidler man skal benytte til tilsynet. For de outsourcede behandlingsaktiviteter, der vurderes med en lav risiko for de registrerede, vil det i langt de fleste tilfælde være tilstrækkeligt at udsende spørgsmål til databehandlere der omhandler de aftalte sikkerhedsforanstaltninger. For et printsystem som kun lagrer historik og medarbejder initialer vil der ikke skulle udføres særlige handlinger hertil, da risikoen for de registrerede vurderes at være lav, som forklaret af Respondent F.

Respondent F [5:44]

"Denne her, det må være en rimelig simpel en, i kan se der behandles jo ingenting, lagring af print historik. Vi har sådan nogle kort når vi printer sikkert, at det bliver opbevaret på printeren, og det eneste den opbevarer er dine initialer"

Citatboks 25

Hvis dette eksempel fra Citatboks 25 anses ud fra Tabel 6, vil lagring af printhistorik og medarbejderinitialer ikke give anledning til høj risiko, da der kun behandles to typer af personoplysninger, hvortil medarbejderinitialer er pseudonymiseret. Des højere risiko, jo større krav vil der være til tilsynets omfang. Yderligere forklarer Respondent F, at denne ikke bruger sin tid på printsystemet, da der ikke vurderes risici hertil.

Respondent F [12:08]

"De kritiske, det er det jeg synes er interessant, det er lidt ligegyldigt med det der printer system hvor initialerne ligger. Det der er interessant for mig det er det system der indeholder alle lønoplysninger, alle straffeattester osv. er det beskyttet godt nok."

Citatboks 26

Respondenten forklarer at prioriteringen vil være der hvor der er en højere risiko, som eksempelvis ved lønoplysninger og straffeattester. Hvis der behandles få kategorier af følsomme oplysninger og en simpel databehandlerkonstruktion, vil det derimod være nødvendigt at foretage opfølgningsmøder med databehandleren og modtage løbende rapportering for at sikre at behandlingen sker i overensstemmelse med databehandleraftalen. Hvis der behandles mange kategorier af følsomme oplysninger, store mængder af følsomme oplysninger og der også er en kompleks databehandlerkonstruktion vurderes der at være en høj risiko forbundet hertil. Dette medfører at det vil være nødvendigt at foretage yderligere

end førnævnte i form af test af kontroller og stikprøver hos databehandleren. Opsummeret betyder dette at jo højere risiko der vurderes, jo flere handlinger til tilsynet skal der foretages af den dataansvarlige. Dette forhold er skematiseret i nedenstående matrix.

		Tilsynsformer	
	Kriterier	**Fysisk besøg**	**Skriftlig informationsindsamling**
Høj	• Behandling af stor mængde og mange kategorier af almindelige personoplysninger • Behandling af stor mængde og mange kategorier af følsomme personoplysninger • Kompleks databehandlerkonstruktion • Overførsel til tredjelande og internationale organisationer	• Halvårlige (eller hyppigere) opfølgningsmøder vedrørende efterlevelse af databehandleraftalen og dokumentation heraf • Test af kontroller • Stikprøver • Fysisk besigtigelse	• Løbende rapportering omkring behandlingen af de outsourcede aktiviteter • Databehandlers dokumenterede gennemgang af underdatabehandlere • Dokumentation for overførselsgrundlag
Risiko	• Behandling af stor mængde og mange kategorier af almindelige personoplysninger • Behandling af lille mængde og få kategorier af følsomme personoplysninger • Simpel databehandlerkonstruktion	• Årlige opfølgningsmøder vedrørende efterlevelse af databehandleraftalen og dokumentation heraf • Test af kontroller • Stikprøver • Fysisk besigtigelse	• Løbende rapportering omkring behandlingen af de outsourcede aktiviteter • Databehandlers dokumenterede gennemgang underdatabehandlere • Dokumentation for overførselsgrundlag
Lav	• Behandling af almindelige personoplysninger • Simpel Databehandlerkonstruktion	• Ikke nødvendigt	• Udsende spørgsmål omkring efterlevelse af databehandleraftalen

Tabel 7: Tilsynsmatrix.
Kilde: Egen tilvirkning

Det må i Tabel 7 påpeges at den ene tilsynsform ikke udelukker den anden. Dette betyder at der både skal udføres fysiske besøg og skriftlige informationsindsamlinger ved mellem og høj risiko. Kombinationen af disse vil variere alt afhængig af den dataansvarliges risikovurdering. Det bemærkes at på trods af at handlingerne til de fysiske besøg og skriftlige informationsindsamlinger kan ligne hinanden i mellem og høj risiko, vil detaljegraden af tilsynshandlingerne være mere omfattende og hyppigheden være oftere. Dette skyldes at der ved den høje risiko oftest vil være en mere kompleks og kritisk behandling, hvorfor der vil være behov for mere gennemgående og hyppigere afklaring af den outsourcede behandling. For at illustrere Tabel 7, vil denne blive eksemplificeret med en uddannelsesinstitution som dataansvarlig. Systemer en uddannelsesinstitution typisk benytter og de beskrevne kriterier vil danne grund-

lag for tilsynsformer for uddannelsesinstitutionen. Respondent B fortæller at de hovedsageligt behandler personoplysninger om studerende, ansatte og deltagere i forskningsprojekter. Hertil forklarer respondenten hvilke personoplysninger der behandles til de enkelte typer:

Respondent B [2:37]

"Man kan sige for alle tre kategorier er det en ret stor mængde af almindelige oplysninger, der er. Der er selvfølgelig forskel på hvad vi har. Studerende, hvad er dit adgangsgrundlag for at komme ind på Universitetet, hvad for en gymnasial uddannelse har du taget, der er en masse oplysninger, CPR numre, generelt hvad der er nødvendigt for at du kan blive optaget på universitetet. (…) Så er der andre der har klagesager, dispensationssager, frameldinger fordi de er langtidssygemeldt, eller hvad der måtte være. (…) Det er mange forskellige almindelige oplysninger og så har vi primært noget om deres helbredsforhold som er i den følsomme kategori når vi snakker studerende."

Citatboks 27

Respondent B [4:33]

"Ansatte, det er lidt det samme som med de studerende, der er noget med CV, karakterer, kandidatbevis og hvad der måtte være nødvendigt for at man kan blive ansat i den stilling man nu søger. Så er der noget CPR-nummer, ellers er det svært at udbetalte løn hvis vi ikke har deres CPR-nummer. Helbredsoplysninger, det er en naturlig del af det at være ansat et sted. Det kan både være fordi man konkret er syg, men det kan også være barsel og hvad der nu ellers måtte være af forskellige ting i den der dur."

Citatboks 28

Respondent B [5:45]

"Så kan man sige forskning, det er alt. Der er ingen tvivl om at vi har, der er nærmest alle de almindelige oplysninger man kan komme i tanke om og helt sikkert alle de følsomme oplysninger der overhovedet er opregnet i artikel 9, dem behandler vi også i forskningsøjemed. På den ene eller anden måde."

Citatboks 29

I Citatboks 27 fortæller respondenten omkring de oplysninger de har og behandler omkring studerende, i Citatboks 28 omkring de ansatte og i Citatboks 29 omkring forskningsdeltagere. Der bliver behandlet almindelige og følsomme personoplysninger om alle tre typer af registrerede. Fælles for alle disse er at uddannelsesinstitutionen benytter mange systemer til behandlingen, som det forklares af respondenten:

Respondent B [8:22]

"De studerende, der har vi nogle studieadministrative systemer, som ofte er nogle fælles løsninger for alle universiteterne, STADS og digital eksamen og hvad der nu ellers er af forskellige systemer. (…) Så har vi Learning Management System (…) Så har vi det her ESDH-system som, hvor alle studerende har sådan en studentermappe hvor vi journaliserer de sager der måtte være med de enkelte studerende (…) Vi har masse forskellige systemer som hjælper med at få hverdagen til at glide, planlægningssystem med eksamen og lokalebookingsystemer og hvor der også godt kan være personoplysninger i fordi der står noget om hvem der har booket lokalerne (…) så er der en anden platform som er de studerendes indgang til alt hvad de nu skal vide om sig selv eller deres uddannelse. Der er en ret stor portefølje. Man kan sige i forhold til de ansatte jamen igen, vi har personalesager som ligger på det her ESDH-system og så har man et system som vi bruger til at registrere fravær, ferie og sygdom og hvis man har andre, omsorgsdage og hvis du har ekstra fridage eller et eller andet (…)."

Citatboks 30

Der er mange eksempler på systemer som anvendes på en uddannelsesinstitution, hvortil respondenten i Citatboks 30 inddrager studieadministrativt system, learning management system, elektronisk sags- og dokumenthåndteringssystem og lokalebookningssystem. Dertil bliver respondenten spurgt ind til om de selv udvikler og drifter systemerne eller om der benyttes leverandører. Respondenten fortæller at der til disse systemer bliver benyttet mange leverandører, som forklaret i det følgende:

Respondent B [13:27]

"Mange af de studieadministrative systemer ligger ikke på universitetet. De bliver driftet af ministeriets IT, digital eksamen bliver driftet af nogle ude på DTU, vi har nogle systemer der bliver driftet her, men vi har mange der bliver driftet andre steder."

Citatboks 31

Respondenten fortæller i Citatboks 31 at nogle af de systemer uddannelsesinstitutionen benytter sig af bliver håndteret af leverandører. Det er hertil vigtigt at skabe sig et overblik over leverandørerne, hvorfor det kan være relevant at have en metode for at kategorisere leverandørerne og for dermed at kunne fastlægge hvilke tilsynshandlinger der skal udføres hos den enkelte leverandør.

9.2.1 Risikovurdering af behandlingsaktiviteter

Der vil i det følgende blive gennemgået eksempler på systemer i en uddannelsesinstitution som er blevet outsourcet, hvor relevante kriterier beskrevet i Tabel 6 inddrages og benyttes til en risikovurdering i henholdsvis lav, mellem og høj risiko. Derudover vil der også blive set på anvendelsen af en

rekrutteringsportal. Når risikoniveauet er fastlagt, kan Tabel 7 benyttes til at fastlægge, hvilke tilsynshandlinger der skal udføres af den dataansvarlige.

Dataansvarlig	Behandlingsaktiviteter	Kriterier	Risikovurdering
Uddannelsesinstitution	Drift af studieadministrative system[46]	• Behandler stor mængde af almindelige personoplysninger af studerende • Behandler fortrolig information i form af CPR-numre • Behandling af lille mængde og få kategorier af følsomme personoplysninger • Simple databehandler konstruktion	Mellem
Uddannelsesinstitution	Drift af Learning management system (LMS)[47]	• Behandler stor mængde og få kategorier af almindelige personoplysninger til studerende og ansatte • Simpel databehandlerkonstruktion	Lav - Mellem
Uddannelsesinstitution	Drift af Elektronisk sags- og dokumenthåndtering system (ESDH)[48].	• Behandler stor mængde af almindelige personoplysninger til studerende og ansatte • Behandler fortrolig information i form af CPR-numre • Behandler stor mængde og mange kategorier af følsomme personoplysninger	Høj
Uddannelsesinstitution	Drift af rekrutteringsportal	• Behandler stor mængde af almindelige personoplysninger til ansøgere • Behandling af lille mængde og få kategorier af følsomme personoplysninger • Simpel databehandlerkonstruktion	Mellem
Uddannelsesinstitution	Drift af lokalebookingsystem	• Behandler almindelige personoplysninger • Simpel databehandlerkonstruktion	Lav

Tabel 8: Eksempler på risikovurdering af behandlingsaktiviteter.
Kilde egen tilvirkning.

Risikovurdering af eksemplerne fra Tabel 8 er baseret på de opstillede kriterier i Tabel 6. Det fremgår af en risikovurdering at et lokalebookingssystem er vurderet til lav risiko, da der i denne sammenhæng typisk kun behandles få kategorier af almindelige personoplysninger som er nødvendige for at kunne booke et lokale. De nødvendige oplysninger for at booke et lokale er eksempelvis navn og studie- eller medarbejdernummer. Ved outsourcing af et lokalebookingsystem indgår en simpel databehandler-konstruktion. Tilsynsforpligtelsen vil i dette tilfælde være tilstrækkeligt med et tilsyn som består af skriftlig informationsindsamling, ved at udsende spørgsmål til databehandleren jf. Tabel 7. For de behandlingsaktiviteter der er vurderet til at have en mellem risiko, vil det være et krav fra den dataansvarlige at modtage løbende skriftlig rapportering omkring behandlingen samt foretage fysiske besøg som kan

[46] Link til beskrivelse af Uddannelses- og Forskningsministeriets studieadministrative system, STADS: https://ufm.dk/uddannelse/videregaende-uddannelse/studieadministrative-systemer/stads
[47] Definition af LMS: Softwareprogram til administration og levering af uddannelseskurser.
[48] Definition af ESDH system: Softwareprogram til journalisering, arkivering, sagsstyring og dokumentstyring.

indebære årlige opfølgningsmøder med databehandleren, fysisk besigtigelse, test af kontroller, stikprøver og databehandlerens dokumenterede gennemgang af underdatabehandlere. I tilfældet med drift af ESDH-systemet er der vurderet en høj risiko for de registrerede. Der arbejdes med både en stor mængde og mange kategorier af følsomme oplysninger, da ESDH-systemet kan indeholde dispensationsansøgninger, som kan indeholde følsomme personoplysninger jf. bilag F. For denne behandlingsaktivitet skal der udføres de samme handlinger som for dem ved mellem risiko, men de skal udføres mere gennemgribende og hyppigere. Disse er blot få eksempler på risikovurderinger af behandlingsaktiviteter, der kan outsources. Det er altid vigtigt at vurdere risikoen i den konkrete situation og når der anvendes databehandlere, for derefter at kunne vurdere hvordan tilsynet skal udformes.

9.2.2 Behov for ekstern part

For tilsynshandlingerne som den dataansvarlige skal foretage, er nødvendigt at klarlægge om den dataansvarlige selv skal udføre det hele, eller om en ekstern part i form af eksempelvis en revisor skal inddrages. En revisorerklæring er relevant at inddrage i tilsynsforpligtelsen, som redegjort for under afhandlingens afsnit 9.1.1. Dette understøttes endvidere af Respondent A's udtalelse fra Citatboks 18. Det er herudover også vurderet at det kan være en tung proces for nogle organisationer at få udarbejdet en erklæring. For ovenstående inddeling i henholdsvis lav, mellem og høj risiko vil der vurderes hvornår erklæringen bør inddrages, og hvilken udformning erklæringen bør have.

I de situationer hvor risikoen vurderes som lav vil det være for omfattende at inddrage en revisorerklæring, fordi tilsynet kan baseres alene på spørgsmål fra databehandleren. Såfremt en dataansvarlig ønsker at inddrage en ekstern part til at hjælpe med tilsyn i den lave risiko, vil det eksempelvis være muligt at benytte sig af advokater. Hertil udbyder nogle advokatfirmaer en ydelse, hvor de skriftligt hjælper dataansvarlige med at føre tilsyn, ved at stille et værktøj til rådighed[49], som strukturerer processen med at sende spørgeskemaer til databehandlere og derefter analysere og vurdere de indkomne svar. Det skal igen konstateres at dette kun er et værktøj til at udføre de skriftlige tilsyn, hvorfor det kan benyttes i alle niveauer af risikovurderingen. Det kan dog kun være et selvstændigt tilsyn i de tilfælde, hvor risikoen vurderes som lav og rapporten fra advokatfirmaet vurderes.

[49] Link til advokatfirmaet Bech-Bruuns værktøj: https://www.bechbruun.com/da/om-os/extraservices/legal-tech-dpa-service

Ved en risiko på mellemniveauet kan der inddrages en ISAE 3000 erklæring, såfremt det vurderes af den dataansvarlige at denne ikke selv kan eller vil udføre test af kontroller, fysisk besigtigelse og stikprøver. En databehandler vil ofte have en databehandleraftale som de benytter som udgangspunkt til alle deres kunder, en generel databehandleraftale. Til denne generelle databehandleraftale vil det være muligt at få udarbejdet en ISAE 3000 erklæring, som vil fungere som en generel erklæring til brug for mange dataansvarlige. Udfordringerne ved at benytte en generel erklæring er at der kan være områder som ikke er relevant for den dataansvarlige, og der kan være områder som den dataansvarlige finder relevant, men ikke er omfattet af erklæringen. Førstnævnte scenarier giver ikke umiddelbare udfordringer, da den dataansvarlige får afdækket alle områder de vurderer som relevant. I det andet scenarie skal den dataansvarlige vurdere om de områder som ikke omfattet af erklæringen, er områder som vurderes som særlige vigtige eller kritiske. Såfremt dette er tilfældet, vil en generel erklæring ikke være et tilstrækkeligt tilsynsværktøj, medmindre den dataansvarlige selv udfører supplerende handlinger, eksempelvis egne test af kontroller og fysisk besigtigelse, for at afdække de risici, som erklæringen ikke dækker. Hvis de ikke omfattede områder vurderes som uvæsentlige eller med meget lav betydning, vil den dataansvarlige kunne benytte en generel ISAE 3000 erklæring. Dette skyldes at en evt. påvirkning af de ikke omfattede områder, ikke vil have en indvirkning på de registrerede.

