BEGREBET DATAANSVARLIG EFTER GDPR

af August Skoubo Hasselbalch

Engelsk titel: The concept of data controller according to GDPR

Forfatter: August Skoubo Hasselbalch, studienummer: 20195243

Studie: Erhvervsøkonomi-jura HA (jur.)

Vejleder: Tanja Kammersgaard Christensen

Abstract

This thesis has investigated when one is considered a data controller according to Regulation (EU) 2016/679, including whether a private individual and a manufacturer can be considered data controllers because of the processing of their product. The thesis has analyzed the definition of a “data controller” as well as the scope of the regulation. The scope is broad, and almost all processing of personal data is covered. However, private individuals can be exempted from the scope if their processing is of a purely personal or household activity.

The thesis can conclude that a data controller can be a natural or legal person, public authority, agency or other body who participates in determining the purposes and means of processing. In this regard, it is possible for several individuals to be joint data controllers, but also be individually responsible for the processing. In cases where several data controllers are joint data controllers, obligations may not necessarily be evenly distributed but instead depends on the specific situation. This is assessed based on who is in the best position to observe and comply with the obligations.

Finally, the thesis has applied this knowledge to the processing of personal data carried out by a robotic vacuum cleaner. It can be concluded that private individuals using the vacuum cleaner in their own home would fall under the exemption of the scope and therefore not be subject to the Regulation's scope. However, the manufacturer can still be considered a data controller regardless of whether the buyer is one.

The crucial factors here are whether the manufacturer has determined the purposes and means of processing. The manufacturer has, in all cases, determined the purpose of the processing by choosing to use cameras in their product. They have specified the purpose in the specific example to be household monitoring. However, they would not be considered a data controller if the private individual chooses to take this robot vacuum cleaner to a public area, as it would not be used for the purpose specified by the manufacturer. The producer is unlikely to be considered the data controller if the buyer simply uses the product as a security camera in their home. In this case, the buyer can turn it on and off, thus solely controlling the devices and, to some extent, their purpose."

The buyer can also become a data controller if they themselves determine the purpose of the processing. This will notably occur if the product is used for purposes other than those specified by the manufacturer. Additionally, the buyer will also be a data controller for the processing that involves storing the video recordings or if the buyer otherwise shares this information on the internet.

Indholdsfortegnelse

Indledning

Den teknologiske udvikling har medført en digital tidsalder, hvor enorme mængder af persondata konstant indsamles og behandles. Begrebet dataansvarlig og dennes forpligtelser er derfor blevet endnu vigtigere for at beskytte fysiske personer i forbindelse med behandlingen af personoplysninger. I centrum af denne beskyttelse findes begrebet dataansvarlig, som er den vigtigste rolle i forhold til at sikre at personoplysninger behandles i en grad, der medfører individet tilstrækkelig beskyttelse. Forståelsen af, hvem det er der bærer ansvaret og netop hvordan man vurderer dette er derfor vigtigt.

Forståelsen af begrebet dataansvarlig udvikles løbende i takt med flere afgørelser på området og flere vejledninger, der vedrører specifikke typer af behandling, men i samme tempo som disse afgørelser og vejledninger udstedes, udvikler teknologien sig yderligere og skaber endnu flere problemstillinger.

Det er derfor nødvendigt at undersøge dette begreb og forsøge at opstille en række kriterier, som taler for og imod at en person kan være dataansvarlig. Hvilke områder kan man med sikkerhed beslutte, hvem den dataansvarlige er og hvilke områder er stadig uklare. Løsningen er ikke blot at identificere, hvem der er mest dataansvarlig, da flere personer godt kan være fælles dataansvarlige. Denne konstruktion åbner yderligere op for et hav af overvejelser, hvor det kræver en skarp vurdering af den konkrete situation og undersøger hvorvidt disse behandlere er med til at bestemme formål og hjælpemidler.

For at vurdere hvorvidt en person er dataansvarlig, skal der tages udgangspunkt i forordningens definition af dataansvarlig. Denne definition indeholder flere underliggende begreber, som er nødvendige at forstå, for at kunne vurdere hvorvidt man er dataansvarlig eller ej. Forordningen er underlagt en dynamisk fortolkning for at følge med den teknologiske udvikling og der er i den forbindelse, en række nyere problemstillinger, som begynder at dukke op. For hvem er egentlig dataansvarlig, når producenten løbende kan opdatere og desuden behandler personoplysninger ved hjælp af det produkt de har solgt? Den teknologiske udvikling gør det svært at følge med i rækkevidden og der opstår mere komplekse situationer, hvor definitionerne for formål og hjælpemidler bliver sværere og sværere at placere.

Problemformulering

Denne afhandling vil undersøge generelt om, hvornår man er dataansvarlig, som defineret i forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (herefter Forordningen), art. 4, nr. 7. Derudover hvorvidt en producent og en køber kan blive dataansvarlig på baggrund af producentens produkt.

I denne forbindelse vil Forordningens anvendelsesområde og principperne om databehandling blive undersøgt, for at undersøge hvilke principper, som den dataansvarlige skal iagttage, men også for at vurdere, hvornår man er dataansvarlig. Det vil først blive undersøgt generelt om, hvilke relevante bestemmelser, der knytter sig til at vurdere om man er dataansvarlig og herefter de betragtninger der lægges vægt på i praksis ved denne vurdering. Herefter vil det blive undersøgt, i hvilket omfang man er dataansvarlig, som henholdsvis producent og som køber af et produkt. Afhandlingens primære formål er at klarlægge hvornår man er dataansvarlig, som defineret i Forordningen. Afhandlingen vil behandle spørgsmålet ud fra tragtmetoden, ved at starte bredt med de generelle definitioner, dernæst undersøge relevante afgørelser og til sidst anvende denne viden på et konkret produkt, for at vurdere hvorvidt producenter og købere kan blive dataansvarlige.

På baggrund af ovenstående er problemformuleringen for denne afhandling følgende:

"Hvornår er man dataansvarlig ifølge EU-forordning 2016/679 om databeskyttelse og kan en køber og en producent være dataansvarlig på baggrund af et produkt?"

Afgrænsning

Dette speciale vil ikke inddrage andre lovgivninger end Databeskyttelsesforordningen. Der er beskrevet en række scenarier, hvor tv-overvågningsloven og straffeloven kan være relevant og i nogle tilfælde også medføre, at de udtænkte scenarier aldrig ville være relevante i forhold til Forordningen. Disse scenarier vil dog udelukkende blive behandlet ud fra Databeskyttelsesforordningen, men det anerkendes, at disse scenarier sandsynligvis ville blive behandlet anderledes i praksis, pga. tv-overvågningsloven og straffeloven. Scenarierne er dog stadig relevante i diskussionen om Forordningen og er derfor udtænkt for at behandle denne bedst muligt.

Principperne og behandlingsgrundlag vil blive behandlet i specialet, men de yderligere forpligtelser vil ikke blive undersøgt, da disse ikke er relevante i vurderingen af, om man er dataansvarlig eller ej. Der vil derudover heller ikke blive undersøgt, hvilke sanktioner der vil være aktuelle, ved ikke at overholde Forordningen, da dette heller ikke er relevant for specialets problemformulering.

Overførsel til tredjelande vil desuden heller ikke blive behandlet, selvom denne problemstilling er aktuel i specialets afsluttende behandling af scenarier. Producenten er fra Asien og der sker derfor sandsynligvis overførsel til tredjelande ved behandlingen af personoplysninger. Dette er dog heller ikke relevant i forhold til at vurdere hvorvidt producenten er dataansvarlig eller ej og vil derfor ikke blive inddraget. Det ville dog være relevant for at forstå samtlige implikationer af den behandling som robotstøvsugerne foretager.

Der vil blive undersøgt danske afgørelser, men national lovgivning, som fungerer som tillæg til Forordningen, vil ikke blive inddraget, da dette speciale vil fokusere på, hvornår man er dataansvarlig i Forordningen. Der vil dog blive inddraget nogle få danske afgørelser, men disse henviser ikke til de supplerende bestemmelser der fremgår af Databeskyttelsesloven.

Behandlingssikkerhed vil ikke blive gennemgået yderligere end det der fremgår om privacy-by-design og privacy-by-default, da disse behandlingsskridt er særligt relevante for en producent, som er dataansvarlig.

Metode

Dette speciales problemformulering vil blive undersøgt ved at analysere og beskrive gældende ret. Der anvendes derfor den retsdogmatiske metode, hvis formål er at analysere og beskrive retsregler på et område, finde eller fastlægge almindelige regler og principper for et retsområde, systematisere retsregler og analysere systematikken, forholde sig til hypotetiske eller faktiske konflikter, og præcisere eventuel retlig tvivl.[1]

På baggrund af dette, vil specialet analysere og beskrive de retsregler, der vedrører Forordningens anvendelsesområde og hvornår man i henhold til Forordningen er dataansvarlig. Derudover vil principperne for Forordningen blive fastlagt og understøtte den efterfølgende systematisering af retsreglerne. Specialet vil systematisere kravene og de elementer der lægges vægt på i vurderingen af, hvorvidt man er dataansvarlig. Til sidst vil denne viden blive anvendt på både hypotetiske og en faktisk "konflikt" og det vil i den forbindelse blive fastslået, hvilke situationer man er dataansvarlig og hvilke man ikke er – og i de situationer hvor dette ikke endegyldigt kan fastslås, præciseres den retlige tvivl.

Specialet vil anvende en række retskilder. Den centrale retskilde i specialet vil være Forordningen, hvor relevante bestemmelser vil blive anvendt. Det er denne forordnings definition af dataansvarlig, som skal undersøges. Fremgangsmåden for alle de delområder, der skal undersøges for at afdække problemformuleringen, vil først og fremmest bestå af en ordlydsfortolkning. Herefter vil relevante afgørelser analyseres for at fastslå gældende ret og derved supplere ordlydsfortolkningen. Derudover vil præambelbetragtningerne, vejledninger og til dels retslitteratur inddrages, selvom disse ikke er bindende retskilder, kan de sammen med de bindende retskilder, hjælpe med at uddybe disse betragtninger. Retskilderne vil blive anvendt i den førnævnte rækkefølge og der vil derfor også lægges mest vægt på de retskilder, som har den største retskildeværdi.

[1] (Munk-Hansen, 2018), s. 205

Kapitel 1. Forordningens anvendelsesområde

For at kunne undersøge, hvorvidt man er dataansvarlig i henhold til Forordningen, er det nødvendigt at fastslå Forordningens anvendelsesområde. Forordningens materielle og territorielle anvendelsesområde vil derfor blive undersøgt i dette kapitel.

Kapitel 1.1 Det materielle anvendelsesområde

Forordningens materielle anvendelsesområde følger af Forordningens artikel 2, stk. 1.

"Denne forordning finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register."

Bestemmelsen fastslår forordningens anvendelsesområde og det følger af ordlyden, at anvendelsesområdet er gældende, når der sker *"behandling"* af *"personoplysninger"* og at disse desuden enten *"helt eller delvist foretages ved hjælp af automatisk databehandling"* eller *"vil blive indeholdt i et register"*. Det er derfor disse begreber, der er nødvendige at undersøge, for at finde ud af præcis hvad det materielle anvendelsesområde dækker. Begreberne er defineret i forordningens art. 4 og vil blive undersøgt i de følgende afsnit.

Kapitel 1.1.1 Behandling

Begrebet *"behandling"* er defineret i forordningens art. 4, nr. 2, som:

" Enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse."

Definitionen er meget bred og indeholder en ikke-udtømmende liste af eksempler på behandling af personoplysninger. Det er derfor som udgangspunkt alle aktiviteter der falder ind under denne definition. Udsen mener dog, at *"sporadiske og atypiske behandlinger"* såsom oplysninger, der midlertidigt kopieres på en internetudbyders servere, ikke vil være omfattet af denne definition. [2]

[2] (Udsen, 2022), s. 69

Kapitel 1.1.2 Personoplysning

Begrebet personoplysning er defineret i forordningens art. 4, nr. 1:

"Enhver form for information om en ***identificeret eller identificerbar fysisk person*** *(»den registrerede«); ved identificerbar fysisk person forstås en fysisk person, der* ***direkte eller indirekte*** *kan identificeres, navnlig ved en* ***identifikator*** *som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet"*

Begrebet dækker over enhver information om en identificerbar fysisk person, som i forordningen er defineret som *"den registrerede"*. Den registrerede forstås som en fysisk person, der direkte eller indirekte kan identificeres.

Definitionen skelner imellem identificeret og identificerbar person, hvor den identificerede person direkte kan forbindes med personoplysningerne, eksempelvis navn, adresse eller andre oplysninger, der direkte kan forbindes med denne person. En identificerbar person er modsat en person, hvor tilknytningen af personoplysninger umiddelbart kræver flere "efterforskningsskridt", eller yderligere oplysninger for at identificere, men hvor det trods alt stadig er realistisk at kunne forbinde denne person med personoplysningerne. Denne vurdering er kommenteret i præambelbetragtning 26 i Forordningen, hvori der står at afgørelsen af, hvorvidt en fysisk person er identificerbar, beror på en rimelighedsvurdering af de midler, der tænkes at bringes til anvendelse i udpegelsen af personen, derudover indikerer EU-lovgivers brug af ordet indirekte, at en personoplysning ikke nødvendigvis forudsætter, at den alene gør det muligt at identificere den registrerede, jf. sag C-582/14, præmis 41. Herunder er blandt andet tid og omkostninger væsentligt i vurderingen. Det behøver derfor ikke at være umuligt at kunne forbinde personoplysningen med personen, for at det ikke falder ind under denne definition, men det beror i stedet på en vurdering af, hvorvidt det er rimeligt. I sag C-582/14 udtalte EU-domstolen, at hvis identificeringen enten var forbudt ved lov eller praktisk uigennemførlig *"f.eks. på grund af det forbehold, at den vil indebære en større indsats i tid, omkostninger og arbejde, således at risikoen for en identificering i virkeligheden synes ubetydelig"* ville der ikke være tale om en identificerbar person. Udgangspunktet som tages med videre i undersøgelsen er således, at alle oplysninger, som med få skridt kan forbindes til en fysisk person, er en personoplysning som defineret i Forordningen. Et billede eller en videooptagelse af en fysisk person ville f.eks. være en personoplysning, da dette billede ville være en "*identifikator"* der er "*særlig for denne fysiske persons fysiske identitet"*.