I de situationer hvor den dataansvarlige har vurderet risikoen som høj, eller har stillet krav til specifikke sikkerhedsforanstaltninger vil det som udgangspunkt ikke være tilstrækkeligt med en generel erklæring. I denne situation skal der udarbejdes en specifik ISAE 3000 erklæring, som går på den konkrete databehandleraftale. Selvom det vurderes at der skal udarbejdes en specifik ISAE 3000 erklæring ved høj risiko, kan der være enkelte situationer, hvor en databehandler udelukkende leverer et standardiseret program og databehandleraftale, uden at de enkelte dataansvarlige kan have nogen påvirkning på denne. I de særtilfælde vil det af sagens natur være tilstrækkeligt med en generel ISAE 3000, da det i praksis vil svare til en specifik ISAE 3000. Det skal igen understreges at den dataansvarlige selv skal vurdere om der skal benyttes en revisorerklæring, da dette er et alternativ til selv at foretage test af kontroller, stikprøver og fysisk besigtigelse hos databehandleren. Behovet for at inddrage en erklæring kan opsummeres i nedenstående tabel.

Vurderet risiko	Erklæringsbehov
Lav	Der vurderes ikke behov for en erklæring.
Mellem	En ISAE-3000 erklæring på baggrund af en standard databehandleraftale bør benyttes (generel ISAE 3000 erklæring).

Vurderet risiko	Erklæringsbehov
Høj	En ISAE-3000 erklæring på baggrund af en specifik databehandleraftale bør benyttes. (specifik ISAE 3000 erklæring). (I særtilfælde kan en generel ISAE 3000 benyttes, hvis der udelukkende leveres en standardydelse og databehandleraftale)

Tabel 9: Erklæringsbehov.
Kilde: Egen tilvirkning

Det fremgår af Tabel 9 at der ikke altid er behov for en erklæring og at det afhænger af en risikovurdering af den enkelte behandlingsaktivitet. Forholdet mellem risikovurdering og brug af erklæringer forklares af Respondent E:

Respondent E [5:07]

"Hvis man skal have den fulde sikkerhed jamen så får man lavet en erklæring, der står på mål for at den data-behandleraftale man har indgået rent faktisk er efterlevet i en given periode, så der er et helt katalog af hvad man bør gøre, hvis det man outsourcer er noget der kun har en perifer tilknytning til eller indhold af persondata så synes jeg ikke det giver nogen mening at bede om en erklæring, men det jo det man skal finde ud af i risiko-vurderingen som dataansvarlig, hvor databehandlere ligger, i hvilken kategori og tage de measures der hører til der. Hvis vi har de høje med store mængder af data eller særlige kritiske der kan det være en særlig god måde at få det her afdækket det på."

Citatboks 32

Som det også forklares af Respondent E i Citatboks 32, er der ikke altid behov for en erklæring. Det er op til den dataansvarlige at foretage en risikovurdering af deres behandlingsaktiviteter, og vurdere hvilke tilsynshandlinger der skal foretages for at opfylde tilsynsforpligtelsen.

9.3 Delkonklusion

Tilsynsforpligtelsen står ikke eksplicit i GDPR artikel 28, men det må fortolkes, at det ikke er muligt at sikre de fornødne garantier, uden en vis form for tilsyn, når der opstår et principal-agent forhold med asymmetrisk information. Tilsynet kan gradueres i både fremgangsmåde og risiko. Et tilsyn kan være ved skriftlige informationsindsamling eller fysisk besøg. Det skal hertil vurderes om den dataansvarlige selv kan foretage tilsynet, eller om en ekstern part, som en revisor, skal inddrages. For at fastlægge hvor omfattende et tilsyn der skal foretages på den enkelte databehandler, kan den dataansvarlige opdele sine databehandleraftaler i lav, mellem og høj risiko. For lav risiko vil skriftlige informationsindsamlinger være tilstrækkelige, mens der for højere risiko vil være krav om både fysiske besøg i form af besigtigelse, stikprøver og test af kontroller samt skriftlig informationsindsamling.

Det er konstateret at det ikke er et krav fra hverken Datatilsynets standarddatabehandleraftale eller GDPR at inddrage en revisor, men såfremt begge aftaleparterne er enige, kan dette forhold indskrives i aftalen. Det er konkluderet at benyttelsen af arbejdet fra en revisor, vil være en optimal situation for både den dataansvarlige og en databehandler, hvis inddragelsen af en erklæring afspejler de aktuelle risici for de registrerede. En revisorerklæring kan være omkostningstung, hvorfor dette ikke vil være løsningen for alle dataansvarlige og databehandlere. Såfremt en revisorerklæring inddrages, skal dette være en ISAE 3000, hvortil en generel erklæring som udgangspunkt kan benyttes til mellem risiko, og en specifik erklæring benyttes til den høje risiko. Det er konkluderet hvornår en revisor kan og bør inddrages som led i at føre tilsyn, og der vil i det næste kapitel undersøges hvordan en revisorerklæring skal anvendes.

10. ISAE 3000 erklæring om behandling af personoplysninger

Det er i det forrige kapitel blevet konkluderet at anvendelsen af revisorerklæringer er et effektivt virkemiddel i den dataansvarliges tilsynsforpligtelse. Revisorer har de rette kompetencer som kræves i til stikprøver og test af kontroller, hvilket de dataansvarlige ofte ikke har. Når revisorer inddrages til at kontrollere at en databehandleraftale bliver efterlevet, er det en fordel for databehandleren da denne ikke skal have besøg af alle dens dataansvarlige, men kun et enkelt team af revisorer. Derudover er fordelen ved at inddrage en revisor også at slutproduktet bliver en ISAE 3000 erklæring med høj grad af sikkerhed, som er udarbejdet af en uafhængig og objektiv tredjepart hvilket øger troværdigheden. Dette kapitel vil besvare Underspørgsmål 4: 'Hvordan bør en ISAE 3000 erklæring om behandling af personoplysninger benyttes af en dataansvarlig?'.

Når der i en databehandlerkonstruktion opstår et principal-agent forhold, som forklaret i kapitel 9, vil det være nødvendigt for den dataansvarlige at reducere informationsrisikoen til et acceptabelt niveau. Når en revisor inddrages i principal-agent forholdet mellem den dataansvarlige og databehandleren, kan dette ske ved at han efterprøver, inspicerer og tester kontroller hos databehandleren i henhold til den indgåede databehandleraftale. En ISAE 3000 erklæring vil munde ud i en konklusion med høj grad af sikkerhed, hvortil revisor be- eller afkræfter om databehandleren i alle væsentlige henseender opfylder den indgåede databehandleraftale. På trods af at en revisor kan udarbejde en erklæring, kan der blandt dataansvarlige og databehandlere stadig være tvivl om hvordan en sådan erklæring skal benyttes og inddrages i den aktive tilsynsforpligtelse, som det forklares af Respondent A:

Respondent A [11:29]

"Men altså det er, det er jo at jeg vil sige hvis man laver en erklæring efter den her, vil man efter min opfattelse lave et, sammenlignet til mad, et rigtigt lækkert måltid. Men dem der sidder og skal spise det kan ikke smage forskel på en hakkebøf og et eller andet fint fransk (…) men modtageren er bare ikke i stand til at tage imod dette produkt, fordi de ikke forstår det arbejde der ligger."

Citatboks 33

10.1 Hvordan skal en erklæring benyttes?

Det er tidligere blevet konkluderet at det ikke er tilstrækkeligt blot arkivere en erklæring fra en revisor som led i et tilsyn. Den modtagne erklæring skal gennemlæses kritisk og vurderes til den enkelte dataansvarliges egen vurdering af risici for de registrerede, førend der er tale om en reel tilsynshandling i

henhold til GDPR artikel 28. Der vil undersøges, hvordan en dataansvarlig bør tage stilling til en modtaget erklæring, samt hvordan denne skal benyttes til tilsynet. Analysen vil tage udgangspunkt i FSR – Danske Revisorers ISAE 3000: 'Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med [Dataansvarlig]'. Det vurderes at denne erklæringsskabelon vil have høj anvendelighed, da den dels er udarbejdet af FSR – Danske Revisorer, samt at den er baseret på Datatilsynets standarddatabehandleraftale. Denne tese bekræftes af Respondent A:

Respondent A [10:57]

"Hvis i sammenligner de to, så den fra 17 led af den enorme svaghed, at den listede samtlige områder i forordningen, også dem en databehandler notorisk aldrig nogensinde kan have ansvaret for. Det havde jeg det en lille smule underligt med, hvorfor i himlens navn vil du erklære dig om noget som ham du erklærer dig om aldrig kan få ansvaret for, der er den her lang bedre, for den er langt mere skarpskåret på databehandlerens forpligtelser. Så den vej rundt synes jeg det er rigtig fint."

Citatboks 34

Den tidligere analyse af databehandlerens forpligtelser i kapitel 8 har taget udgangspunkt i Datatilsynets standarddatabehandleraftale, hvorfor dette også taler for at inddrage FSR – Danske Revisorers erklæringsskabelon, da denne netop erklærer sig på baggrund af Datatilsynets standarddatabehandleraftale. Igennem interviewet med Respondent A er det blevet klart at nogle dataansvarlige ikke er klar over hvad der skal erklæres om, og hvordan en erklæring skal benyttes, samt at nogle dataansvarlige heller ikke er klar over hvilken erklæring de har behov for, som det forklares i følgende:

Respondent A [16:25]

"Det jeg oplever i praksis det er det er sjældent der sidder en modpart som forstår det der med sikkerhed og erklæringer. (...) Det er rigtig fint i beder om en erklæring, men i simpelthen nødt til at sætte jer ned og gøre det klart hvad er det for et minimumsindhold. Ja men det skal bare være en 3000 erklæring eller 3402. Det er fint men standarden siger jo kun noget om hvordan revisor skal opføre sig, den siger ikke noget om hvad for nogle informationer han skal putte ind. (...) Det er i som dataansvarlige nødt til at tage stilling til, hvad er vigtigt for jer (...) Man skal gøre sig klart hvad det egentligt er man vil have en erklæring om, jeg tror rigtig mange opfatter det som et, så får man bare et stempel og der er ingen problemer i det"

Citatboks 35

Respondent A mener i Citatboks 35 at de dataansvarlige skal være med til at bestemme omfanget af en erklæring før den kan benyttes, ellers kan konsekvensen være at der udarbejdes en erklæring som ikke vil have værdi for modtageren. Denne opfattelse deles af Respondent D:

Respondent D [20:21]

"Det starter jo egentligt med, hvis vi kigger i databehandleraftalen så er der et vilkår omkring det her, så kommer databehandler til os og siger vi skal opfylde det her vilkår, og så får lavet denne her erklæring (...) nogle gange har jeg en oplevelse af at den bliver lavet, denne her revisorerklæring med udgangspunkt i databehandler-aftalen, fordi det står som vilkår, men når den så rammer den dataansvarlige så er det måske en der bliver sat tjek ved og sat ind i en mappe og så gør man ikke mere ved det, måske ikke læst og måske ikke forholdt sig til den. Men så har man reelt ikke udført sit tilsyn (...) der er en opgave i at de dataansvarlige får det indarbejdet som en proces og en metode til at få gennemgået de her databehandleraftaler."

Citatboks 36

Det forklares af Respondent D i Citatboks 36 at nogle dataansvarlige har udfordringer og ikke ved hvordan man skal forholde sig til en erklæring. Denne udtalelse fra Respondent D deles af Respondent B, da respondenten med en juridisk baggrund ikke har kompetencerne til at vurdere de IT-mæssige aspekter af en erklæring:

Respondent B [43:41]

"Men meget af det her er IT-teknisk, altså nogle af de her ISAE-rapporter, jo jeg kan da godt sidde og læse dem, men det er ikke mig som jurist der får super meget ud af det. Det er vores IT-folk som kan sige, det der står her, er det også det vi har aftalt, især på den tekniske front. Det kan være på den organisatoriske jeg kan forholde mig til det. Men IT-teknikken har jeg ikke den tekniske indsigt til at vurdere om det er, så der er jo også noget."

Citatboks 37

Som forklaret af Respondent B i Citatboks 37, er det nødvendigt at en organisation tager stilling til hvem der har de rette kompetencer til at vurdere indholdet af en modtaget revisorerklæring. Der vil derfor i det følgende blive undersøgt hvordan en dataansvarlig bør forholde sig til en ISAE 3000 erklæring udarbejdet på baggrund af FSR – Danske Revisorers skabelon.

10.1.1 Stillingtagen til FSR – Danske Revisorers ISAE 3000

Indledningsvis skal den dataansvarlige undersøge om den modtagne erklæring er relevant for den indgåede databehandleraftale. Der kan være situationer hvor en databehandler leverer mange forskellige systemer, og udfører mange forskellige behandlingsaktiviteter, hvortil de kan have flere forskellige databehandleraftaler. Den dataansvarlige skal undersøge om den erklæring der modtages er vedrørende et system, behandlingsaktivitet og databehandleraftale som er relevant for dem. Respondent D udtaler at et tilsyn ikke er gennemført førend der er taget stilling til erklæringen.

Respondent D [21:14]
"For at kunne dokumentere sit tilsyn skal man læse den erklæring der kommer ind man skal forholde sig til den, og specielt hvis der er forbehold, absolut, men der kan jo også godt være nogle mindre afvigelser, det vi konkluderer på i erklæringen er jo i alt væsentlighed, eller alle væsentlige henseender, så har der ikke været noget, men så kan der godt være nogle mindre ting som står ude i den der afvigelses, resultat af test kolonne, hvor man så kan gå ned og læse at der er nogle mindre ting."

Citatboks 38

Som det konstateres i Citatboks 38, er en erklæring først anvendelig som led i tilsynet når der er taget stilling til denne. Overordnet indeholder ISAE 3000 erklæringen følgende afsnit, som den dataansvarlige skal tage stilling til:

- Ledelsens udtalelse,
- Uafhængig revisors erklæring,
- Systembeskrivelse,
- Kontrolmål, kontrolaktivitet, test og resultat heraf

<u>Ledelsens udtalelse</u>

Dette afsnit i erklæringen omfatter en udtalelse fra ledelsen, hvori ledelsen udtaler sig om hvilken databehandleraftale og hvilke behandlingsaktiviteter erklæringen omhandler. Ledelsen bekræfter at de medfølgende beskrivelser af behandlingsaktiviteter er retvisende for en given periode. Dernæst udtaler ledelsen at de implementerede kontroller er hensigtsmæssige i forhold til de opstillede kontrolmål. Afslutningsvis udtaler ledelsen sig om at der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger for at efterleve den indgåede databehandleraftale.

I afsnittet med ledelsens udtalelse skal den dataansvarlige tage stilling til om de behandlingsaktiviteter, kontroller, kontrolmål og tekniske og organisatoriske foranstaltninger er relevante i forhold til den dataansvarliges vurderede risiko. Hertil kan der være udfordringer når databehandleren får udarbejdet en generel ISAE 3000. Omfanget i denne erklæring kan afvige i forhold til hvad den dataansvarlige vurderer som væsentligt for at sikre de registreredes rettigheder. Eksempelvis kan en databehandler i en generel ISAE 3000 erklæring have vurderet at indhentelse straffeattester ikke skulle være omfattet af erklæringen, men hvis den dataansvarlige har vurderet dette som den mest kritiske kontrol, så vil erklæringen ikke kunne benyttes som led i et tilsyn.