Kapitel 1.2.3 Automatisk databehandling og manuelle registre

Det tidligere kriterie i persondatadirektivets art. 3, stk. 1, var at behandlingen var foretaget "ved hjælp af edb", men denne definition er i den nye forordning ændret til "automatisk databehandling". Dette kan tyde på en udvidelse af begrebet og afspejles også i dansk ret, hvor en manuel videregivelse af elektroniske oplysninger udgjorde elektronisk behandling, jf. U.2011.2343H.

Manuelle registre er derimod sværere at afgrænse definitionen af. Dette er defineret som en samling af personoplysninger, der er tilgængelig efter bestemte kriterier. Dette indebærer blot, at personoplysningerne let skal kunne hentes frem, jf. C-25/17, præmis 57. Dette er derfor en forholdsvis bred definition, hvor man kun kan forestille sig en rodebunke med dokumenter undtagelsesvist kan være udenfor Forordningens anvendelsesområde.

Kapitel 1.2.4 Delkonklusion

Er der tale om en *personoplysning* og er der tale om *automatisk behandling* eller *behandling* af personoplysninger indeholdt i et register? Selvom disse krav skal vinges af, før vi er indenfor Forordningens anvendelsesområde - så er de alle bredt defineret. Det betyder at man i praksis, oftest er indenfor det materielle anvendelsesområde, lige så snart der er tale om personoplysninger. Det centrale er derfor at vurdere, hvorvidt der er tale om en personoplysning og i så fald, er man sandsynligvis indenfor det materielle anvendelsesområde. Der er en række undtagelser hertil og særligt én af disse er relevant, når man skal vurdere hvorvidt privatpersoner kan være dataansvarlige eller ej. Denne bestemmelse vil blive undersøgt i næste kapitel.

1.3 Privatreglen

Forordningens materielle anvendelsesområde er bredt og behandlingen vil som hovedregel, som tidligere fastslået, være omfattet af Forordningen, hvis behandlingen vedrører personoplysninger. Alligevel er der dog en række undtagelser og her er bestemmelsen om privatreglen særlig relevant i forhold til private personer, der behandler oplysninger. Derfor vil denne bestemmelse også blive undersøgt ud fra specialets overordnede problemformulering om, hvornår man er dataansvarlig. De andre undtagelser vil ikke blive gennemgået.
Privatreglen, som er en undtagelse til anvendelsesområdet, er at finde i Forordningens artikel 2, stk. 2, punkt c. Denne bestemmelse er afgørende for at vurdere hvornår private personer er undtaget fra Forordningens anvendelsesområde – og modsat, hvornår de kan være dataansvarlige. I bestemmelsen står følgende:

"Denne forordning gælder ikke for behandling af personoplysninger: som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter".

Bestemmelsen svarer til den lignende bestemmelse i det tidligere databeskyttelsesdirektiv artikel 3, stk. 2, 2. pind.[1] Der har derfor, som udgangspunkt, ikke været en hensigt med at ændre gældende ret. Bestemmelsen er derfor en videreførelse af den tidligere bestemmelse, med de tilføjelser der fremgår af præambelbetragtning 18. Afgørelser, bemærkninger, fortolkninger m.m. der er afsagt med udgangspunkt i den tidligere bestemmelse i databeskyttelsesdirektivet, er derfor stadig relevante. EU-domstolen har også fastslået dette i afgørelser i den nye Forordning. Dette vedrører kun de bestemmelser, som behandles i afgørelsen, men tendensen ses i langt de fleste afgørelser. Domstolen udtalte eksempelvis i sag C-597/19 følgende: *"Da forordning 2016/679 har ophævet og erstattet direktiv 95/46, og da de relevante bestemmelser i forordningen i det væsentlige har samme indhold som de relevante bestemmelser i direktivet, finder Domstolens praksis vedrørende direktivet principielt ligeledes anvendelse på forordningen)."*

Bestemmelsen omfatter udelukkende "*fysiske personer"*, som behandler personoplysninger i "*rent personlige eller familiemæssige aktiviteter"* og forudsætter således at disse to betingelser er opfyldt. Det er svært at vurdere denne artikels anvendelsesområde ud fra ordlyden, da det ikke er defineret i Forordningen hvad dette dækker over. Eksempler herpå fremgår dog af Forordningens præambelbetragtning 18. Heri står der, at bestemmelsen modsætningsvist ikke dækker, hvis der er en forbindelse til erhvervsmæssig eller kommerciel aktivitet. Derudover oplistes der en række eksempler, der er dækket af denne bestemmelse. Disse eksempler er: *"korrespondance og føring af en adressefortegnelse eller sociale netværksaktiviteter og onlineaktiviteter, der udøves som led i sådanne aktiviteter"*. Ved aktiviteter skal forstås *"personlig eller familiemæssig aktivitet"* som formuleret i bestemmelsen. Præambelbetragtningerne anvendes som fortolkningsbidrag.

Denne liste er ikke udtømmende, da formuleringen er, at aktiviteterne *kan* omfatte ovenstående. Samtidig er disse eksempler heller ikke absolut fritaget fra Forordningens anvendelsesområde. De principielle afgørelser omhandler primært onlineaktiviteter eller sociale netværksaktiviteter og det er også disse, der vil blive undersøgt for at fastslå retstilstanden på området.

Det er tidligere blevet undersøgt hvad behandling af personoplysninger indebærer og det er derfor de to ovenstående krav i bestemmelsen, der er nødvendig at undersøge, for at forstå bestemmelsens anvendelsesområde – eller undtagelsesområdet.