Uafhængig revisors erklæring

Dette afsnit i erklæringen omfatter den uafhængige revisors erklæring, hvori revisor erklærer sig om hvorvidt databehandleren har levet op til den indgåede databehandleraftale. Hertil konkretiseres det, at det er databehandlerens ansvar at udarbejde beskrivelser og udtalelser om de leverede ydelser. Det er også databehandlerens ansvar at udforme, implementere og udføre kontroller. Dernæst erklærer revisor sig om at denne har været uafhængig, samt hvordan revisor skal agere i henhold til sit ansvar. Revisor tydeliggør at der kan være begrænsninger i brug af erklæringen, da databehandlerens beskrivelser i en generel erklæring er udarbejdet for at opfylde de almindelige behov for en bred kreds af dataansvarlige. Dette medfører at erklæringen muligvis ikke dækker alle aspekter i en given behandlingsaktivitet som en dataansvarlig måtte have vurderet væsentlige. Afslutningsvis er revisors konklusion hvori han be- eller afkræfter ledelsens udtalelse, hvorefter der henvises til de test af kontroller, der er udført i forbindelse med revisionen og en formålsbegrænsning.

Den dataansvarlige skal forholde sig til revisors konklusion, hvori der kan være eventuelle forbehold og fremhævelse af forhold, med den forudsætning at revisors øvrige beskrivelser stemmer overens med ledelsens udtalelse. I de tilfælde hvor der enten er forbehold eller fremhævelse af forhold, skal den dataansvarlige tage stilling til og vurdere hvordan dette kan have en indvirkning på netop deres outsourcede behandlingsaktivitet. Eksempelvis kan revisor have taget forbehold for at kontroller vedrørende den fysiske adgangsbegrænsning ikke har været effektiv i hele perioden. Her skal den dataansvarlige vurdere, om det er noget som har en væsentlig indflydelse på deres risikovurdering af de registreredes rettigheder. Endegyldigt kan den dataansvarlige ende ud i at skulle opsige aftalen, hvis det vurderes at indvirkningen af forbeholdet ikke kan mitigeres på andre måder og dermed reducere den overordnede risiko.

Systembeskrivelse

Dette afsnit i erklæringen indeholder en beskrivelse af behandlingsaktiviteterne. Disse vil som udgangspunkt spejle sig i databehandleraftalen. Heri indgår, som det også gør i databehandleraftalen, karakteren af behandlingen, hvilke personoplysninger der indgår, hvilke praktiske tiltag der er implementeret og en risikovurdering. Til sidst fremgår de kontrolforanstaltninger som databehandleren har implementeret og komplementerende kontroller hos den dataansvarlige. Det essentielle til systembeskrivelsen er at den dataansvarlige sikrer sig at de beskrivelser af behandlingsaktiviteter og personoplysninger stemmer overens med den indgåede databehandleraftale.

Kontrolmål, kontrolaktivitet, test og resultat heraf

I dette afsnit i erklæringen fremgår en beskrivelse af de opsatte kontrolmål og tilhørende kontroller. Dertil forefindes en beskrivelse af revisors udførte tests og tilhørende resultater. Et eksempel hertil er at der er opstillet et kontrolmål med implementering af tekniske foranstaltninger i henhold til behandlingssikkerheden. En kontrol til dette kontrolmål kunne være at al udveksling af følsomme personoplysninger skal krypteres. Revisors test vil være at inspicere at der foreligger formaliserede procedurer, som sikrer at overførsel af følsomme personoplysninger over internettet er beskyttet af en stærk kryptering, som er baseret på en anerkendt algoritme. Dertil skriver revisor resultatet af sin test, enten at der ikke har været nogle afvigelser eller at der har været noget som giver anledning til bemærkninger.

For den dataansvarlige er det især i dette afsnit at der skal foretages en grundig gennemgang, da der som forklaret af Respondent D i Citatboks 38, godt kan være forhold af betydning for den enkelte dataansvarlige. Hvis revisor har konstateret afvigelser til nogle af de fastlagte kontroller, skal den dataansvarlige vurdere hvorvidt disse afvigelser har betydning for dennes vurdering af risikoen for de registrerede, samt hvilke supplerende handlinger der skal udføres for at reducere risikoen til et acceptabelt niveau. Respondent F fortæller hvordan de har oplevet mindre afvigelser i en modtaget erklæring og hvordan de har taget stilling til dette

Respondent F [39:24]

"Ja, du kan se denne her fra Leverandør XY, der var faktisk nogle afvigelser i den, hvor jeg har skrevet opfølgning. I denne her erklæring var det noget med deres brugerstyring, det er altid brugerstyring, der er problemer med. (…) Det er altid noget med, der bliver givet en eller anden rettighed, og så ændrer folk funktion og så har de glemt at opdatere den. Det er altid det samme, fordi de kan ikke finde ud af det. (…) Så hiver jeg så fat i den ansvarlige herinde, og det er så tilfældigvis XYZ, og så spørger jeg jamen de har tydeligvis ikke styr på det, mener revisor. Der var så og så mange stikprøver hvor der var fejl i. Hvad gør vi? Og så, siger han der er allerede igangsat noget (…) Så det er i de igang med at fikse nu, og så på et eller andet tidspunkt får jeg så forhåbentligt af vide at nu er det fikset. (…) I mine øjne er det et lille problem, det er nogle administratorer, de styrer det i nogle grupper, jeg tror det var nogle administratorer som havde bredere administrator adgange end var nødvendigt. Men persondatamæssigt kan man sige at administratoren har altid bred adgang. Sådan er det. (…) Igen lav risiko, for god ordens skyld så følger jeg op på det. "

Citatboks 39

I Citatboks 39 fortæller respondenten hvordan revisor har konstateret at der har været fejl i brugerstyringen hos leverandøren. Den dataansvarlige vurderer hvilken effekt fejlen har for de registrerede, hvortil det bliver vurderet at fejlen er uvæsentlig, grundet den vurderede lave risiko. Den dataansvarlige vurderer at der for god ordens skyld vil blive fulgt op på at dette forhold bliver løst. Hvis det var vurderet at fejlen omkring brugerstyringen havde stor betydning for de registreredes rettigheder, kunne en konsekvens være at den dataansvarlige måtte udtræde af aftalen med databehandleren.

Det er tidligere blevet konkluderet at den dataansvarlige ikke kan bruge en erklæring som led i sit tilsyn, medmindre der aktivt tages stilling til og vurderes den modtagne erklæring. Der er derfor gennemgået og vurderet hvordan en dataansvarlig bør forholde sig til de fire overordnede afsnit i en ISAE 3000 erklæring med udgangspunkt i FSR – Danske Revisorers skabelon.

10.2 Delkonklusion

Når der opstår et principal-agent forhold i en databehandlerkonstruktion medfører dette asymmetrisk information, hvorfor der kan være et behov for uafhængig tredjepart. Den uafhængige tredjepart vil typisk være en revisor som udarbejder erklæringer til brug for at forsikre den dataansvarlige om, at databehandleren overholder den gældende aftale.

For en revisorerklæring er det vigtigt at den dataansvarlige har fokus på at fastlægge omfanget korrekt når denne efterspørges af en databehandler. Dette skyldes at en ISAE 3000 ikke fortæller noget om hvilke informationer en revisor skal medtage i en erklæring, men kun hvordan han skal opføre sig. Såfremt omfanget af en erklæring ikke er i overensstemmelse med den indgåede databehandleraftale, vil den dataansvarlige ikke kunne benytte erklæringen som led i sit tilsyn, medmindre der udføres supplerende handlinger til at afdække de risikofyldte områder som en erklæring ikke dækker.

Yderligere er der gennemgået FSR – Danske Revisorers ISAE 3000 erklæringsskabelon, som tager afsæt i Datatilsynets standarddatabehandleraftale. Hertil er der redegjort for de enkelte afsnit i erklæringen, og forklaret hvordan en dataansvarlig skal tage stilling de enkelte afsnit. Erklæringsskabelonen er opdelt i fire overordnede afsnit, som består af ledelsens udtalelse, uafhængig revisors erklæring, systembeskrivelse og kontrolmål, kontrolaktivitet, test og resultat heraf. Den dataansvarlige skal læse de fire afsnit kritisk og tage stilling til hvert enkelt afsnit og om de beskrevne procedurer, behandlingsaktiviteter, sikkerhedsforanstaltninger m.m. er relevante for dennes outsourcede behandlingsaktiviteter. Dertil skal der tages stilling til evt. forbehold, fremhævelse af forhold og afvigelser i revisors test af kontroller. Såfremt dette er tilfældet, skal den dataansvarlige vurdere indvirkningen af revisors resultat. Hvis den dataansvarlige vurderer at dette har betydning for de registreredes rettigheder, skal der iværksættes handlinger der reducerer risikoen til et acceptabelt niveau.

Underspørgsmål 1-4 er blevet gennemgået i kapitel 7-10, hvor der er undersøgt hvordan en databehandlerkonstruktion opstår, og hvilke forpligtelser en databehandler er underlagt i en databehandleraftale. Dette skaber et krav for den dataansvarlige til at føre tilsyn, hvortil der er undersøgt hvordan omfanget og handlinger til et tilsyn fastlægges, samt hvordan en revisor kan inddrages i denne proces ved at afgive en ISAE 3000 erklæring. For at sætte dette i perspektiv til en finansiel revision, hvor revisor erklærer sig om et regnskab, vil der i det næste kapitel blive gennemgået underspørgsmål 5, som omhandler hvilke overvejelser en revisor ved en finansiel revision har til GDPR.

11. GDPR i den finansielle revision

I de forrige underspørgsmål er der blevet gennemgået hvordan en dataansvarlig opfylder sin tilsynsforpligtelse i henhold til GDPR artikel 28. Dette kapitel vil besvare Underspørgsmål 5: 'Hvilke overvejelser til GDPR bør en revisor have under en finansiel revision?'. Det er er hertil interessant at undersøge hvordan den eksterne revisor ved en finansiel revision, kan benytte viden fra de forrige kapitler i den ordinære revisionsproces.

For den eksterne revisor vil dennes arbejde under en finansiel revision ofte bestå i at udarbejde en ISA 700 erklæring. Denne erklæring omhandler revision af årsregnskabet. Som led i en ISA 700 erklæring er revisor underlagt en række andre ISA'er som beskriver, hvordan der skal planlægges, udføres og rapporteres om en revision. I planlægningen er det påkrævet at revisor skal identificere og vurdere risici for væsentlig fejlinformation igennem forståelse af virksomheden og dens omgivelser, jf. ISA 300.9 som henviser til ISA 315. Der er i ISA 315 beskrevet hvordan revisor skal identificere og vurdere risici for væsentlig fejlinformation igennem forståelse af virksomheden og dens omgivelser. I denne proces vil revisor tage stilling til relevante reguleringsforhold, jf. ISA 315.11(a). Dette henleder til ISA 250 som omhandler overvejelser i forbindelse med love og øvrig regulering. I ISA 250 er det defineret hvilke typer af regulering som revisor skal forholde sig til. Af ISA250.6 fremgår:

Denne ISA differentierer revisors ansvar med hensyn til overholdelse mellem følgende to forskellige kategorier af love og øvrig regulering: (jf. afsnit A6, A12-A13)

(a) bestemmelserne i de love og øvrig regulering, der normalt anses for at have en direkte virkning på fastsættelsen af væsentlige beløb og oplysninger i regnskabet, f.eks. love og øvrig regulering om skat og pension (se afsnit 14) (jf. afsnit A12), og

(b) andre love og øvrig regulering, der ikke har direkte indvirkning på fastsættelsen af beløb og oplysninger i regnskabet, men hvis overholdelse kan være afgørende for virksomhedens driftsforhold, dens mulighed for at fortsætte sine forretningsaktiviteter eller dens mulighed for at undgå væsentlige bøder (f.eks. overholdelse af vilkårene i en driftslicens, solvenskrav eller miljøregler). Manglende overholdelse af sådanne love og øvrig regulering kan derfor have væsentlig indvirkning på regnskabet (se afsnit 15) (jf. afsnit A13).

Det må hertil konstateres at GDPR falder under kategori (b), da denne ikke har en direkte påvirkning på fastsættelsen af væsentlige beløb og oplysninger i regnskabet. Overholdelsen af GDPR kan være afgørende for en virksomheds driftsforhold, eksempelvis i tilfælde af bøder. Manglende overholdelse af GDPR kan have en væsentlig indvirkning på regnskabet[50], da det højeste bødeniveau jf. GDPR artikel 83 stk. 5 kan være op til 20 millioner euro eller 4% af den samlede globale omsætning, hvorfor dette må antages ofte at være over det fastlagte væsentlighedsniveau. Der har i Danmark ikke været mange sager med bøder grundet manglende overholdelse af GDPR. Et eksempel herpå er Taxa 4x35 som er politianmeldt af Datatilsynet, der har lagt op til en bøde på 1,2 millioner kr.[51]. Foreningen opnåede i 2017 et resultat på 3,1 millioner kr. før skat i regnskabsåret[52], hvorfor en bøde af en sådan størrelse vil have en væsentlig indvirkning på regnskabet[53]. Da det er blevet konkluderet at GDPR kan have en væsentlig indflydelse på regnskabet, er det nødvendigt at fastlægge hvilke handlinger revisor skal udføre. I ISA 250.15 fremgår at revisor i henhold til love og øvrig regulering skal:

Revisor skal udføre følgende revisionshandlinger med henblik på at identificere tilfælde af manglende overholdelse af andre love og øvrig regulering, der kan have væsentlig indvirkning på regnskabet (jf. afsnit A13-A14):

(a) forespørge den daglige ledelse og, hvor det er passende, den øverste ledelse om, hvorvidt virksomheden overholder sådanne love og øvrig regulering, og
(b) inspicere eventuel korrespondance med relevante bevillingsudstedende eller lovgivende myndigheder (jf. afsnit A9-A10)

I ISA 250.A6 fremgår en række eksempler på love og øvrig regulering som kan være relevant for revisor at tage stilling til i henhold til ISA 250.6. Heri fremgår bl.a. love om databeskyttelse, hvortil en dansk revisor vil skulle forholde sig til GDPR. GDPR kan munde ud i store bøder, hvorfor det vurderes at være omfattet af revisors pligter i henhold til ISA 250. Der vil i derfor i kapitlet blive udarbejdet en tjekliste

[50] Revisors væsentlighedsniveau fastlægges efter ISA 320 og er en beløbsgrænse for fejl, som vil påvirke en regnskabsbrugers dispositioner.
[51] Link til Datatilsynet vedr. bøde til Taxa 4x35: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/mar/datatilsynet-indstiller-taxaselskab-til-boede-paa-1-2-mio-kr/
[52] Resultat før skat jf. pressemeddelelse fra TAXA 4x35 17. maj 2018. Der henvises til bilag G for print af pressemeddelelse.
[53] Jf. ISA 320.A8 kan 5% af resultat før skat bruges som væsentlighedsniveau. Bøden svarer til 38,71% af Taxa 4x35's resultat før skat, hvorfor det vurderes langt over revisors væsentlighedsniveau.

som en revisor kan anvende i sine forespørgsler til ledelsen og vurdere hvorvidt der er behov for yderligere handlinger i form af evt. substansrevision.

Tjeklisten vil omfatte store dele af GDPR, hvoraf tilsynsforpligtelsen, som er redegjort og analyseret i kapitel 7-10, kun er et af de områder som skal spørges ind til og kan have en væsentlig indvirkning på regnskabet. Det må dog påpeges at når revisor gennemfører nedenstående tjekliste, er udgangspunktet at revisor ikke skal vurdere om procedurer og behandlingshjemler er lovlige, men blot tage stilling til om der foreligger disse, som det forklares af Respondent A:

Respondent A [42:06]
"Revisorer er rigtig glade, hvis der ligger en proces der siger, at man skal gøre et eller andet. Du kan have en proces der siger du skal huske at spørge en der har forstand på det (...) og så kan man i øvrigt se at det har man gjort 8 gange i løbet af året (...) Det er da fint du har en proces at du skal huske og spørge en eller anden, men hvad var det materielle indhold med det han kom ud med, det får du aldrig i en erklæring. (...) Revisorer skal aldrig udtale sig om det har de ikke forudsætninger for, med alt respekt. Hvis der står i proceduren hos databehandleren at de skal huske at spørge vores interne advokat, hver gang vi støder på det her, og de kan vise at de har husket at spørge deres interne advokat, så skal revisor ikke begynde at forholde sig til om den interne advokats juridiske vurdering var korrekt."

Citatboks 40

Ud fra betragtningen i Citatboks 40, at revisor ikke nødvendigvis skal vurdere det juridiske indhold af de svar han får, vil der udarbejdes en tjekliste hvor der oplistes en række "Ja/Nej" spørgsmål med tilhørende uddybning. Disse spørgsmål er relevante for revisor at spørge om i forbindelse med en finansiel revision og den indvirkning GDPR kan have på regnskabet. Spørgsmålene skaber en grundlæggende forståelse og overbevisning om hvorvidt den virksomhed der revideres, har procedurer inden for GDPR.

Forespørgsel	Uddybning	Ja / Nej
Er der taget stilling til GDPR?	Spørgsmålet stilles for at revisor kan få en grundlæggende forståelse for om klienten har taget stilling til GDPR.	
Har i taget stilling til behovet for en databeskyttelsesrådgiver/DPO?	Spørgsmålet stilles for at revisor kan få en forståelse for om klienten har taget stilling til om der er behov for en DPO	
Udarbejdes og opdateres der fortegnelser over personer hvis personoplysninger behandles?	Spørgsmålet stilles for at revisor kan få en overbevisning om at klienten ved hvem der behandles personoplysninger omkring, for at kunden kan leve op til diverse forpligtelser i GDPR, som ret til sletning og indsigt.	
Foreligger der en persondatapolitik?	Spørgsmålet stilles for at revisor kan få en forståelse for om klienten har taget stilling til grundlæggende principper og rettigheder for de registrerede. Såfremt der foreligger en persondatapolitik, har virksomheden alt andet lige taget aktiv stilling til deres behandling af personoplysninger	

Forespørgsel	Uddybning	Ja / Nej
Findes der dokumenteret hjemmel for behandlingsaktiviteter?	Spørgsmålet stilles, da der i GDPR er krav om dokumenteret hjemmel til behandlingsaktiviteter.	
Uddannes de ansatte i GDPR?	Spørgsmålet stilles, da alle i klientens virksomhed skal forstå, hvordan de skal behandle personoplysninger og efterleve GDPR, da det ikke er nok at ledelsen har taget stilling til det, men at alle medarbejdere i alle relevante stillinger ved dette.	
Tager i løbende stilling til det organisatoriske og tekniske sikkerhedsniveau?	Spørgsmålet stilles, da der i GDPR stilles krav til passende tekniske og organisatoriske sikkerhedsforanstaltninger, hvortil krav til disse kan stige i takt med udviklingen.	
Har der i årets løb været ændringer til væsentlige behandlingsaktiviteter og tilhørende systemer	Spørgsmålet stilles, da det er relevant for revisor for at identificere risici at vide, om der har været væsentlige ændringer til eksempelvis ERP-systemer eller behandlingsaktiviteter.	
Har der i årets løb været databrud som påvirker de registrerede og er der producere for rapportering heraf?	Spørgsmålet stilles, da der jf. GDPR kan være krav om at rapportere brud til de registrerede og Datatilsynet.	
Benyttes der leverandører hvori der videregives personoplysninger?	Spørgsmålet stilles, da det er relevant for revisor at vide om klienten har outsourcet behandling af personoplysninger.	
Foreligger der en databehandleraftale med alle leverandører der behandler personoplysninger?	Spørgsmålet stilles, da der efter GDPR stilles krav til skriftlig og elektronisk databehandleraftale.	
Har der i årets løb været rapporterede incidents fra jeres leverandører?	Spørgsmålet stilles, da det er relevant for revisor at vide om klienten har taget stilling til eventuelle problemer eller brud hos leverandører.	
Har i en procedure for risikovurdering af outsourcede behandlingsaktiviteter?	Spørgsmålet stilles, da det er relevant for revisor at vide om klienten har taget stilling til kritikaliteten af den behandlingsaktivitet der outsources	
Fører i tilsyn med jeres databehandlere?	Spørgsmålet stilles, da der jf. GDPR artikel 28 stilles krav om tilsyn med databehandlere. Som dataansvarlig skal man være opmærksom på at man har ansvaret for behandling af personoplysninger, også selvom denne behandlingsaktivitet er outsourcet.	
Har i modtaget og forholdt jer til revisorerklæringer vedrørende risikofyldte databehandlere?	Spørgsmålet stilles, da der som led i tilsynsforpligtelsen kan benyttes revisorerklæringer, hvortil der stilles krav om klienten har taget aktiv stilling til disse.	

Tabel 10: Tjekliste om GDPR til en finansiel revision.
Kilde: Egen tilvirkning

Bliver der svaret ”nej” til et eller flere af de stillede spørgsmål, skal revisor foreslå klienten at dette forbedres og overveje om afvigelserne enkeltvis eller samlet giver anledning til en effekt på regnskabet i form af højere sandsynlighed for bøder. Såfremt revisor vurderer at selskabet kan få en bøde og at denne vil være væsentlig karakter, vil revisor først bede virksomheden om at hensætte et beløb i regnskabet, og hvis selskabet ikke ønsker dette, må revisor tage et forbehold for den mulige indvirkning af den manglende hensættelse. Derudover skal revisor altid overveje om ledelsen kan ifalde ansvar, såfremt det er konstateret at GDPR ikke bliver overholdt. Det vurderes at fordi bøder omkring GDPR sendes til virksomheden, vil udgangspunktet være at der ikke kan være tale om ledelsesansvar, medmindre der er tale om tilfælde hvor ledelsen groft tilsidesætter deres ansvar og handler groft uagtsomt eller forsætligt. Eksempelvis i det tilfælde hvor en ledelse er blevet gjort opmærksom på overtrædelser, men aktivt vælger ikke at rette ind. I de tilfælde hvor revisor vurderer at ledelsen kan ifalde erstatnings- eller strafansvar, skal revisor jf. Erklæringsbekendtgørelsen §7, stk. 2 medtage dette i hans påtegning af regnskabet, som en fremhævelse af forhold.

11.1 Delkonklusion

I dette kapitel er GDPR undersøgt i henhold til den eksterne revisor og dennes overvejelser i forbindelse med en finansiel revision. I en ISA 700 vil revisor planlægge sin revision ud fra ISA 300 og identificere risici efter ISA 315. Hertil kan en risiko være en manglende overholdelse af relevant regulering. ISA 250 omhandler hvordan revisor skal forholde sig til regulering. Det fremgår i ISA 250 at regulering er opdelt i to kategorier, som er regulering med og uden direkte indvirkning på regnskabet. Det vurderes at GDPR vil falde i sidstnævnte kategori som en indirekte virkning på regnskabet i form af bøder. Bøder inden for GDPR er ikke udbredt i Danmark endnu, hvorfor det kan være svært for revisor at vurdere om en manglende overholdelse af GDPR kan føre til en væsentlig bøde. Hertil er der inddraget en sag fra Danmark, hvor et taxaselskab er blevet politianmeldt af Datatilsynet som lægger op til en bøde på 1,2 mio. kr. svarende til 38,71% af resultatet før skat for regnskabsåret 2017. Det konkluderes dermed at GDPR bøder kan være af væsentlig karakter.

For at imødekomme denne risiko, skal revisor forespørge og inspicere korrespondance i henhold til ISA 250.15(b) og såfremt der er forhold af betydning, kan det være nødvendigt med substansrevision. Til at hjælpe revisor med at vurdere om der er væsentlig risiko forbundet med virksomhedens overholdelse af GDPR, og om der skal udføres substansrevision, er der udarbejdet Tabel 10 som er en tjekliste med 15 spørgsmål. Såfremt der svares ”nej” til et eller flere af disse spørgsmål kan det give anledning til at revisor skal udføre yderligere handlinger, for at revidere mod risikoen for GDPR’s indirekte indvirkning på regnskabet. Det skal understreges at revisor som udgangspunkt ikke skal vurdere det juridiske indhold i de svar han får, men blot konstatere om der foreligger procedurer inden for GDPR. Der kan være en forpligtelse for revisor at rapportere om manglende overholdelse af GDPR i hans påtegning, men kun i de tilfælde hvor det vurderes at der skal hensættes til en bøde eller ved ledelsens grove uagtsomhed som kan medføre erstatnings- eller strafansvar til et medlem af ledelsen.

Da alle fem underspørgsmål er gennemgået, vil der i det næste kapitel opstilles en fiktiv case der skal prøve at omfavne alle de overvejelser og konklusioner der er udledt af underspørgsmålene.

12. Case: De Grønne Ingeniører A/S

Casen der vil blive gennemgået tager udgangspunkt i virksomheden De Grønne Ingeniører A/S, der outsourcer hele deres rekrutteringsproces til HR Eksperterne A/S. I casen vil der blive gennemgået hvordan De Grønne Ingeniører skal forholde sig til at benytte sig af HR Eksperterne A/S. Der vil fokuseres på overvejelser til GDPR og den indgåede databehandleraftale, både før og efter indgåelsen, men også under aftalens levetid. Formålet med casen er at vise hvordan en dataansvarlig skal overholde sin tilsynsforpligtelse i henhold til GDPR artikel 28. Opbygningen af casen vil være en tilnærmelsesvis afspejling af afhandlingens kapitel 7-11, hvorfor casen skal fungere som en praktisk tilgang til delkonklusionerne fra de forrige kapitler.

12.1 Casebeskrivelse

De Grønne Ingeniører (herefter "DGI") blev stiftet i 2008 med en vision om at gøre verden til et bedre sted gennem bæredygtige ingeniørydelser og har en mission om at levere værdiskabende løsninger til miljøproblemer i hele verden. Organisationsdiagram for DGI fremgår af bilag H. DGI har igennem de sidste 3 år vokset fra en omsætning på 123 mio. kr. og 112 ansatte i 2016 til 267 mio. kr. i omsætning og 245 medarbejdere i det netop afsluttende regnskabsår 2018. Ifølge virksomhedens budgetter og ambitioner, vil de frem til 2022 øge medarbejderstaben og omsætningen til det dobbelte. Målet er at DGI ved udgangen af 2022 skal have en omsætning på over 550 mio. kr. og 500 medarbejdere. Disse tanker om øget vækst har medført at ledelsen i DGI vil undersøge på hvilke områder de kan effektivisere.

Grundet den øgede medarbejderstab, har den HR-ansvarlige igennem længere tid benyttet sig af utallige excel-ark og mailkorrespondance med mulige kandidater. DGI er en meget attraktiv arbejdsplads og modtager helt op til 60 ansøgninger på mail for et enkelt stillingsopslag, da den grønne profil taler til mange kandidater. De nuværende metoder for rekruttering har gjort processen omkring stillingsopslag og ansættelsessamtaler meget ineffektiv. Derudover har den HR-ansvarlige også måtte erkende, at der i HR-afdelingen ikke er ressourcer nok til selv at sortere i alle indkomne ansøgninger, hvorfor kandidater ofte skal vente meget længe inden der bliver indkaldt til samtaler. Efter afsluttede samtaler er processen om at sende mails til dem der ikke blev tilbudt job eller samtale også meget tung, da man manuelt skal åbne alle ansøgningerne som er modtaget på mail. Den HR-ansvarlige vurderer også at ledelsens visioner om øget medarbejderstab vil medføre at afdelingen ikke kan følge med. DGI har besluttet at iværksætte

en målrettet indsats for at aflaste HR-afdelingen og valgte i den forbindelse at indgå et samarbejde med HR Eksperterne A/S (herefter "HRE") om at varetage hele DGI's rekrutteringsproces.

12.2 Overvejelser før aftaleindgåelsen

I dette afsnit vil der blive redegjort for hvilke overvejelser DGI har gjort sig til outsourcing som danner grundlag for udvælgelsen af HRE som leverandør af rekrutteringsydelsen. DGI skal overveje hvorvidt outsourcing overhovedet er den rigtige vej og skal overveje hvordan de skal løse udfordringen med HR-afdelingens rekrutteringsproces. Dette giver anledning til at overveje om det fortsat skal være HR-afdelingen der skal stå for rekrutteringsprocessen eller om DGI fremadrettet skal benytte en ekstern leverandør. Til dette blev der fremlagt tre mulige løsninger:

Løsningsforslag	Uddybning	Fordele	Ulemper
Ansætte medarbejdere som specifikt arbejder med rekruttering	Der ansættes flere medarbejdere i HR-afdelingen som specifikt får opgaven til at varetage de mange fremtidige rekrutteringer.	Bevarer fuld kontrol over hele processen Sikre sig at kompetencerne til rekruttering er tilstede	Ikke fleksibelt
Eksternt IT-system til rekruttering	Portalløsning som foregår i en webbrowser, hvortil HR-afdelingen kan koble sig på og oprette stillingsopslag, indkalde til samtaler o.l.	Strømlinet rekrutteringsproces Tidsbesparende, da processen strømlines	Afgiver delvis kontrol over processen, fordi man ikke selv drifter IT-systemet
Leverandør varetager rekrutteringsprocessen	Der vælges en leverandør som kan varetage hele rekrutteringsprocessen som omfatter: Udarbejdelse af job og kandidatprofil Søgning og udvælgelse af kandidater Udarbejdelse af stillingsopslag og markedsføring Screening og indkaldelse til interview Deltagelse i interview Håndtering af den administrative proces Drift og vedligeholdelse af IT-system	Nem og overskuelig proces Tidsbesparende, da man skal bruge langt mindre tid på det administrative Sikre sig at kompetencerne er tilstede	Afgiver næsten alt kontrol for rekrutteringsprocessen, hvilket betyder at der skal bruges ressourcer på at kontrollere leverandøren

Tabel 11: Løsningsforslag.
Kilde: Egen tilvirkning

DGI mente at muligheden med at benytte en ekstern leverandør, som beskrevet i Tabel 11, til hele processen ville være hensigtsmæssig. Dette sikrede at HR-afdelingen ikke skulle byrdes med en tidskrævende opgave, det blev sikret at folk med de rette kompetencer sad med området og at DGI som led i deres strategi kunne fokusere på egne kernekompetencer. Dertil blev rekrutteringsprocessen ikke vurderet som et kritisk område for DGI, hvorfor der ikke var store risici i denne proces.

I udvælgelsen af leverandører til at varetage rekrutteringsprocessen havde DGI en række overvejelser hvortil der blev udarbejdet en risikovurdering. Til udvælgelsen af leverandør blev følgende fastlagt som kriterier der skulle overvejes:

#	Kriterier
1	Leverandørens ry, evner, ekspertise, kapacitet, ressourcer og organisationsstruktur samt eventuelle certificeringer.
2	Leverandørens forretningsmodel, natur, fleksibilitet, kompleksitet, finansiel situation, ejerskab og selskabsstruktur.
3	Sikre at leverandøren handler i overensstemmelse med DGI's værdier, også når underleverandører benyttes.
4	Den operationelle risiko ved at outsource, herunder: - Hvad sker der hvis noget går galt eller leverandøren nægter at samarbejde - Om leverandøren benytter underleverandører
5	Om leverandøren kan sikre de fornødne garantier i henhold til GDPR.

Tabel 12: DGI's overvejelser til outsourcing.
Kilde: Egen tilvirkning

DGI havde undersøgt hvem der i markedet kunne levere en fuld rekrutteringsydelse, hertil var tre nedenstående leverandører fremhævet som mulige leverandører.