Fysiske personer

Formuleringen *Fysiske personer* indebærer, ud fra en ordlydsfortolkning, at virksomheder og andre juridiske personer ikke er omfattet af denne undtagelse. Dette betyder yderligere at databehandling foretaget af politiske partier, velgørende organisationer og andre foreninger ikke er omfattet.[3] Afgrænsningen af hvornår fysiske personer, som medlemmer af en organisation behandler personoplysninger og hvornår der er tale om, at organisationen behandler oplysninger er uklar og der kan derfor være situationer, hvor det konkret skal vurderes, om privatreglen kan påberåbes – afhængigt af om det er den fysiske person eller organisationen der behandler personoplysningerne.[4]
Privatpersonen der deler personoplysninger, som privat person i egen fritid, kan være omfattet af bestemmelsen. Der er en række betragtninger der afholder privatpersonen fra at undgå Forordningens anvendelsesområde. Deltagelse i debatter om sportsfolk blev fastslået til at være dækket under *"rent personlig karakter"* i Justitsministeriets besvarelse af 13. april 1999 af spørgsmål nr. 89 (pkt. 19.1.b) vedrørende lovforslag nr. L 44.
Sag C-101/01 (herefter Lindqvist-sagen) omhandler en person, med tilknytning til en kirkelig menighed, som havde oprettet en hjemmeside på hendes private computer, som skulle hjælpe til konfirmationsforberedelser. Denne hjemmeside indeholdt en række personoplysninger, herunder helbredsoplysninger. Hertil konkluderede domstolen, at undtagelsen skal fortolkes, således at den *"kun vedrører de aktiviteter, der indgår i den enkelte borgers privatliv eller familieliv, hvilket åbenbart ikke er tilfældet med hensyn til behandling af personoplysninger, som består i, at de offentliggøres på internettet, hvorved disse personoplysninger bliver tilgængelige for et ubestemt antal personer."*[5].
Domstolen udtalte desuden i sag C-25/17 (herefter omtalt som Jehovas Vidner) at undtagelsen: *"Udelukkende vedrører de aktiviteter, der indgår i den enkelte borgers privatliv eller familieliv. I denne forbindelse kan en aktivitet ikke anses for at være rent personlig eller familiemæssig som omhandlet i denne bestemmelse, når dens* ***formål*** *er at gøre* ***personoplysninger tilgængelige for et ubestemt antal personer****, eller når denne aktivitet endda – om end kun delvist – omfatter det* ***offentlige rum*** *og derfor er rettet uden for privatsfæren for den, der foretager* ***behandlingen*** *af disse oplysninger"*
Disse afgørelser fastslår, at det er nødvendigt at kigge på, hvorvidt udlæggelsen af personoplysninger videregives til en lukket privat kreds eller et ubestemt antal personer, som der også blev lagt vægt på i Lindqvist-sagen, hvor artiklen blev fortolket indskrænkende og derfor lagde grundlag for at

[3] (Udsen, 2022), s. 74
[4] IBID
[5] Præmis 47

hovedreglen som udgangspunkt er, at offentliggørelse af personoplysninger på internettet ikke er omfattet af undtagelsesreglen.

En anden nævneværdig afgørelse er C-212/13, František Ryneš, hvor det blev fastslået at opsætning af et kamerasystem på privat grund heller ikke er omfattet af undtagelsen, såfremt det filmer ud på offentlig grund. Afgørelsen i František Ryneš afspejler Jehovas Vidner-sagen i forhold til, at undtagelsen ikke gælder offentliggørelse af personoplysninger til et ubestemt antal personer, eller hvis aktiviteten omfatter **det offentlige rum**. Undtagelsens anvendelsesområde skal derfor fortolkes indskrænkende, sandsynligvis for at undgå omgåelse af reglerne.

Konsekvensen for de fysiske personer, hvis behandling falder ind under Forordningens anvendelsesområde og derved ikke er omfattet af privatreglen, er at de på lige fod med private virksomheder skal efterleve de forpligtelser, som Forordningen fastsætter, men at de samtidig er berettiget til at behandle personoplysninger under de samme betingelser.[6]

1.3 Det territoriale anvendelsesområde

Det territoriale anvendelsesområde følger af Forordningens art. 3.

*"**1.** Denne forordning finder anvendelse på behandling af personoplysninger, som foretages som led i aktiviteter, der udføres for en dataansvarlig eller en databehandler, som er etableret i Unionen, uanset om behandlingen finder sted i Unionen eller ej.*

***2.** Denne forordning finder anvendelse på behandling af personoplysninger om registrerede, der er i Unionen, og som foretages af en dataansvarlig eller databehandler, der ikke er etableret i Unionen, hvis behandlingsaktiviteterne vedrører:*

***a)** udbud af varer eller tjenester til sådanne registrerede i Unionen, uanset om betaling fra den registrerede er påkrævet, eller*

***b)** overvågning af sådanne registreredes adfærd, for så vidt deres adfærd finder sted i Unionen.*

***3.** Denne forordning anvendes på behandling af personoplysninger, som foretages af en dataansvarlig, der ikke er etableret i Unionen, men et sted, hvor medlemsstaternes nationale ret gælder i medfør af folkeretten."*

Denne bestemmelse omfatter både dataansvarlige og databehandlere, som behandler personoplysninger, på vegne af en dataansvarlig eller databehandler der er etableret i Unionen, uanset om behandlingen finder sted i Unionen. Derudover også for alt behandling af registrerede i Unionen,

[6] (Lotterup & Nielsen, 2020), s. 220

foretaget af en dataansvarlig eller databehandler, der ikke er etableret Unionen, hvis behandlingsaktiviteterne vedrører udbud af varer eller tjenester, uanset om betaling af dette er påkrævet, eller hvis der sker overvågning af de registreredes adfærd i Unionen. I forhold til at skulle vurdere, om en person eller virksomhed er dataansvarlig, er der derfor to scenarier, som skal undersøges, for at fastlægge hvornår den dataansvarlige er indenfor det territoriale anvendelsesområde.

Dataansvarlige etableret i EU

Hvis den dataansvarlige er etableret i EU, vil denne, i henhold til art. 3, stk. 1, være omfattet af det territoriale anvendelsesområde, uanset om behandlingen foregår indenfor eller udenfor EU. Definitionen af "etableret" er mere vidtrækkende end blot "oprettet". I sag C-230/14, vurderede EU-domstolen at kravet om "etablering" er opfyldt, når den dataansvarlige har en permanent struktur i landet. I sagen blev en Tjekkisk-registreret virksomhed, fastslået til at være etableret i Ungarn, fordi der var oprettet hjemmesider på ungarsk og at virksomheden havde en repræsentant med bopæl i Ungarn. I Google Spain-dommen (C-131/12) medførte Googles datterselskab, som var etableret i Spanien og primært stod for annoncesalg (og derved ikke havde noget at gøre med Googles behandling), at Googles behandling af personoplysninger var omfattet af den spanske persondatalov, da annonceaktiviteterne var et "led i aktiviteter". Begrebet "etableret" består derfor af en bred definition i Forordningen og virksomheder med en "uløselig forbindelse" til en dataansvarlig eller databehandler indenfor EU er også ofte omfattet af det territoriale anvendelsesområde.

Dataansvarlig ikke etableret i EU

Hvis den dataansvarlige ikke er etableret i EU, er der to scenarier hvor den dataansvarlige stadig vil være indenfor Forordningens territoriale anvendelsesområde. Den første er når der bliver udbudt varer eller tjenesteydelser til borgere i EU. Dette krav er ikke opfyldt blot fordi der er adgang til en hjemmeside i det pågældende land, heller ikke selvom denne hjemmeside er på det lokale sprog, jf. præambelbetragtning 23. Det er dog ifølge præambelbetragtningen en konkret vurdering, hvor flere faktorer skal være til stede. Her vil sprog, valuta og omtale af brugere i Unionen være med til at fastslå, hvorvidt den dataansvarlig påtænker at udbyde varer eller tjenesteydelser i Unionen, jf. Forordningens præambelbetragtning 23. Bestemmelsen indebærer også brugere af gratis ydelser, såsom sociale medier og andre internettjenester.[7] Bestemmelsens litra b, indebærer også overvågning

[7] (Udsen, 2022), s. 84

af de registreredes adfærd. Her nævnes i præambelbetragtning 24, at dette kan være fysiske personernes adfærd på nettet, som efterfølgende anvendes til at analysere eller forudsige den pågældendes præferencer, adfærd og holdninger. Dette vil man blandt andet se i forhold til markedsføring på internettet.[8]

Det territoriale anvendelsesområde er, ligesom det materielle anvendelsesområde, bredt. En producent udenfor EU, der sælger til det europæiske marked, vil falde ind under dette anvendelsesområde og derfor være forpligtet i henhold til Forordningen. Det er selv for dataansvarlige udenfor EU, svært at undgå anvendelsesområdet og det er derfor vigtigt for alle virksomheder, der behandler personoplysninger, at vurdere hvorvidt de er omfattet af det territoriale anvendelsesområde.