Leverandør	Beskrivelse
HR Eksperten A/S	Dansk selskab, som siden 1983 har leveret fulde HR-løsninger. Selskabet er ejet af en større dansk fond, hvortil der ikke er noget gæld i selskabet. Selskabet har et godt ry og mange kundecases på hjemmesiden, som fremhæver deres løsninger. Hertil er de ISO 27001[54] certificeret. Selskabet har siden GDPR blev vedtaget i 2016 haft stort fokus på dette og indrettet deres programmer og processer så beskyttelse af de registreredes rettigheder og frihedsrettigheder var topprioritet, hvortil deres databehandleraftale ligger frit tilgængeligt på deres hjemmeside. Selskabet tilbyder en årlig ISAE 3000 erklæring baseret deres databehandleraftale. Selskabet bruger egne udviklede programmer og personale, med undtagelse af hosting af servere, som udføres af et ukrainsk selskab.
Ansættelsespartnerne ApS	Dansk selskab, som siden 2017 har leveret HR løsninger. Selskab er ejet af en mindre gruppe af private aktionærer, som arbejder i selskabet. Siden stiftelsen har selskabet endnu ikke haft profit og har opbygget en stor gæld og negativ egenkapital. Selskabet har ikke en stor kundebase, men bliver omtalt positivt i både pressen og af kunder. Selskabet har egne udviklere ansat og benytter primært egne systemer. Selskabet har stort fokus på at levere et produkt, som de mener kan hjælpe deres kunder med at overholde GDPR. Dertil benytter de underleverandører til at levere deres primære rekrutteringsplatform.
We Do Recruit ApS	Dansk selskab, som siden 2007 har leveret HR løsninger til en bred vifte af europæiske organisationer. Selskabet er igennem det schweiziske moderselskab ejet af en tidligere svindeldømt dansk forretningsmand, som nu er bosiddende i Rusland. Selskabet har ingen gæld og har af kunder fået gode

[54] ISO 27001: En informationssikkerheds standard, som er en del af ISO/IEC 27000 serien af standarder. ISO 27001 specificerer ledelsessystemer, skal tilvejebringe informationssikkerhed under ledelsens kontrol og har specifikke krav hertil. Link til ISO, som udarbejder standarden: https://www.iso.org/isoiec-27001-information-security.html

Leverandør	Beskrivelse
	anmeldelser. Selskabet har siden GDPR's ikrafttræden haft stor fokus på dette og indrettet produkter efter GDPR. Selskabet udvikler og udfører alt arbejde selv, og benytter sig af underleverandører i Litauen til hosting af servere til deres rekrutteringsportal. Den danske ejer har været meget omtalt i medierne som kraft af hans rolle under finanskrisen, hvor han udnyttede forskellige finter til at trække penge ud af konkurstruede virksomheder, som han senere blev dømt for.

Tabel 13: Leverandører til rekrutteringsydelsen.
Kilde: Egen tilvirkning

Umiddelbart mente DGI at alle tre leverandører fra Tabel 13, på trods af deres forskelle, ville kunne levere det ønskede produkt. En vigtig del af DGI's overvejelser var GDPR da man havde identificeret at ved at outsource rekrutteringsprocessen ville det inkludere både almindelige og følsomme personoplysninger, hvortil der kan være udsigt til store bøder ved manglende overholdelse. I vurderingen af en fremtidig leverandør var der derfor lagt vægt på at leverandøren skulle garantere et højt niveau af sikkerhed for behandlingen af personoplysninger.

For DGI betød den operationelle risiko også meget, da de med deres aggressive vækstplan ikke ville risikere at benytte en leverandør, som måske ikke ville kunne levere ydelsen i fremtiden. Det blev derfor besluttet at Ansættelsespartnerne ApS, grundet deres negative egenkapital og manglende evne til at genere overskud blev sorteret fra. Derudover havde DGI også et ønske om at den leverandør de benyttede skulle være en leverandør som man kunne tale højt om, uden at folk ville associerede dette med tidligere begivenheder. Grundet dette blev We Do Recruit ApS sorteret fra, grundet ejerens tidligere kriminelle handlinger. Valget af leverandør faldt derfor på HR Eksperterne A/S da de var sidste mulige leverandør. På trods af dette var det stadig vigtigt for DGI at denne leverandør kunne leve op til deres bekymringer og krav omkring GDPR samt operationelle overvejelser. HRE garanterede DGI at de igennem deres kontinuerlige fokus på GDPR ville kunne stille de fornødne garantier. Derudover henviste de også til deres historik og at de havde leveret HR-løsninger i næsten 40 år, hvorfor de også skulle kunne klare DGI's behov uden problemer.

DGI og HRE indgik derfor en aftale om at HRE de næste 4 år skulle levere en komplet rekrutteringsydelse til DGI. Til hovedaftalen blev der indgået en databehandleraftale som skulle regulere alle forhold relevant til behandlingen af personoplysninger, hvilket var et krav da outsourcing af rekrutteringsydelsen indeholdt behandling af personoplysninger og dermed skabte en databehandlerkonstruktion. Grundet

afhandlingens undersøgelsesområde vil der fremadrettet fokuseres på og tages udgangspunkt i aftaleparternes databehandleraftale. Til aftaleindgåelsen havde HRE en standarddatabehandleraftale som de tilbyder alle deres kunder. DGI accepterede databehandleraftalen uden ændringsforslag. I denne databehandleraftale fremgik beskrivelser af behandlingsaktiviteter, kontroller og alle andre forhold, som skulle reguleres. Databehandleraftalen i dens helhed fremgår af bilag I. Outsourcing af rekrutteringsprocessen var ensbetydende med afgivelse af kontrol til en leverandør. DGI havde identificeret at de efter GDPR artikel 28 havde en forpligtelse til at sikre sig, at de ved benyttelse af databehandlere, skulle have de fornødne garantier. Derudover havde de også forstået artikel 28 som et krav til dem om at føre et aktivt tilsyn med deres databehandlere, da de på trods af at de kan outsource en behandling, ikke kan outsource ansvaret for behandlingen.

Næste afsnit omhandler forhold under aftalens levetid i henhold til GDPR. For afhandlingens synspunkt og for læserens forståelse bliver der først redegjort for DGI's risikovurdering og vurdering af tilsynsbehov under aftalens levetid. I praksis vil dette blive gjort inden hovedaftalen og databehandleraftalen indgås. Dette afspejles i databehandleraftalen under punkt C.6, da der på forhånd skal tages stilling til, hvilke procedurer og virkemidler et tilsyn skal foretages med.

12.3 Under aftalens levetid

Den outsourcede aktivitet omhandler en rekrutteringsproces som lægger op til behandling af en stor mængde af almindelige personoplysninger. Samtidigt kan der indgå følsomme personoplysninger, som det fremgår af databehandleraftalens bilag A. Det fremgår at personoplysningerne som er omfattet af behandlingen er nødvendige for at søge et job, såsom almindelige personoplysninger som navn, adresse, uddannelse m.fl. Derudover kan der også indgå alt hvad ansøgere selv vælger at skrive i en ansøgning eller et CV, som kan være alt, herunder alle de oplistede kategorier af følsomme personoplysninger jf. GDPR artikel 9.

Grundet dette skal DGI som dataansvarlig overveje, hvordan de skal sikre sig at behandlingssikkerheden er tilstrækkelig under hele aftalens levetid. For at sikre at risikoen for de registreredes rettigheder og frihedsrettigheder ikke stiger til et niveau højere end det acceptable. Dette betyder at DGI på den ene eller anden måde skal føre et tilsyn med HRE og kontrollere om HRE efterlever den indgåede databehandleraftale. Omfanget af tilsynet kan dog variere alt afhængig af hvilken risiko der vurderes for de

registrerede. DGI udarbejdede en risikovurdering for rekrutteringsprocessen som bliver gennemgået i det følgende. I afhandlingens afsnit 9.2 er der i Tabel 6 gennemgået kriterier som kan benyttes af en dataansvarlig til at vurdere risikoen forbundet med behandling af personoplysninger. Med udgangspunkt i tabellen kan DGI fastsætte et overordnet risikoniveau for den outsourcede behandlingsaktivitet. Til at fastsætte et risikoniveau har DGI haft tabellens elementer inddraget i overvejelserne, som bliver gennemgået i nedenstående:

Kriterie	Overvejelser	Risikopåvirkning
Hvilke personoplysninger behandles?	DGI har kortlagt rekrutteringsprocessen og hvilke personoplysninger der behandles heri. Det der i overvejende grad bliver behandlet, er de almindelige personoplysninger, da det oftest ikke er nødvendigt med andet for at søge et job. Da man i en ansøgningsproces anvender ansøgning og CV, er der mulighed for ansøgere til at skrive hvad som helst.	Det forventes at behandlingen primært omfatter almindelige personoplysninger, hvorfor der som udgangspunkt ikke er meget risiko for de registrerede med dette. Da der bliver indsendt ansøgninger og CV, hvor ansøgerne har fri mulighed for at skrive hvad som helst som hverken de dataansvarlige eller databehandlerne har kontrol over, hvorfor der kan forekomme følsomme personoplysninger og dermed en øget risiko. Der vurderes hertil et risikoniveau der ligger i mellemniveauet.
Hvor mange kategorier af almindelige personoplysninger behandles?	DGI har kortlagt at de almindelige personoplysninger, som vil indgå i processen er: navn, adresse, e-mail, telefonnr., uddannelsesbaggrund samt andet, som kan indgå i en ansøgning.	Da udgangspunktet er at det er en mindre mængde af definerede kategorier af almindelige personoplysninger, taler dette ikke for en særlig høj risiko for de registrerede. Der er dog mulighed for at en ansøger potentielt kan skrive alle former for almindelige personoplysninger i en ansøgning, hvilket taler for en højere risiko. Overordnet må det dog vurderes at risikoen stadig vurderes som lav, da der kun er tale om almindelige personoplysninger.
Hvor stor en mængde af almindelige personoplysninger behandles?	Da der normalt har været 60 ansøgere pr. stillingsopslag, er dette en lille mængde af registrerede, hvilket betyder at det også er en lille mængde af personoplysninger.	Der vurderes ikke særlige risici til mængden af personoplysninger, som bliver behandlet igennem rekrutteringsprocessen, hvorfor risikoen vurderes som lav.
Hvor mange kategorier af særlige personoplysninger behandles?	Da det er muligt for en ansøger at skrive hvad som helst i en ansøgning, er det ikke muligt på forhånd at vurdere hvor mange kategorier af særlige personoplysninger, som vil blive behandlet.	Da det kan være alt fra ingen til samtlige kategorier af følsomme personoplysninger, som kan indgå i en ansøgning, må det vurderes at dette taler for en høj risiko, fordi DGI ikke kan vide og tage hensyn til om der er få eller mange kategorier af følsomme personoplysninger. Dette betyder at det må antages at der kan være følsomme personoplysninger i samtlige ansøgninger der behandles.
Hvor stor en mængde af særlige personoplysninger behandles?	Den potentielle mængde af registrerede, som kan skrive følsomme personoplysninger er det samme som for de almindelige, da mængde af registrerede vil være det samme. Det er dog forskelligt, hvor mange ansøgere der vælger at skrive følsomme personoplysninger i en ansøgning.	Da det ikke kan vides med sikkerhed hvor stor en mængde af følsomme personoplysninger der behandles, må der ageres som at der behandles en stor mængde. Dette betyder at risikoen vil være høj, da der potentielt kan være en stor mængde af følsomme personoplysninger.

Kriterie	Overvejelser	Risikopåvirkning
Hvor kompleks er databehandler-konstruktionen?	I databehandleraftalen med HRE fremgår at behandlingen foregår hos HRE og at der kun benyttes en underdatabehandler til hosting.	Da der kun benyttes en underdatabehandler og at behandlingen foregår hos HRE vurderes risikoen hertil at være lav.
Bliver personoplysninger overført til et tredjeland eller en international organisation?	Personoplysninger bliver jf. Databehandleraftalen overført til Ukraine, som er et tredjeland.	Da personoplysninger bliver overført til et tredjeland, vurderes risikoen at være mellem til høj. Ved overførsel til tredjelande vil risikoen blive talt op, mens risikoen bliver talt ned, ved at det er en begrænset mængde af funktionalitet som foregår i et tredjeland.

Tabel 14: Risikovurdering af rekrutteringsproces.
Kilde: Egen tilvirkning

Elementer i risikovurderingen der taler risikoen ned for de registrerede er at der som udgangspunkt vil være få kategorier og en lille mængde af almindelige personoplysninger samt ingen følsomme personoplysninger, hvortil der er en simpel databehandlerkonstruktion. De elementer der taler risikoen op for de registrerede er at der kan indgå mange kategorier og store mængder af almindelige personoplysninger. Derudover kan der indgå en ukendt mængde følsomme personoplysninger, hvortil der også indgår overførsel til tredjelande. Den samlede risiko ud fra alle ovenstående betragtninger i henhold til behandlingen af rekrutteringsprocessen udmunder i at DGI vurderede det til at være på et mellemniveau. Ud fra risikovurderingen skal DGI fastlægge omfanget af et tilsyn med HRE, hertil hvordan og hvornår de skal føre tilsyn, herunder om hvorvidt der skal indgå fysiske tilsyn, skriftlige tilsyn, driftsstatusmøder osv. Til fastlæggelsen af omfanget vil afhandlingens tilsynsmatrix, Tabel 7, inddrages, hvor der skal vurderes hvilke former for tilsyn DGI skal udføre i henhold til den vurderede risiko. Af tilsynsmatrixen fremgår det at DGI, ved en vurderet mellem risiko, både skal foretage fysiske besøg og udføre skriftlig informationsindsamling. Den skriftlige informationsindsamling omfatter løbende rapportering om rekrutteringsprocessen. De fysiske besøg kan være mere omfattende og vedrører bl.a. årlige opfølgningsmøder, der tager afsæt i den indgåede databehandleraftale.

Den løbende rapportering indebærer at DGI skal følge op på HRE. Dette kan udføres ved at der periodisk udsendes spørgsmål eller mailkorrespondancer med HRE for at orientere DGI om den løbende behandling. DGI vil gerne sikre sig at den løbende behandling sker i overensstemmelse med databehandleraftalen, hvorfor det er besluttet at der skal være en månedlig rapportering fra HRE til DGI og et kvartalsvis spørgeskema fra DGI til HRE.

Den månedlige rapport som DGI skal modtage, skal omhandle både de operationelle elementer af hovedaftalen, men også den løbende behandling. Rapporteringen vil være i form af en månedlig e-mail fra HRE. Hertil vil de operationelle elementer af rapporteringen omfatte hvor mange der har været indkaldt til samtale, hvor mange ansættelser der har været, hvor mange ansøgere der har været, samt hvilke stillingsopslag der har været. Derudover vil der rapporteres om oppetid på serveren, brud, indsigelser fra registrerede eller andet som måtte være relevant for behandlingen. Et eksempel på en af de månedlige rapporter fremgår af bilag J. Det kvartalsvise spørgeskema fra DGI til HRE vil være en række spørgsmål, som DGI stiller til HRE for at få klarhed for, hvordan HRE de foregående tre måneder konkret har efterlevet den indgåede databehandleraftale. Til dette skal der spørges ind til om der har været ændringer til de aftalte forhold. Hertil kan der spørges ind til om der har været ændringer i hvem der har adgang til DGI's personoplysninger, bekræftelse af om der fortsat handles efter instruks, har der været forhold som giver anledning til bekymringer herunder fortrolighed, har der været væsentlige ændringer til den overordnede behandlingssikkerhed og om der er sket ændringer til underdatabehandlere samt om der styr på disse. Dertil skal DGI efterspørge status på anmodninger fra de registrerede og nye vurderinger af brud. Et eksempel på et af disse spørgeskemaer fremgår af bilag K.

Indhentning af de skriftlige informationsindsamlinger er i sig selv ikke nok til at udgøre en del af tilsynet. Det afgørende er at DGI tager stilling til de informationer de modtager. Når DGI modtager den månedlige rapport, eller får svar på deres kvartalsvise spørgeskema, skal de gennemgå det og tage stilling til det i forhold i databehandleraftalen og om det kan have nogen indvirkning på vurderingen af risikoen for de registrerede. Hvis det eksempelvis fremgår af den månedlige rapportering fra HRE, at IT-systemet har været nede i en periode, kan dette give anledning til overvejelser om hvorvidt data er gået tabt. Såfremt dette er tilfældet kan dette have en risiko for den registrerede, da det kan betyde at den registreredes indsigtsret efter GDPR artikel 15, stk. 3, vil være umulig at efterleve. Betydningen heraf er at DGI skal spørge HRE om nedbruddet har haft eller kan have en påvirkning på behandlingen eller de registreredes rettigheder. Hvis dette er tilfældet skal DGI vurdere hvilken indvirkning dette kan have for de registrerede. Når DGI har udsendt og modtaget svar på deres spørgeskema, kan der også være afvigelser til det forventede hertil. HRE kan eksempelvis havde skrevet at der har været ændringer til personsammensætning som har adgang til DGI's data. I den situation skal DGI overveje hvilken påvirkning det kan have at det nu er nye personer, som sidder med deres behandlingsaktivitet. Det skal hertil vurderes om det nye personale har den tilstrækkelige viden inden for persondatasikkerhed, samt om de er underlagt en tavshedspligt som det følger af databehandleraftalen. Igen er det essentielle at DGI forholder sig til om

ændringen har nogen betydning for de registrerede. De skriftlige informationsindsamlinger for DGI er gennemgået, hvorfor det næste DGI skal tage stilling til er hvordan de skal udføre fysiske besøg, da de jf. deres vurdering af en mellem risiko, ikke kan nøjes med de skriftlige informationsindsamlinger.