1.4 Delkonklusion

Forordningens materielle og territoriale anvendelsesområde er blevet undersøgt. Dertil også den relevante undtagelse i art. 2, stk. 1. Det kan konkluderes, at anvendelsesområdet er bredt og at det forsimplet vil omfatte stort set alle der behandler personoplysninger i Unionen, men der er samtidig også en mulighed for private, for at være undtaget af anvendelsesområdet.

Det er herefter relevant at undersøge hvilke forpligtelser den dataansvarlige skal iagttage, når dennes aktiviteter falder ind under Forordningens anvendelsesområde.

Kapitel 2. Forpligtelser som dataansvarlig

Følgende afsnit vil forsøge at fastslå, hvorfor det er relevant at placere et dataansvar samt hvilke forpligtelser den dataansvarlige skal iagttage. Dette vil senere anvendes som fortolkningsbidrag, i forhold til hvad hensigten er med at finde den dataansvarlige.

I takt med den teknologiske udvikling har der været et øget fokus på privatlivets fred. I den moderne informationsteknologiske verden, har de øgede muligheder for at dele informationer og derved personoplysninger betydet, at privatlivets fred har været truet. En personoplysning i sig selv involverer typisk en forventning om privatliv og set i et historisk perspektiv har mennesket altid ønsket selv at være herre over, hvilke informationer de deler. Nogle oplysninger vælger man at dele med ens intimsfære, andre oplysninger vælger man at dele med hele sin sociale kreds og nogle

[8] (Udsen, 2022), s. 84

oplysninger ønskes måske helt hemmeligholdt. Individet har aldrig helt selv kunne bestemme, hvilke oplysninger der videredeles fra eksempelvis intimsfæren, men en eventuel videredeling har været langsom og er blevet begrænset af ens egen sociale sfære. Historisk har det ikke været relevant for en virksomhed i London at vide hvad en tilfældig person i Hjørring Kommune har af helbredsproblemer, men i det moderne samfund er det mere relevant end nogensinde at vide disse "ligegyldige" oplysninger om tilfældige personer på tværs af landegrænser og disse oplysninger indsamles og sælges af tech-giganter verden over. Det er næsten lige meget hvor vi færdes på internettet, så indsamles der adskillige personoplysninger igennem blandt andet cookies, som videresælges til højeste bud. Informationsteknologiens udvikling har betydet, at retten til at tilbageholde private oplysninger er blevet begrænset, som følge af de øgede muligheder for at dele oplysninger samt den øgede efterspørgsel efter disse personoplysninger. Man er derfor ikke længere herre over sine oplysninger i samme omfang, som man tidligere har været.

Databeskyttelsesforordningen fastslår at beskyttelsen af fysiske personer i forbindelse med behandlingen af disses personoplysninger, er en grundlæggende rettighed. Det fastsættes at enhver har ret til beskyttelse af de personoplysninger som vedrører denne, jf. Den Europæiske Unions charter om grundlæggende rettigheder, artikel 8, stk. 1 og i traktaten om Den Europæiske Unions Funktionsmåde (TEUF), artikel 16, stk. 1. Præambelbestemmelserne i Forordningen fastslår, at reglerne og principperne for beskyttelse af fysiske personer i forbindelse med behandling af disses personoplysninger, bør respektere deres grundlæggende rettigheder og frihedsrettigheder. Formålet med forordningen er desuden at bidrage til at skabe et område med frihed, sikkerhed og retfærdighed. Det fastslås desuden at retten til beskyttelse ikke er en absolut ret, men skal ses i dens sammenhæng med resten af samfundet og afvejes i forhold til andre grundlæggende rettigheder og i overensstemmelse med proportionalitetsprincippet. Forordningens mål er altså at beskytte dele af individets grundlæggende menneskerettigheder ved at beskytte individets personoplysninger. Med rettigheder følger modsat også en forpligtelse fra den anden part og det er derfor relevant at undersøge, hvem der er forpligtet, og i et vist omfang, hvad disse forpligtelser indebærer.

Følgende afsnit vil gennemgå de behandlingsprincipper, som skal iagttages i henhold til Forordningen.

2.1 De grundlæggende behandlingsprincipper

Følgende afsnit vil gennemgå de grundlæggende principper for behandling af personoplysninger, samt hvem der skal iagttage disse principper.

Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes, jf. Forordningen, artikel 5, stk. 2. Dette kaldes også princippet om ansvarlighed og er den centrale forpligtelse der pålægges den dataansvarlige i forordningen. De omtalte principper vil blive gennemgået, for at fastlægge vigtigheden i, at identificere den dataansvarlige.

2.1.1 Lovlighed, rimelighed og gennemsigtighed

Det følger af Forordningens, art. 5, stk. 1, litra a, at *"Oplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede"*.

Denne bestemmelse har samme ordlyd, som det tidligere databeskyttelsesdirektiv artikel 6, stk. 1, litra a og også persondatalovens § 5, stk. 1. Denne bestemmelse kan derfor forstås i overensstemmelse med hidtil gældende ret.[9] Bestemmelsen medfører en "bred retlig standard", som giver mulighed for at opsætte krav til behandlingen af personoplysninger, som ikke direkte følger af forordningen.[10] Dette er tidligere set i det gamle databeskyttelsesdirektiv, hvor der blev indført en pligt til at informere om sikkerhedsbrud, som i den nye forordning er fastsat i art. 33 og 34.[11] Bestemmelsen var tidligere implementeret som et krav om "god databehandlingsskik" og dette begreb anvendes stadig som udtryk for de krav, der følger af den nuværende bestemmelse.[12] Kravet om lovlighed, fastsætter at behandlingen skal følge Forordningens bestemmelser, herunder både de specifikke krav, men også det nævnte krav om god databehandlingsskik.

Princippet om gennemsigtighed, er beskrevet i præambelbetragtning 39:

[...] Princippet om gennemsigtighed tilsiger, at enhver information og kommunikation vedrørende behandling af disse personoplysninger er lettilgængelig og letforståelig, og at der benyttes et klart og enkelt sprog. Dette princip vedrører navnlig oplysningen til de registrerede om den dataansvarliges identitet og formålene med den pågældende behandling samt yderligere oplysninger for at sikre en rimelig og gennemsigtig behandling for de berørte fysiske personer og deres ret til at få bekræftelse og meddelelse om de personoplysninger vedrørende dem, der behandles [...]