De fysiske besøg indebærer opfølgningsmøder med HRE, test af kontroller, stikprøver og fysisk besigtigelse hos HRE. Risikoen er vurderet til mellem, hvorfor DGI vurderer at hyppigheden for opfølgningsmødet vil være tilstrækkeligt med et årligt opfølgningsmøde, da det bliver suppleret med den løbende skriftlige rapportering. Dette årlige møde skal inkludere relevante personer fra både DGI og HRE. Til møderne diskuteres bl.a. forholdene i databehandleraftalen og hvordan parterne opfylder deres forpligtelser. Dertil skal der også diskuteres det fremadrettede samarbejde, herunder databehandleraftalen, og hvad der fungerer, hvor det er oplagt at inddrage dokumentationen fra de skriftlige informationsindsamlinger. Ydermere skal der føres referat, så de årlige opfølgningsmøder kan dokumenteres. Udover de årlige opfølgningsmøder, skal DGI udføre andre fysiske besøg jf. Tabel 7. DGI skal sammen med HRE identificere kontroller der er relevant for den indgåede databehandleraftale, jf. databehandleraftalen bilag C.2. Kontrollerne skal vurderes, hvortil udvalgte kritiske kontroller skal testes af DGI, for at sikre at de faktisk fungerer. Relevante kontroller er bl.a. at sikre alle ansatte i HRE løbende får uddannelse inden for områder af GDPR og løbende ajourføring af brugerstyring, hvortil DGI også skal vurdere hvorvidt der skal tages stikprøver heraf. Ved den fysiske besigtigelse skal DGI bl.a. kontrollere om der er den aftalte fysiske sikkerhed og om printede dokumenter med personoplysninger om DGI's registreredes bliver arkiveret i overensstemmelse med databehandleraftale.

Det er vigtigt at DGI tager stilling til de ovenstående handlinger som de fysiske besøg lægger op til. For opfølgningsmødet er det ikke tilstrækkeligt kun at afholde et. DGI er nødt til at tage stilling til de diskuterede emner og vurdere hvorvidt det ændrer deres vurdering af risikoen for de registrerede. Til et møde kunne der eksempelvis diskuteres hvilke overvejelser HRE har omkring udskiftning af den underdatabehandler, som står for hosting. DGI skal hertil overveje indvirkningen af en eventuel ny underdatabehandler, herunder underdatabehandlerens fysiske lokation og hvordan HRE sikrer sig at en ny underdatabehandler bliver pålagt de samme forpligtelser som den forrige underdatabehandler. For test af kontroller, stikprøver og den fysiske besigtigelse skal DGI sikre sig at resultaterne er i overensstemmelse med databehandleraftalen, samt om eventuelle afvigelser eller fejl ved de fysiske besøg kan have nogen indvirkning for de registrerede. Konstateres det eksempelvis at adgangsstyringen ikke fungerer optimalt, ved

at tidligere medarbejdere og ikke relevante medarbejdere har adgang til DGI's data, skal de udover at påpege dette overfor HRE, også vurdere hvilken påvirkning det har for de registrerede.

For de fysiske besøg skal DGI også vurdere hvorvidt de selv har kompetencerne og ressourcerne til at udføre test af kontroller og stikprøver. Da GDPR artikel 28 stiller krav om tilsyn med databehandlere, vurderer DGI at de selv skal afholde de årlige opfølgningsmøder og efterfølgende dokumentation af disse. Grundet deres virke som ingeniører vurderer DGI at de ikke umiddelbart besidder kompetencerne til at teste kontroller og foretage stikprøver. DGI vurderer at de ikke har den nødvendige viden til at fastlægge om en kontrol er designet hensigtsmæssigt, hvor mange gange de enkelte kontroller skal testes, på hvilke tidspunkter de skal testes og hvad der skal gøres hvis en test viser en afvigelse. DGI vurderer derfor, at for at de kan udføre et effektivt tilsyn i henhold til de omtalte handlinger vil inddrage en ekstern part. Da DGI udvalgte HRE som leverandør blev der lagt vægt på at HRE kunne tilbyde en årlig ISAE 3000 erklæring, da DGI som beskrevet i det foregående ikke selv har kompetencerne til at teste kontroller og foretage stikprøver. Derfor har DGI og HRE i databehandleraftalens punkt 12, som henviser til bilag C, aftalt at der årligt skal udarbejdes en ISAE 3000 erklæring. I denne erklæring skal en uafhængig revisor skal udtale sig om hvorvidt HRE i alle væsentlige henseende overholder den indgåede databehandleraftale og tilhørende tekniske og organisatoriske foranstaltninger. I henhold til den fysiske besigtigelse, vurderer DGI at de selv kan foretage dette, men DGI vælger dog at overlade dette til revisor. Dette skyldes at kravet om bl.a. fysisk sikring er omfattet af databehandleraftalen, hvorfor det vil være omfattet af revisors erklæring. Grunden til dette er at DGI ikke ser nogen grund til at udføre et stykke arbejde som revisor i forvejen vil foretage. Det påpeges igen at en ISAE 3000 erklæring i sig selv ikke er kan indgå som et led i et tilsyn. DGI's stillingtagen til en modtaget erklæring vil være det som indgår som et led i et tilsyn. Det samlede tilsyn vil som det tidligere er beskrevet være kombinationen af alle de skriftlige og fysiske handlinger. DGI's gennemgang af en modtaget ISAE 3000 erklæring fremgår af nedenstående afsnit.

12.3.1 Gennemgang af modtaget ISAE 3000 erklæring

Erklæringen som DGI har modtaget fra HRE fremgår af bilag L og revisors stikprøveberegninger fremgår af bilag M[55]. Som det er blevet konkluderet i kapitel 10 er det vigtigt at DGI sikrer sig at den modtagne erklæring er relevant for den indgåede aftale. Af den modtagne erklæring fra HRE fremgår det at det er

[55] Der afgrænses fra beregningen af det statistiske stikprøvegrundlag, og vil ikke blive gennemgået yderligere

en ISAE 3000 erklæring om HR Eksperterne A/S' databehandleraftale for rekruttering, hvilket umiddelbart giver en indikation på at det er en relevant erklæring for den outsourcede aktivitet. DGI's dokumenterede gennemgang af erklæringen fremgår af bilag N og hvordan DGI forholder sig til de 4 afsnit i erklæringen og deres overvejelser hertil fremgår af det følgende.

Ledelsens udtalelse

Det fremgår af erklæringen at ledelsen udtaler sig på baggrund af deres standarddatabehandleraftale for rekruttering pr. 1. februar 2018. DGI skal vurdere hvorvidt de mener at erklæringen dækker deres indgåede databehandleraftale. Som det tidligere er nævnt, underskrev DGI HRE's standarddatabehandleraftale uden ændringer. Det fremgår af databehandleraftalens sidefod, at det er den samme databehandleraftale som der erklæres om. Da DGI har indgået en databehandleraftale med HRE efter deres standard, kan DGI konkludere at erklæringsemnet i ISAE 3000 erklæringen stemmer overens med den databehandleraftale de har indgået. Herudover skal DGI tage stilling til om den periode ledelsen udtaler sig om, også dækker den periode DGI har benyttet ydelsen. Det fremgår i databehandleraftalen at denne er underskrevet og trådte i kraft d. 4. april 2019. Af ledelsens udtalelse fremgår at erklæringsperioden er d. 1. januar 2019 til d. 31. december 2019, hvorfor DGI's benyttelse af ydelsen er inkluderet.

Den uafhængige revisors erklæring

I revisors erklæring skal DGI kontrollere det revisor erklærer sig om og hvorvidt perioden stemmer overens med det ledelsen har udtalt sig om. DGI skal endvidere forstå, at det er ledelsen i HRE, som har ansvaret for udarbejdelse, beskrivelser, udformning, implementering og effektiv udførsel af kontroller. I erklæringen skriver revisor også at HRE's beskrivelse er udarbejdet til at opfylde de almindelige behov hos en bred kreds af dataansvarlige. Her har DGI ved ledelsens udtalelse konstateret at de falder ind under denne kategori. Dertil skriver revisor at selvom der er kontroller hos en databehandler kan der stadig opstå et brud på persondatasikkerheden, samt at kontroller i fremtiden kan blive utilstrækkelige eller svigte. Til revisors konklusion skal DGI undersøge om der taget forbehold eller om der bliver fremhævet forhold. I revisors erklæring omkring HRE's rekrutteringsydelse er dette ikke tilfældet, hvorfor der ikke umiddelbart er punkter i revisors erklæring, som har betydning for DGI.

Systembeskrivelsen

Til dette afsnit skal DGI påse og forholde sig til at de behandlingsaktiviteter som beskrives stemmer overens med det indgåede. Dette betyder at DGI skal afstemme karakteren af behandling og beskrivelsen af personoplysninger til databehandleraftalens bilag A. Herudover kan de praktiske tiltag afstemmes til databehandleraftalens bilag C. I dette afsnit vil det også være synligt hvis der er aftalt yderligere krav i databehandleraftalen, som ikke er omfattet af omfanget i HRE's ISAE 3000 erklæring. Da DGI har accepteret HRE's standarddatabehandleraftale uden ændringer, vil der ikke være afvigelser af de ovennævnte forhold.

Kontrolmål, kontrolaktivitet, test og resultat heraf

I revisors konklusion var der ikke taget forbehold eller fremhævet forhold. Dette er ikke ensbetydende med at revisor ikke kan have haft bemærkninger under revisionen som DGI skal forholde sig til. I dette afsnit skal DGI se på hvilke kontrolmål der er udvalgt og tilhørende kontroller. DGI skal forholde sig til de kontroller som revisor har gennemgået og om de stemmer overens med kravene som fremgår af databehandleraftalen samt om de mener kontrollerne er tilstrækkelige til at sikre de registreredes rettigheder. For langt størstedelen af revisors test har der ikke været afvigelser, hvorfor der ikke er forhold at bemærke. DGI skal dog bemærke at revisor i sine tests af kontrol B.7 og B.11 har konstateret afvigelser, som må anses for mindre afvigelser, da de ikke har været væsentlige og har ikke givet anledning til forbehold. Når DGI skal tage stilling til kontrollerne og deres eventuelle afvigelser er det vigtigt at dette ikke kun gøres af den HR-ansvarlige. For at vurdere alle aspekter af kontrollerne er der behov for medarbejdere som både kan forstå de tekniske og organisatoriske tiltag, hvorfor den IT-ansvarlige inddrages til at vurdere de tekniske aspekter af kontrollerne.

Kontrollerne B.7 og B.11 knytter sig til kontrolmålet om de tekniske foranstaltninger. B.7 omhandler anvendelse af effektiv kryptering, hvilket stemmer overens med kravet i databehandleraftalen bilag C om at alt dataudveksling skal krypteres. Det fremgår af revisors resultat at der i Q1 2019 ikke har været anvendt sikre overførselsmetoder, men at der i de efterfølgende kvartaler har været anvendt sikre overførselsmetoder. DGI skal dermed forholde sig til om denne afvigelse har betydning for de registrerede. DGI har vurderet at afvigelsen ikke har betydning for de registrerede da afvigelsen kun har eksisteret i Q1 2019, hvor DGI ikke har benyttet sig af rekrutteringsydelsen, hvortil revisor bekræfter at afvigelsen ikke har eksisteret i de efterfølgende kvartaler. For revisors resultat af kontrol B.11 fremgår at der ved tildeling af brugeradgange har foreligget godkendelse, men at denne ikke har været dokumenteret. Igen

skal DGI vurdere om dette har betydning for deres risikovurdering. Ifølge DGI er det væsentligste for denne kontrol at der har været en godkendelse hvilket revisor bekræfter. Den manglende dokumentation er en udfordring men bliver af DGI ikke vurderet til at øge risikoen for den registrerede. DGI bør dog spørge HRE om de efter erklæringsperioden har rettet dette forhold. De ovenstående afvigelser til kontrollerne giver efter DGI's vurdering ikke anledning til at foretage yderligere handlinger og er enige i revisors betragtninger. Ved at DGI har taget stilling til omfanget af erklæringen og vurderet de afvigelser revisor har påpeget, kan DGI få en overbevisning om at HRE faktisk har handlet i overensstemmelse med den indgåede databehandleraftale i løbet af 2019. Dette betyder at DGI i alt væsentlighed kan vide sig sikker på, at både de tekniske og organisatoriske tiltag som HRE har implementeret også har været effektive. DGI skal som ved alle andre elementer i tilsynet sørge for at dokumentere dette, eksempelvis som notaen bilag N, som er den HR-ansvarlige og IT-ansvarliges gennemgang og kommentarer til den modtagne erklæring.

Som det tidligere er beskrevet består tilsynet ikke kun af stillingtagen til en erklæring. Tilsynet består af en kombination af at DGI hver måned modtager rapportering fra HRE, at de hvert kvartal udsender et spørgeskema, at de hvert år har opfølgningsmøder og at de tager stilling til den årlige ISAE 3000 erklæring. Ud fra alle de ovenstående handlinger som DGI har gennemgået og vurderet er der dermed gennemført et tilstrækkeligt tilsyn af HRE som databehandler. Denne proces med tilsyn skal gentages så længe DGI benytter HRE som databehandler. I denne case er der hidtil gennemgået de overvejelser som DGI har både før og under en aftale hvori der indgår outsourcing af behandling af personoplysninger. Det næste der vil blive gennemgået er hvordan DGI skal forholde sig når aftalen ophører, herunder overvejelser omkring sletning af personoplysninger og andre relevante aspekter i GDPR.

12.4 Overvejelser ved ophør af aftalen

Inden hovedaftalen og den tilhørende databehandling er afsluttet, skal DGI som den dataansvarlige gøre sig overvejelser omkring afslutningen af den outsourcede behandling. DGI skal sikre sig at alt deres data bliver tilbageleveret, og at HRE og deres underdatabehandler som udgangspunkt sletter alt data der tilhører DGI. Enkelte data kan være fritaget for det umiddelbare sletningskrav, såfremt der eksempelvis er igangværende klagesager eller andre gyldige behandlingshjemler. Ved tilbageleveringen skal DGI gøre dette i samarbejde med HRE's IT-afdeling og finde en måde hvorpå alt data kan blive udleveret i et læs-

bart format. I forbindelse med sletningen skal dette foregå efter at DGI har modtaget alt data. Udfordringen ved dette er at det i praksis kan være næsten umuligt for en dataansvarlig at efterse, om en databehandler faktisk har slettet data som lovet. En mulig løsning er at DGI udarbejder en tro og love erklæring, som siger at HRE har slettet alt data.

12.5 Revision af De Grønne Ingeniører A/S 2020

I forbindelse med den årlige finansielle revision er DGI's revisorer til møde med ledelsen. Til mødet har revisor bl.a. en række spørgsmål til DGI's håndtering af GDPR, som fremgår af Tabel 10 i kapitel 11. Spørgsmålene der stilles af revisor favner bredt om GDPR, hvor der hertil indgår spørgsmål omkring anvendelse af leverandører og databehandleraftaler. For casens synspunkt afgrænses der til at der kun ses på de spørgsmål der forholder sig til databehandlere. De yderligere spørgsmål vil revisor også stille, men vil ikke fremgå af denne gennemgang, hvorfor det antages at der ikke var bemærkninger til disse. I henhold til leverandører og databehandleraftaler havde revisoren følgende spørgsmål med tilhørende svar fra ledelsen som er oplistet i nedenstående tabel:

Spørgsmål fra Revisor	Svar fra ledelsen
Benyttes der leverandører hvori der videregives personoplysninger?	Ja, vi har bl.a. en leverandør som hjælper os i vores rekrutteringsproces, en leverandør som leverer et bookingsystem til booking af mødelokaler og en leverandør som leverer printersystem samt flere leverandører hvor der behandles få personoplysninger.
Foreligger der en databehandleraftale med alle leverandører der behandler personoplysninger	Ja, vi indgår en databehandleraftale hver gang vi vurderer at den outsourcede aktivitet indeholder personoplysninger.
Har i en procedure for risikovurdering af outsourcede behandlingsaktiviteter?	Ja, vi har en skala fra lav til høj, hvor vi vurderer ud fra nogle kriterier som omfanget af behandlingen og typer af information.
Fører i tilsyn med jeres databehandlere?	Ja, og omfanget af et tilsyn afhænger af vores risikovurdering.
Har i modtaget og forholdt jer til revisorerklæringer vedrørende risikofyldte databehandlere?	Ja, vi har bl.a. Modtaget en ISAE 3000 omkring vores databehandleraftale med HRE hvor vi outsourcer vores rekruttering til. I denne fremgik nogle mindre afvigelser som vi vurderede ikke havde væsentlig betydning for de registrerede.

Tabel 15: Revisors spørgsmål til DGI.
Kilde: Egen tilvirkning

DGI understøttede svarene fra Tabel 15 ved at fremvise nedenstående skema, som er et udklip af DGI's interne værktøj til at håndtere databehandlere samt udleverede bl.a. HRE's ISAE 3000 erklæring og DGI's dokumentation for gennemgang af denne.

Behandling	Leverandør	Risikovurdering	Tilsyn	Resultat af tilsyn	Kommentarer	Sidste opfølgning
Rekruttering	HR Eksperterne A/S	Mellem	Erklæring + Rapportering + Møder	OK	ISAE 3000 havde mindre afvigelser, som ikke vurderes at øge risikoen for de registrerede	D. 12. februar 2020. Gennemgang af ISAE 3000
Lokalebooking	EZ Booking ApS	Lav	Skriftlig spørgeskema årligt	OK	Ved opfølgningen var der ingen ændringer til systemet eller behandlingsaktiviteten	D. 17. december 2019. Spørgeskema modtaget retur og gennemgået
Printersystem	Printer Solutions A/S	Lav	Skriftlig spørgeskema årligt	OK	Ved opfølgningen var der ingen ændringer til systemet eller behandlingsaktiviteten	D. 14. december 2019. Spørgeskema modtaget retur og gennemgået

Billede 2: Udklip af DGI's oversigt af databehandlere.
Kilde: Egen tilvirkning

Revisor tog DGI's ovenstående svar og materiale til efterretning, hvortil det blev vurderet at der ikke var umiddelbare forhold som kunne give anledning til påvirkning på regnskabet i form af forbehold eller fremhævelse af forhold. Revisor vurderede at DGI overordnet havde styr på kontrollen med databehandlere. Overordnet så revisor heller ikke et behov for at påpege noget i erklæringen i henhold til hvorvidt ledelsen kan forventes at ifalde straf- eller erstatningsansvar, da de efter revisors vurdering havde handlet som det kunne forventes.

12.6 Opsummering af De Grønne Ingeniører A/S

Formålet med casen var igennem tænkte eksempler at vise hvordan en dataansvarlig gennemgår en proces med at benytte sig af en databehandler. Casen startede med de indledende overvejelser omkring at DGI ville outsource rekrutteringsprocessen, for derefter at konstatere at der skal indgås en databehandleraftale som regulerer forholdet mellem den dataansvarlige og databehandleren i henhold til databehandling. Derefter blev det fastlagt hvordan DGI under kontraktens levetid skulle foretage tilsyn, for at efterleve deres forpligtelse i henhold til GDPR artikel 28. DGI vurderede risikoen ved at outsource rekrutteringsprocessen til mellem. Hertil bestod DGI's tilsyn af månedlig rapportering, kvartalsvise spørgeskemaer, årlige opfølgningsmøder og årlige ISAE 3000 erklæringer om den indgåede databehandleraftale. Herefter blev det fastlagt at når aftalen er slut, skal DGI sikre sig at de får tilbageleveret alt data som er deres og herefter får HRE til at slette denne data. At kontrollere om data rent faktisk bliver slettet kan være svært, hvorfor DGI ligeledes skal få HRE til at underskrive en tro og love erklæring. Til sidst i casen blev der gennemgået hvordan den eksterne revisor ved en finansiel revision vil forholde sig til DGI og deres benyttelse af databehandlere. Hertil stillede revisor en række spørgsmål til DGI, hvortil revisor ud fra DGI's svar ikke stødte på forhold som gav anledning til hverken forbehold, fremhævelse af forhold eller ledelsesansvar.

13. Diskussion

Gennem afhandlingen er der fremlagt mange konklusioner, som giver anledning til diskussion. Dette kapitel vil kort diskutere hvilke yderligere overvejelser konklusionerne har givet anledning til.

13.1 Er man dataansvarlig eller databehandler?

I kapitel 7 blev det konkluderet hvornår en databehandlerkonstruktion opstår. Der er hertil fremlagt en række udsagn fra Datatilsynet til at foretage vurderingen af om man er dataansvarlig, hvorfor udgangspunktet bør være at det er ligetil at vurdere hvorvidt man er dataansvarlig eller databehandler. I praksis er denne adskillelse dog ikke altid tydelig, som det fremgår af de afholdte interviews og følgende udtalelser fra Respondent B og F:

Respondent B [35:17]

"Jo så er der selvfølgelig sådan noget med at diskutere om man overhovedet er databehandler (…) jeg tror næsten vi har haft størst problemer med dem der mener vi er databehandler for dem, end hvor vi mener at nogle er databehandlere for os. Vi har haft flere af sådan nogle universiteter og samarbejdspartnere der mener at vi er databehandlere for dem, der har vi haft nogle drøftelser, det løser sig ret hurtigt igen, eller nej det løser sig ikke ret hurtigt, det tager faktisk ret lang tid at få dem til at forstå det, men det løser sig altid."

Citatboks 41

Respondent F [24:03]

"Der er to af dem vi stadig ikke har fået lukket, det er lidt sjovt. Det sjove er at i begge tilfælde er vi databehandlere, det er noget vi udfører noget for Skatteministeriet som sikkert hedder Skat nu, men på et tidspunkt hed de Skatteministeriet. Vi kører nogle kørsler for dem, (...) Der har de ikke formået endnu at få underskrevet databehandleraftalen, hvor vi har sendt det til dem. Vi har ikke lyst til at være dataansvarlig, for noget som vi overhovedet ikke har noget at gøre med, vi skal nok være databehandler, vi skal nok underlægge os jeres instruktion som de jo tydeligvis ikke er helt på toppen af."

Citatboks 42

Det fremgår både af Citatboks 41 og Citatboks 42 at der, på trods af Datatilsynets udsagn, kan være udfordringer når to parter skal blive enige om hvilke roller de har. Rollen har en afgørende betydning for de forpligtelser man har over for hhv. de registrerede og dataansvarlige. Dette stiller også spørgsmålstegn til om man er omfattet af GDPR artikel 28 og den tilhørende tilsynsforpligtelse og krav til databehandleraftaler.

13.2 Udformning af tilsynet

I kapitel 9 er det konkluderet at der i en databehandlerkonstruktion vil være en forpligtelse for den dataansvarlige til at påse at dennes databehandler efterlever den indgåede databehandleraftale. Der er hertil ikke tvivl om at der jf. GDPR er krav om tilsyn for de dataansvarlige. Omfanget og fremgangsmåden af tilsynet efterlader dog meget rum til fortolkning, da dette hverken er defineret i GDPR eller af Datatilsynet. Fra GDPR står kun at de fornødne garantier skal forsikres og fra Datatilsynet fremgår af deres vejledning om tilsyn med databehandlere kun hvilke former for tilsyn der kan udføres og at tilsynet skal baseres på en risikovurdering. Definitionen af at sikre de fornødne garantier og udarbejdelsen af en risikovurdering er op til de enkelte dataansvarlige. Ved udarbejdelsen af afhandlingen, er der af forfatternes bekendtskab ikke udstedt administrative bøder for manglende overholdelse af tilsynsforpligtelsen. Dette gør det også svært for de dataansvarlige at vurdere hvorvidt et tilsyn er udført tilstrækkeligt, da der ikke er noget sædvane at basere sig på. I GPDR artikel 28, stk. 3, litra h, forpligtes databehandleren til at stille alle oplysninger til rådighed, som er nødvendige for den dataansvarlige til at påvise dennes overholdelse af kravene i artikel 28. Processen med at den dataansvarlige skal føre tilsyn med databehandleren kræver tilvænning hos databehandlerne, som forklaret af Respondent F i nedenstående citat.

Respondent F [36:26]

"Det er rimelig op ad bakke at få leverandørerne i tale, de synes det er spændende det her, men det er lidt besværligt, så vil de have betaling for at man auditerer dem til timepris og det ene eller det andet. (…) Så næste år så tror jeg det bliver lettere, for så har de også prøvet det flere gange, de bliver lidt mere komfortable i den situation. (…) De skal jo på en eller anden måde forstå at det det handler om er ikke at vi vil misbruge det til at komme ud af kontrakten. Det handler om at vi skal have en form for sikkerhed for at de rent faktisk efterlever vores instruktioner."

Citatboks 43

Respondenten fortæller i Citatboks 43, at databehandlere har svært ved at se formålet med et tilsyn. Dette kan skyldes at GDPR stadig er forholdsvist nyt, hvorfor processen omkring et tilsyn er ikke modent. De dataansvarlige og databehandlerne har brug for at forventningsafstemme hvad et tilsyn er og består af. Herudover er det også uklart hos de to parter om hvilken part der skal bære omkostningen ved et tilsyn, som det også forklares af Respondent B, da der bliver spurgt ind til udfordringer ved indgåelse af databehandleraftaler:

Respondent B [31:30]

"Der er noget med hvem betaler for hvad, hvor meget skal vi betale, eller nej ikke hvor meget, skal vi i det hele taget betale for at de hjælper os med at dokumentere deres forpligtelser. Det er noget af det."

Citatboks 44

Afstanden mellem den dataansvarlige og databehandleren kan medføre at omfanget og hyppigheden af tilsyn bliver reduceret, hvilket kan skabe en øget risiko for de registrerede, hvorfor der er et behov for at begge parter komfortable med både at udføre tilsyn og blive ført tilsyn med.

13.3 Brugen af erklæringer

I kapitel 9 er det blevet konkluderet at en revisorerklæring i form af en ISAE 3000 med udgangspunkt i den indgåede databehandleraftale, vil være en løsning for begge parter, hvis risikovurderingen kan forsvare brugen af en erklæring. Hertil må det vurderes at i kraft af at FSR – Danske Revisorers skabelon til en ISAE 3000 er ny, har denne ikke fået bred benyttelse endnu. Dette medfører at nogle dataansvarlige er tilbageholdende med at få en sådan erklæring af deres databehandlere, da den dataansvarlige kan blive pålagt omkostningen for udarbejdelsen af denne. Respondent F, udtrykker:

Respondent F [44:26]

"Jeg synes simpelthen ikke det er det værd, det koster, jeg mener prisen er 150.000 kr. for sådan en og jeg kan simpelthen ikke se at jeg får den værdi. Så vil jeg hellere selv tage ud og tale med dem. Det sku ikke det værd. For det er os der kommer til at betale for den."

Citatboks 45

Argumentet for nogle dataansvarlige for ikke at anvende en ISAE 3000, er dermed at denne er for omkostningstung på nuværende tidspunkt. Hertil kan det dog diskuteres hvorvidt en ISAE 3000 på baggrund af den indgåede databehandleraftale kan blive branchestandard i fremtiden. Omkostningen vil dermed kunne blive spredt ud til mange kunder, som det er på nuværende tidspunkt med bl.a. en ISAE 3402. Hertil forklarer Respondent F, hvordan denne forestiller sig fremtiden kunne se ud:

Respondent F [44:26]

"Jamen man kan godt sige, lige nu er standarden en 3402, sådan har det været i 10 år i hvert fald. Nu bliver det måske det samme for den nye, så laver man på tværs af kunder og så siger man i dækket af denne her, så vil jeg selvfølgelig tage imod den. Så vil den have højere værdi end 3402'eren fordi begge dele er gratis, og indkalkuleret i prisen på forhånd. Men at købe den for 150, det kan jeg simpelthen ikke se. Det kan jo være den eneste mulighed for at dække sig ind."

Citatboks 46

Den overordnede værdi af en erklæring kan diskuteres, da en databehandler vil være forberedt når revisor kommer på besøg for at udføre sine revisionshandlinger. Det kan tænkes at databehandleren vil sikre sig at alt er i orden i netop den periode revisor er forbi. Dette er også en bemærkning som fremgår i revisors erklæring, men bør ikke negligeres. Denne risiko vil dog altid eksistere, også når den dataansvarlige selv er på besøg hos databehandleren. Det kan endvidere diskuteres hvilken værdi brugen af erklæringer inden for GDPR kan have for den eksterne revisor. Det er konkluderet hvordan den eksterne revisor igennem den udarbejdede tjekliste kan få en overbevisning om den der bliver revideret, efterlever GDPR. På nuværende tidspunkt fylder GDPR ikke meget i den eksterne revision, men det kan tænkes at dette kan blive aktuelt i fremtiden. Dette kan blive aktuelt enten ved et ændret fokus fra revisor, eller hvis der bliver udstedt mange bøder indenfor GDPR. Såfremt bødemængden stiger voldsomt kan revisor være påtvunget at spørge ind til GDPR, da en bødestørrelse kan være væsentlig. Til dette kan det tænkes at den eksterne revisor, som det i dag fungerer med en ISAE 3402, adspørge den der revideres om en ISAE 3000 erklæring for dermed at opnå overbevisning for overholdelse af bl.a. tilsynsforpligtelsen i henhold til GDPR igennem en anden revisors arbejde.

13.4 Giver et tilsyn værdi?

Fra EU's side er formålet med GDPR at værne om de registreredes rettigheder og frihedsrettigheder. Det kan diskuteres om tilsynsforpligtelsen skaber en reel værdi for de registrerede, eller om det blot er et formelt krav som de dataansvarlige skal overholde. Det må vurderes at ved at stille krav om tilsyn vil sikkerheden for de registrerede blive øget, hvorfor der faktisk er en værdi i et tilsyn. Tilsynsforpligtelsen er blot en af mange tiltag i GDPR, men skaber alt andet lige en øget værdi for de registrerede, da der skabes kontrol over behandlingen af deres personoplysninger.

13.5 Opsummering af diskussion

Diskussionen bærer præg af at både GDPR og FSR – Danske Revisorers erklæringsskabelon er forholdsvis nyt. For de diskuterede emner betyder det at det er svært at konkludere om noget er rigtigt eller forkert, da der indenfor området ikke er meget historik at basere sig på.

Der er diskuteret hvorvidt der er en klar skillelinje for at identificere sig som dataansvarlig eller databehandler. Diskussion ender ud i at der ikke er en klar skillelinje på trods af at Datatilsynet har udarbejdet en række udsagn netop til at klarlægge dette forhold. Denne manglende identifikation af hvilken rolle hver part har, kan medføre at man ikke kan efterleve sine forpligtelser overfor de registrerede.

Herudover er det tidligere blevet konkluderet at der ikke tvivl om at man som dataansvarlig har en tilsynsforpligtelse overfor databehandlerne. Det er hertil blevet diskuteret hvorvidt de dataansvarliges tilsynshandlinger er tilstrækkelige, da der hverken fra GDPR eller Datatilsynet fremgår klare retningslinjer for hvor omfattende et tilsyn skal være og hvilken fremgangsmåde man skal arbejde efter. Hertil er det også konstateret at det er vigtigt at afklare hvilken part der skal pålægges omkostningen ved et tilsyn. Konsekvensen for manglende afklaring er øget risiko for de registrerede.

I diskussionen er det vurderet at udbredelsen af en ISAE 3000 erklæring på baggrund af en indgået databehandleraftale stadig er begrænset. Erklæringsskabelonen er forholdsvis ny både for de dataansvarlige og databehandlerene, hvorfor de skal have tid til at vænne sig til den. Hertil diskuteres det at den største barriere på nuværende tidspunkt er, at der ikke er en kritisk masse af kunder, hvorfor omkostningen sandsynligvis vil ramme den enkelte dataansvarlige, som medfører at erklæringen ikke bliver udarbejdet. Det diskuteres afslutningsvis at det måske i en nærmere fremtid kan blive en branchestandard, på samme måde som en ISAE 3402 samt hvorvidt et tilsyn har en reel værdi for de registrerede.

14. Konklusion

Som følge af de nye sanktionsmuligheder i kraft af GDPR, er beskyttelse af personoplysninger blevet et højaktuelt emne for de omfattede organisationer. De dataansvarlige har overfor de registrerede en forpligtelse til at værne om deres personoplysninger, uagtet om behandlingen bliver outsourcet. For at analysere problemstillingen har der været en kvalitativ undersøgelse hvortil der er foretaget seks interviews med de parter der indgår i databehandlerkonstruktion og eksterne parter som kan indgå i processen, enten som rådgiver eller uafhængig tredjepart.