Bestemmelsen og den dertilhørende præambelbetragtning, medfører individet en bred beskyttelse og kræver at behandlingen er gennemsigtig og derved også giver den registrerede en god mulighed for at gennemskue den behandling, der foretages af den registreredes personoplysninger. Princippet

[9] (Lotterup & Nielsen, 2020), s. 314
[10] (Udsen, 2022), s. 127
[11] IBID
[12] IBID

medfører således et krav om, at enhver registrerede, skal kunne gennemskue hvordan deres personoplysninger behandles og i hvilket omfang de behandles. Princippet relaterer sig til reglerne om oplysningspligt, indsigtsret og princippet om ansvarlighed.

2.1.2 Formålsbegrænsning

Det fremgår af art. 5, stk. 1, litra b, at personoplysninger skal *"indsamles til udtrykkeligt angivne og legitime formål og ikke må viderebehandles på en måde, der er uforenelig med disse formål".* Dette kaldes også for princippet om formålsbestemthed. Denne bestemmelse indebærer, at den dataansvarlige, skal "beslutte" sig for formålet inden behandlingen finder sted. Dette formål skal være "udtrykkeligt" angivet og kan derfor ikke bero på en bred formulering. Eksempler på brede formuleringer kan ifølge Udsen være "improving user's experience", "marketing purposes", "IT security purposes".[13] Dette medfører at virksomheder ikke kan anvende en bred formulering, som et fremtidssikkert formål, men i stedet skal begrænse sig til det på forhånd-bestemte formål med indsamlingen. Dette betyder også, at en dataansvarlig ikke kan viderebehandle indsamlede oplysninger, til et formål, der ikke var fastlagt på forhånd. Hvorvidt viderebehandlingen er "*uforenelig"* med det oprindelige formål ved indsamlingen, beror på en konkret vurdering.[14] Dette ville kræve en ny indsamling til det nye formål. Princippet er i korte træk en forhindring imod fri viderebehandling, men der ligger samtidig et krav om "legitime formål". Dette indebærer et krav om, at formålene er i overensstemmelse med Forordningen og anden lovgivning.

I praksis kunne man forestille sig, at et formål blot ville kunne blive "opfundet" lang tid efter man har indsamlet samtlige oplysninger og vurderet, hvilke man skal bruge og hvilke man ikke skal bruge. Dette er dog ikke muligt, da den dataansvarlige, som tidligere nævnt, har en pligt til at kunne dokumentere at Forordningen overholdes og derudover følger der en oplysningspligt ift. de registrerede af artikel 13 og 14 i forordningen.

2.1.3 Dataminimering

Det fremgår af art. 5, stk. 1, litra c, at personoplysninger skal *"være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles"*. Dette kaldes også for princippet om dataminimering. Ordlyden i bestemmelsen er meget lig dens praktiske anvendelse og den spiller sammen med princippet om formålsbegrænsning. Det er ikke tilladt at indsamle

[13] (Udsen, 2022), s. 129
[14] (Lotterup & Nielsen, 2020), s. 322

oplysninger der ikke er nødvendige i forhold til det formål de behandles. I en afgørelse af 11. februar 2019, Dt.s jr.nr. 2018-31-0070, fastslog Datatilsynet at TDC's behandling af personoplysninger var i strid med denne bestemmelse. TDC lagde til grund at de var forpligtet efter logningsbekendtgørelsen til at registrere lokaliseringsdata for al mobildatatrafik. Datatilsynet fastslog dog, at størstedelen af de personoplysninger som TDC indsamlede, ikke var nødvendige for at overholde logningsbekendtgørelsen og de behandlede derfor flere personoplysninger end nødvendigt. Databehandlingen gik udover det formål TDC havde fastlagt med indsamlingen og var derfor i strid med art. 5, stk. 1, litra c. Bestemmelsens anvendelsesområde beror på en konkret vurdering og det kan dermed ikke siges, at alt dataophobning ville være i strid med denne bestemmelse.[15] Korfits og Lotterup skelner imellem en konkret efterspørgsel og en frivillig opgivelse af personoplysninger i et eksempel, om en dataansvarlig myndighed, der i forbindelse med sagsbehandling behandler oplysninger, som ikke nødvendigvis er relevante for selve sagsbehandlingen og deraf databehandlingen. De antager, at det næppe kan være nødvendigt for den dataansvarlige myndighed *"at gennemgå relevansen og nødvendigheden af hver enkelt oplysning i sagen".*[16] Denne betragtning stemmer også overens med en tidligere afgørelse, Dt.s j.nr. 2018-41-0016 om biometrisk data, hvor datatilsynet anvendte proportionalitetsprincippet i deres vurdering, om at en biometrisk løsning til at foretage entydig identifikation af bloddonere var for indgribende, set i forhold til hvad der kræves til opfyldelse af formålet, og bemærkede at det samme ville gælde efter databeskyttelsesforordningen, art. 5, stk. 1, litra c.

2.1.4 Rigtighed

Det fremgår af art. 5, stk. 1, litra d, at personoplysninger skal *"være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges".* Dette kaldes også princippet om rigtighed og forpligter den dataansvarlige til at sikre at personoplysninger er rigtige. I praksis ville dette oftest indebære ajourførelse og derved berigtigelse af forældede oplysninger. Kontrollen med disse personoplysninger vil afhænge af oplysningernes karakter, deres anvendelse, indsamlingens pålidelighed og af om oplysningerne er af betydning for en eller flere myndigheder, virksomheder m.v.[17] Den registrerede kan selv anmode om berigtigelse, sletning eller begrænsning af oplysninger, jf. forordningen, art. 16-18. Der gælder dog ikke en absolut forpligtelse til at slette alt,

[15] (Lotterup & Nielsen, 2020), s. 329
[16] Ibid
[17] (Lotterup & Nielsen, 2020), s. 331

der kan betegnes som urigtigt, da det i praksis kan være nødvendigt at opbevare, for at kunne dokumentere det faktuelle grundlag, som eksempelvis en afgørelse er truffet ud fra.[18] Dette betyder i praksis, at selvom oplysninger senere viser sig at have været forkerte fra start af, eller senere er blevet det, kræver dette ikke at oplysningerne slettes eller berigtiges, da der kan være behov for at opbevare disse i deres oprindelige form for at kunne dokumentere. For offentlige myndigheder, gælder henholdsvis en notatpligt og journaliseringspligt, jf. offentlighedslovens §§ 13 og 15. Denne pligt fratager offentlige myndigheder fra denne bestemmelses sletteplig, men vil i praksis betyde at offentlige myndigheder i stedet retter den urigtige oplysning, eksempelvis med en kommentar.[19].

For private virksomheder kan der også være en interesse i, at kunne dokumentere et faktuelt grundlag på et senere tidspunkt, hvor oplysningerne viser sig at være urigtige. Eksempelvis oplysninger der har været relevante i forhold til at indgå eller ophæve en aftale. Her vil der i stedet skulle tilføres et notat, der anfører de korrekte oplysninger.[20] Korfits og Lotterup mener, at en egentlig sletning oftest kræves, hvis der er tale om oplysninger, der indgår i et register som tilgår andre dataansvarlige, men de anmærker desuden, at der selv i denne situation, kan være grunde til at opbevare tidligere versioner. I ordlyden *"straks slettes eller berigtiges"* vil det altså oftest være handlingen af berigtigelse der bruges i praksis. Såfremt behandlingen af personoplysninger ikke strider imod princippet om dataminimering, vil de færreste virksomheder have en reel interesse i at slette oplysninger. Det kræver ikke noget at have dem liggende og det kan være svært at gennemskue oplysningernes fremtidige relevans.

2.1.5 Opbevaringsbegrænsning

Det fremgår af art. 5, stk. 1, litra e, at personoplysninger skal *"opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder"*

[18] (Lotterup & Nielsen, 2020), s. 332
[19] (Lotterup & Nielsen, 2020), s. 334
[20] Ibid

Ordlyden i denne bestemmelse indebærer en forpligtelse til at slette eller anonymisere personoplysninger, når disse ikke længere er nødvendige at opbevare, til det formål de blev indsamlet. Et konkret eksempel herpå, er videooptagelser fra overvågning. Det vil næppe være nødvendigt at lagre disse i en længere periode, hvis formålet blot er at kunne identificere en indbrudstyv. Hvis man dagligt har mulighed for at opdage, hvorvidt der er sket et indbrud, vil det ikke være nødvendigt at lagre videooptagelser i flere år.

2.1.6 Integritet og fortrolighed

Det fremgår af art. 5, stk. 1, litra f, at personoplysninger skal *"behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger"*. Bestemmelsen er et udtryk for princippet om behandlingssikkerhed[21] og fungerer enten som en forsmag på, eller en understregelse af vigtigheden af, artikel 32. Der er ingen afgørelser, der konkret har henvist til denne bestemmelse, hvilket kan tyde på, at den blot eksisterer for at fastlægge behandlingssikkerheden som et centralt princip der skal efterleves. Artikel 32 uddyber kravene til behandlingssikkerheden, men vil ikke yderligere blive gennemgået.

2.2 Privacy-by-default og Privacy-by-design

Artikel 25 stiller krav til at behandlingssikkerheden skal iagttages igennem hele behandlingsprocessen – også ved udviklingen eller produktionen af en løsning eller et produkt. Følgende fremgår af bestemmelsen:

"1. Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, som behandlingen indebærer, gennemfører den dataansvarlige både på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen passende tekniske og organisatoriske foranstaltninger, såsom pseudonymisering, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper, såsom dataminimering, og med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i denne forordning og beskytte de registreredes rettigheder.

[21] (Lotterup & Nielsen, 2020), s. 340

2. Den dataansvarlige gennemfører passende tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, behandles. Denne forpligtelse gælder den mængde personoplysninger, der indsamles, og omfanget af deres behandling samt deres opbevaringsperiode og tilgængelighed. Sådanne foranstaltninger skal navnlig gennem standardindstillinger sikre, at personoplysninger ikke uden den pågældende fysiske persons indgriben stilles til rådighed for et ubegrænset antal fysiske personer.
3. En godkendt certificeringsmekanisme i medfør af artikel 42 kan blive brugt som et element til at påvise overholdelse af kravene i nærværende artikels stk. 1 og 2."
Denne bestemmelse kræver, at den dataansvarlige tilvejebringer et tilstrækkeligt sikkerhedsniveau både før behandlingen finder sted og under selve behandlingen, navnlig ved at gennemføre passende tekniske og organisatoriske foranstaltninger. Disse foranstaltninger kan være pseudonymisering, sikkerhed imod hackerangreb, generelt sikkerhed imod at uvedkommende får fat i de behandlede personoplysninger og virusprogrammer. Bestemmelsen hænger sammen med behandlingsprincipperne og forpligter den dataansvarlige til at iagttage disse principper under udviklingen, eksempelvis ved at indføre automatisk sletterutine eller andre foranstaltninger, som sikrer overholdelsen af Forordningen.

Dette medfører en problemstilling, hvis producenten ikke kan anses som dataansvarlig. Hvis en køber er den eneste der er dataansvarlig for den behandling som et produkt udfører, er det ifølge ordlyden af denne bestemmelse, køberen der skal sørge for at privacy-by-default og privacy-by-design efterleves. Det er dog i praksis ikke særlig nærliggende for køberen at skulle sikre sig at disse krav er efterlevet. Denne problemstilling vil blive undersøgt yderligere i kapitel 4.

2.3 Delkonklusion

Nærværende kapitel har fastlagt, hvilke principper for behandling af personoplysninger, som der skal behandles personoplysninger efter. Derudover også en række forpligtelser, som den dataansvarlige skal efterleve. Princippernes bestemmelser er blevet gennemgået og en række afgørelser er blevet undersøgt, for at fastslå hvordan principperne anvendes i praksis samt hvilke betragtninger datatilsynet lægger vægt på i deres afgørelser omkring disse bestemmelser. Dette vil fungere som reference til de næste kapitler og de scenarier der vil blive undersøgt. For at vurdere de gråzoner, hvor der på nuværende tidspunkt ikke foreligger afgørelser, vil det forrige kapitel hjælpe til at danne en idé om, hvordan disse gråzoner eventuelt ville blive betragtet i fremtidige afgørelser, og disse

principper vil dermed også hjælpe til at fastslå, hvornår man egentlig er dataansvarlig, eller hvem der burde være dataansvarlig, i forhold til den beskyttelse man ønsker opnået for fysiske personer.

Kapitel 3. Hvornår er man dataansvarlig

3.1 Definition af dataansvarlig

Dataansvarlig defineres i Forordningens artikel 4, nr. 1. som: *"**en fysisk eller juridisk person**, en offentlig myndighed, en institution eller et andet organ, der **alene eller sammen med andre afgør**, til hvilke **formål** og med hvilke **hjælpemidler** der må foretages **behandling** af **personoplysninger**; hvis formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret, kan den dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret"*

Begrebet dataansvarlig er sammen med begrebet databehandler et af de mest centrale begreber i Forordningen, da det er disse begreber, der afgør hvem der er ansvarlig for at overholde databeskyttelsesreglerne. Det er samtidig også primært den dataansvarlige, som de registrerede kan udøve deres rettigheder overfor, hvilket gør den dataansvarlige absolut nødvendig i beskyttelsen af de registreredes rettigheder.