Afhandlingen tager afsæt i forholdet mellem en dataansvarlig og dennes databehandler i en databehandlerkonstruktion. Af GDPR artikel 5, stk. 1, fremgår de grundlæggende principper for behandling af personoplysninger som en dataansvarlig har ansvaret for at overholde til enhver tid. Det er nødvendigt at have med i overvejelserne at man som dataansvarlig aldrig kan outsource sit ansvar overfor de registrerede. Det er i afhandlingen blevet konkluderet at når der outsources behandlingsaktiviteter der vedrører personoplysninger, kan der opstå en databehandlerkonstruktion. Til at fastslå om en databehandlerkonstruktion eksisterer er der i afhandlingen oplistet en række udsagn som kan bruges af begge parter til at identificere deres rolle.

I en databehandlerkonstruktion stiller GDPR artikel 28, stk. 3, formaliserede krav til udarbejdelse af en databehandleraftale. Databehandlerens forpligtelser er herefter fastlagt ud fra Datatilsynets standard-databehandleraftale. Det konkluderes at databehandleren skal stille de fornødne garantier overfor en dataansvarlig ved bl.a. at indføre organisatoriske og tekniske tiltag og bistå den dataansvarlige i dennes forpligtelser overfor de registrerede. I GDPR fremgår ikke eksplicit at den dataansvarlige skal føre tilsyn med sine databehandlere. Det konkluderes dog at artikel 28 må fortolkes at dette er et krav, da der samtidig opstår et principal-agent forhold med asymmetrisk information og muligvis forskellige incitamenter og modstridende interesser. En dataansvarlig vil ikke kunne leve op til ansvarlighed jf. GDPR artikel 5, stk. 2, eller sikre de fornødne garantier, hvis et tilsyn ikke udføres. Den dataansvarliges tilsyn vil variere afhængig af fremgangsmåde og de vurderede risici. Der findes to måder at føre tilsyn på, enten som skriftlige informationsindsamlinger eller fysiske besøg. De skriftlige tilsynshandlinger inkluderer bl.a. spørgsmål til databehandleren og løbende rapportering. De fysiske besøg vil bl.a. inkludere besigtigelse, stikprøver og test af kontroller. Førend den dataansvarlige kan udføre et tilstrækkeligt tilsyn, er denne nødt til at vurdere alle dens outsourcede behandlingsaktiviteter og inddele dem i forskellige

risikogrupper. Til at foretage denne vurdering er der opstillet en række kriterier, der giver indikation om risikoniveauet for de registreredes rettigheder og frihedsrettigheder. Ud fra afhandlingen opdeles risikoniveauet i henholdsvis lav, mellem og høj. Hertil er der udarbejdet en matrix som ud fra den vurderede risiko oplister tilsynshandlinger. I denne matrix fremgår at der ved en lav risiko ikke vil være behov for andet end skriftlige informationsindsamlinger, mens der ved en høj risiko vil være behov for at udføre både fysiske besøg og skriftlige informationsindsamlinger. Ved at udføre et tilsyn baseret på en risikovurdering opnår en dataansvarlig sikkerhed for at en databehandler efterlever den indgåede databehandleraftale.

For alle tilsynshandlinger skal den dataansvarlige vurdere hvorvidt denne selv vil udføre handlingerne, eller benytte sig af en ekstern part for derefter at vurdere den eksterne parts resultater. Den eksterne part kan eksempelvis være en advokat eller revisor. Revisor vil hertil være et oplagt valg, da denne er underlagt regulering som sikrer et troværdigt produkt. Hvis revisor benyttes vil dette typisk være igennem afgivelse af en erklæring af typen ISAE 3000. Den dataansvarlige skal gennemgå og vurdere revisors resultater førend erklæringen kan indgå som en tilsynshandling. Hvordan den dataansvarlige skal vurdere denne og hvad en ISAE 3000 erklæring indeholder er gennemgået. Den dataansvarlige skal tage stilling til erklæringens fire overordnede afsnit, ledelsens udtale, uafhængig revisors erklæring, systembeskrivelse og kontrolmål, kontrolaktivitet, test og resultat heraf. For hvert af de fire afsnit skal den dataansvarlige gennemlæse og vurdere disse. Omfanget af en ISAE 3000 erklæring kan variere og typisk vil være til en bred kreds af dataansvarlige, hvorfor den enkelte dataansvarlige skal sammenholde og vurdere omfanget af erklæringen med dennes egen databehandleraftale. Det fastlås endvidere at selvom der foreligger en blank påtegning, er det ikke ensbetydende med at der ikke kan være forhold af betydning for den dataansvarlige. Eventuelle afvigelser skal derfor vurderes af den dataansvarlige og om disse har indvirkning på vurderingen af risikoen for de registrerede. Såfremt afvigelser vurderes at have betydning skal der iværksættes mitigerende handlinger.

Manglende efterlevelse af GDPR hos den dataansvarlige kan have en væsentlig indflydelse regnskabet i form af bøder, hvortil manglende tilsyn med databehandlere blot er et område som kan føre til bøder. Der er blevet konkluderet at revisor grundet en eventuel væsentlig indvirkning af GDPR er nødt til at tage stilling til dette under en finansiel revision. Hertil opdeler ISA 250.6 regulering i to kategorier, som er regulering med og uden direkte indvirkning på regnskabet, hvor GDPR falder i sidstnævnte kategori. Revisor skal derfor foretage handlinger for at få en overbevisning om hvorvidt selskabet der revideres

overholder GDPR. Til dette er der udarbejdet en række spørgsmål som revisor kan stille. Disse spørgsmål har til formål at give revisor en forståelse for om virksomheden der revideres har forholdt sig til GDPR, hvorfor der alt afhængigt af svarene kan være behov for yderligere substansrevision. Revisor kan have en forpligtelse til at rapportere om GDPR i regnskabet. Dette vil være tilfældet hvis revisor mener at der skal hensættes til en bøde, som virksomheden ikke har hensat, eller i form af fremhævelse af forhold omkring eventuelt straf- og erstatningsansvar for ledelsen.

For at illustrere alle afhandlingens overvejelser og konklusioner er der opstillet en fiktiv case omkring De Grønne Ingeniører A/S der outsourcer deres rekrutteringsproces til HR Eksperten A/S. Casens struktur er en tilnærmelsesvis spejling af den øvrige analysestruktur, hvorfor der heri indgår både overvejelser før, under og efter en aftale og databehandleraftale bliver indgået. Før aftalens indgåelse blev der overvejet hvorvidt området overhovedet skulle outsources, og derefter hvordan en leverandør blev udvalgt. Under aftalen blev der gennemgået de tilsynshandlinger som De Grønne Ingeniører A/S foretog, med inddragelse af både den konkrete databehandleraftale og revisors ISAE 3000 erklæring på baggrund heraf. Ved aftalens udløb blev der undersøgt hvordan De Grønne Ingeniører A/S skulle sikre at deres leverandør ville slette og tilbagelevere alle personoplysninger om deres registrerede. Yderligere blev der inddraget De Grønne Ingeniører A/S' eksterne revisor og hvordan denne forholder sig under en finansiel revision.

15. Perspektivering

Afhandlingens resultater kan være svære at generalisere, da der er begrænsninger i den anvendte metode, da afhandlingens resultater er baseret på få respondenter, samt forfatterenes egne fortolkninger af vejledninger, artikler, love m.m. Det kunne tænkes at der ved at bruge flere dataindsamlingsmetoder, såsom både kvalitative og kvantitative i kombination, ville have skabt et mere nuanceret og bredere perspektiv. Spørgeskemaer kunne eksempelvis være udarbejdet og udsendt til mange respondenter, for at kortlægge overordnede tendenser indenfor tilsynsforpligtelsen, risikovurdering og brugen af erklæringer. Herudover kunne det også have været relevant at have haft flere respondenter. En anden mulighed kunne også være at have afholdt fokusgrupper eller observationsstudier, for igen at skabe et bredere perspektiv af problemstillingen. I henhold til både respondenter og forfatternes ressourcer, ville dette dog være for tidskrævende.

Et andet aspekt der besværliggører generaliserbarheden ved afhandlingen er at GDPR kun har været gældende siden maj 2018, hvorfor afhandlingen har et kort tidsperspektiv. Det kunne tænkes at vurderingen af både tilsyn, risiko og brugen af erklæringer kan ændre sig over tid, som følge af ændret praksis, ny sædvane, vejledninger fra tilsynsmyndigheder eller domme og administrative bøder.

Afslutningsvis kunne det tænkes, at den eksterne revisor, i stil med den udarbejdede tjekliste, i sine fremtidige revisioner begyndte at have fokus på GDPR. Såfremt dette blev tilfældet, kunne dette have en afledt effekt på de dataansvarlige, som igen kunne ændre deres adfærd omkring hele tilsynsforpligtelsen og indvirkningen af GDPR.

Litteraturliste

Faglitteratur

- Voxted, S. (2006). **Valg der skaber viden – om samfundsvidenskabelige metoder**, Hans Reitzels forlag. S. 52-66. ISBN: 9788776754525.
- Andersen, I. (2014) **Den skinbarlige virkelighed (5. udgave),** Samfundslitteratur. ISBN: 9788759316504**.**
- Guba, E. (1990). **The Paradigm Dialog.** SAGE Publications. S. 17-27. ISBN: 9780803938236.
- Tvarnø, C. D. & Nielsen, R. (2017). **Retskilder og retsteorier (5. udgave)**. Jurist- og Økonomforbundets Forlag. ISBN: 9788757437645
- Jacbobsen, D. I. & Thorsvik, J. (2014). **Hvordan organisationer fungerer - en indføring i organisation og ledelse (3. udgave)**, Hans Reitzels forslag. ISBN: 978874125860
- Eilifsen, A., Messier JR, W. F., Glover S. M. & Prawitt, D. F. (2014). **Auditing & Assurance Services.** Mc-Graw Hill Education. ISBN: 9780077143015
- Füchel, K., Gath, P., Langsted, L. B., Olsen, P. K. & Skovby, J. (2017). **Revisor – Regulering & Rapportering.** Karnov Group Denmark. ISBN: 9788761939593.
- Dall, N. P. & Langemark, J. (2018). **Persondataforordningen – en håndbog for praktikere (2. udgave)**. Ex Tuto Publishing. ISBN: 9788742000175
- Udsen, H. (2016). **IT-RET. (3. udgave)**. Ex Tuto Publishing. ISBN: 9788792598455

Vejledninger og rapporter

- Datatilsynets **skabelon til standarddatabehandleraftale** (16. februar 2018). Hentet fra: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2018/feb/ny-skabelon-skal-hjaelpe-virksomheder-og-myndigheder-med-at-blive-klar-til-databeskyttelsesforordningen/
- Datatilsynets **følgetekst til standarddatabehandleraftale** (16. februar 2018). Hentet fra: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2018/feb/ny-skabelon-skal-hjaelpe-virksomheder-og-myndigheder-med-at-blive-klar-til-databeskyttelsesforordningen/
- Datatilsynets **vejledning om dataansvarlige og databehandlere** (november 2017). Hentet fra: https://www.datatilsynet.dk/media/6560/dataansvarlige-og-databehandlere.pdf
- Datatilsynets **vejledende tekst om tilsyn med databehandlere og underdatabehandlere** (maj 2018). Hentet fra:

https://www.datatilsynet.dk/media/6865/vejledende-tekst-om-tilsyn-med-databehandlere-og-underdatabehandlere.pdf

- Europa-Kommissionen. **Må andre behandle oplysninger på vegne af vores organisation?** Hentet fra: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/can-someone-else-process-data-my-organisations-behalf_da?fbclid=IwAR2Y9YhsWCac8Kp7LDGT6GeH_BjAqpgFa9-fNUFgrfoGoaxFyK6C7Lda9mQ
- Europa-Kommissionen. **Hvad er en dataansvarlig eller databehandler?** Hentet fra: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_da

Lovgivning, regulering og domme

- EU-forordning (27. april 2016). **Europa-Parlamentets og Rådets forordning (EU) 2016/679** Hentet fra: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:32016R0679
- EU-direktiv (24. oktober 1995). **Europa-Parlamentet og rådets direktiv 95/46/EF** Hentet fra: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:31995L0046
- EU-charter (26. oktober 2012). **Den Europæiske Unions Charter om grundlæggende rettigheder 2012/C 326/02**
  Hentet fra: **https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:12012P/TXT**
- Dansk lov (23. maj 2018). **Databeskyttelsesloven.**
  Hentet fra: **https://www.retsinformation.dk/Forms/r0710.aspx?id=201319**
- Dansk lov (20. november 2018). **Revisorloven.**
  Hentet fra: https://www.retsinformation.dk/Forms/R0710.aspx?id=203860
- Dansk bekendtgørelse (12. december 2017). **Bekendtgørelse om godkendte revisorers erklæringer**. Hentet fra: https://www.retsinformation.dk/Forms/R0710.aspx?id=194872

Revisionsstandarder

- **Etiske regler for revisorer** (15. juli 2017). FSR – Danske Revisorer.

- ISA 250 (2017). **Overvejelser vedrørende love og øvrig regulering ved revision af regnskaber.** International Auditing and Assurance Standards Board (IAASB).
- ISA 300 (2009). **Planlægning af revision af regnskaber.** International Auditing and Assurance Standards Board (IAASB).
- ISA 315 (2013). **Identifikation og vurdering af risici for væsentlig fejlinformation igennem forståelse af virksomheden og dens omgivelser**. International Auditing and Assurance Standards Board (IAASB).
- ISA 700 (2016). **Udformning af en konklusion og afgivelse af erklæring om et regnskab**. International Auditing and Assurance Standards Board (IAASB).
- ISAE 3000 (2015). **Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger**. International Auditing and Assurance Standards Board (IAASB).
- ISAE 3000 erklæringsskabelon (2017). **Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger**. FSR – Danske Revisorer. Hentet fra: https://www.fsr.dk/Faglige_informationer/Om_revisor/Persondataforordningen/Erklaering%20om%20persondata_210917
- ISAE 3000 erklæringsskabelon (2019). **Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med [Dataansvarlig]**. FSR – Danske Revisorer. Hentet fra: https://fsr.dk/Faglige_informationer/Om_revisor/Persondataforordningen/FSR%20lancerer%20paa%20baggrund%20af%20samarbejde%20med%20Datatilsynet%20ny%20erklaering%20om%20persondata

Artikler og hjemmesider

- Bjørn-Hansen, S. (20. juli 2016). **Eksperter om CPR-læk: Amatøragtig omgang med data.** DR. Hentet den 14. maj 2019 fra: https://www.dr.dk/nyheder/viden/tech/eksperter-om-cpr-laek-amatoeragtig-omgang-med-data
- Datatilsynet (25. maj 2019). **Datatilsynet indstiller taxaselskab til bøde på 1,2 mio. kr.** Datatilsynet. Hentet den 14. maj 2019 fra:

https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/mar/datatilsynet-indstiller-taxaselskab-til-boede-paa-1-2-mio-kr/

- Andersen, L. H. (10. december 2018). **Yousee lækker 4.800 kunders skjulte navne og adresser**. Version2. Hentet den 14. maj. 2019 fra: https://www.version2.dk/artikel/yousee-laekker-4800-kunders-skjulte-navne-adresser-1087000
- (26. november 2018). **Tysk chat-app får GDPR-bøde for at lagre kodeord i klartekst.** Version2. Hentet den 14. maj 2019 fra: https://www.version2.dk/artikel/tysk-chat-app-faar-gdpr-boede-at-lagre-kodeord-klartekst-1086886
- Østergaard, C. (26. november 2018). **Datatilsynet: Ringe video-evner ugyldigt argument for ikke at udlevere overvågningsklip.** Version2. Hentet den 14. maj 2019 fra: https://www.version2.dk/artikel/datatilsynet-ringe-video-evner-ugyldigt-argument-ikke-at-udlevere-overvaagningsklip-1086872
- (23. november 2018). **Tyskland udsteder sin første GDPR-bøde.** Version2. Hentet den 14. maj 2019 fra: https://www.version2.dk/artikel/tyskland-udsteder-sin-foerste-gdpr-boede-1086870
- **GDPR Fines and Penalties.** Nathan Trust. Hentet den 14. maj 2019 fra: https://www.nathantrust.com/gdpr-fines-penalties?fbclid=IwAR28I6j2NUwMMbypzi5PPa7gh79MOx3CCECvRHn2u1IinCk9G3IYELoaFcA

Bilagsoversigt