Definitionen på "dataansvarlig" i Forordningen kan inddeles i 5 underliggende definitioner, som hver især skal undersøges, for at forstå den samlede definition på dataansvarlig. Definitionerne af behandling og personoplysninger er allerede blevet undersøgt og vil derfor ikke være inkluderet i denne analyse. De resterende 4 definitioner vil hver især blive undersøgt:

- "en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ"
- "afgør"
- "alene eller sammen med andre"
- "formål og hjælpemidler

3.1.1 Den dataansvarlige som person, offentlig myndighed eller institution

Definitionen fastslår at den dataansvarlige kan være *"en fysisk person eller juridisk person, en offentlig myndighed, en institution eller et andet organ"*

Det er i forbindelse med privatreglen defineret hvad en fysisk person er og modsætningsvist hvad en juridisk person er. I praksis vil det oftest være organisationen, der er dataansvarlig og ikke en enkeltperson i denne virksomhed. I Jehovas-vidner sagen udtalte domstolen dog at den daværende bestemmelse skulle *"fortolkes således at et trossamfund kan holdes ansvarligt, sammen med dets forkyndende medlemmer, for behandlingen af personoplysninger foretaget af sidstnævnte ... uden at det i denne forbindelse er påkrævet, at trossamfundet har adgang til disse oplysninger, eller at det har udstedt skriftlige retningslinjer eller anvisninger til dets medlemmer vedrørende denne behandling".* En sammenslutning af personer kan derfor godt være dataansvarlig og desuden være fælles dataansvarlig uden at begge dataansvarlige har adgang til de indsamlede oplysninger. I nærværende sag, forudsatte dette dog at trossamfundet organiserede, koordinerede og tilskyndede behandlingen. Denne betragtning vil blive uddybet senere.

Det er dog som udgangspunkt organisationen der vil være dataansvarlig og ikke den bestemte fysiske person, som påtager sig ansvaret i organisationen eller virksomheden.[22] Medarbejderen anses i stedet som personer der udfører arbejde for den dataansvarlige og er underlagt en forpligtelse om, kun at behandle personoplysninger efter instruks, jf. Forordningen, art. 29.[23] En medarbejders behandling der uretmæssigt overskrider sine beføjelser og derfor behandler personoplysninger til eget brug, vil ikke blive anset som at udføre behandling under organisationens kontrol. Organisationen er dog forpligtet som dataansvarlig, til at sikre tilstrækkelige tekniske og organisatoriske foranstaltninger, jf. Forordningen, art. 26, stk. 1.

3.1.2 "Afgør"

I definitionen anvendes ordet "afgør" i forbindelse med formålene og hjælpemidlerne og dette vedrører dataansvarliges *indflydelse* på behandlingen i kraft af en *beslutningstagningsbeføjelse*.[24] For at være dataansvarlig kræver det, at man træffer beslutning om visse nøgleelementer i behandlingen.[25] For at beslutte hvorvidt man er dataansvarlig, skal man enten definere dette ud fra de faktiske omstændigheder eller ved lov – sidstnævnte kan eksempelvis være en offentlig opgave der består i at

[22] (EDPB, Retningslinjer 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse), s. 11
[23] IBID
[24] (EDPB, Retningslinjer 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse), s. 12
[25] IBID

indsamle personoplysninger, eller en privat virksomhed der for at overholde lovgivning, er nødt til at indsamle personoplysninger.[26]

Ved de faktiske omstændigheder skal der lægges vægt på, hvem der tog beslutningen om at behandlingen skulle finde sted og hvilket formål denne behandling har. Hvem er det der gavner fra behandlingen og hvem er den nødvendig for.[27]

Vurderingen kan bero på de faktiske omstændigheder, herunder kan kontraktvilkår hjælpe med at fastslå, hvem der er dataansvarlig. Dette forudsætter dog at kontraktvilkårene stemmer overens med virkeligheden og det er derfor ikke muligt, igennem en kontrakt, at unddrage sig de dataansvarlige forpligtelser – og modparten kan modsat heller ikke påtage sig disse forpligtelser.[28] Hvis en part derfor i praksis bestemmer formål og hjælpemidler, men det i kontrakten er formuleret således, at denne part er databehandler – vil denne part være dataansvarlig og derved forpligtet som dataansvarlig.

3.1.3 ”Alene eller sammen med andre”

Definitionen anerkender, at behandlingen af formål og hjælpemidler kan afgøres alene eller sammen med andre. En behandling kan derfor godt foretages af flere dataansvarlige. Forudsætningen for dette og opdelingen af forpligtelser vil blive undersøgt yderligere senere.

3.1.3 ”Formål og hjælpemidler”

Som tidligere gennemgået, er et af behandlingsprincipperne at oplysninger skal indsamles til udtrykkeligt angivne og legitime formål og de må ikke viderebehandles på en måde, der er uforenelig med disse formål, jf. Forordningen, art. 5, litra b. Det er derfor vigtigt, at der træffes et formål med behandlingen. Dette formål skal træffes af den dataansvarlige og modsat, vil den der beslutter formålet være dataansvarlig. Det er i ordlyden forudsat at både formål og hjælpemidler skal bestemmes af den dataansvarlige og en databehandler vil derfor ikke kunne beslutte en af disse. Databeskyttelsesrådet har dog udtalt at det kan være nødvendigt for databehandleren at træffe nogle beslutninger i forhold til behandlingen. Vejledningen beskriver grænsen til disse beslutninger og opdeler det i to kategorier, hvor ”væsentlige hjælpemidler” vil tale for at man er dataansvarlig, hvorimod ”ikkevæsentlige hjælpemidler” kan foretages af en databehandler. Det er den

[26] IBID
[27] IBID
[28] (EDPB, Retningslinjer 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse), s. 14

dataansvarlige der bestemmer formålene og hjælpemidlerne til behandlingen. Nogle af de praktiske aspekter af gennemførelsen ("ikkevæsentlige hjælpemidler") kan dog overlades til databehandleren.[29] Vejledningen beskriver nogle af de konkrete elementer, der skal lægges vægt på i vurderingen og denne anvendes i denne forbindelse som fortolkningsbidrag. Efterfølgende vil en række afgørelser blive undersøgt, for at fastslå hvordan formål og hjælpemidler behandles i praksis.

Vejledningen siger at følgende elementer vil vedrøre væsentlige hjælpemidler:

- Typen af personoplysninger, der behandles
- Varigheden af behandlingen
- Kategorierne af modtagere
- Hvilke personers oplysninger behandles

I relation til dette, nævnes at de vigtigste hjælpemidler vil være tæt forbundet med spørgsmålet om, hvorvidt behandlingen er lovlig, nødvendig og forholdsmæssig – altså behandlingsprincipperne.

De ikke-væsentlige hjælpemidler kan blandt andet være valg af bestemt type udstyr eller software – altså hjælpemidler, som ikke direkte er relevant for behandlingen, eller som relaterer sig til virksomhedens interne sikkerhed. Ved en snæver og klar instruks, hvor det kun er software som virksomheden selv bestemmer, vil der således ikke være tvivl om, at kun den person som har afgivet instruks, er dataansvarlig. I disse situationer hvor der modtages en instruks og den anden person behandler data for den dataansvarlige, vil denne person være databehandler og denne databehandlerkonstruktion kræver en databehandleraftale, hvori disse formål og hjælpemidler fastsættes af den dataansvarlige – dette afholder ikke databehandleren fra at formulere disse hjælpemidler, da det i praksis kan være mest nærliggende at det er denne part der formulerer dem, men det kræver dog en klar og præcis formulering som aktivt accepteres af den dataansvarlige. Dette følger af art. 5, stk. 2 og art. 24. Det direkte krav om en databehandleraftale følger af Forordningens art. 28, stk. 3.

3.2 Relevante afgørelser

Følgende kapitel vil analysere en række afgørelser, for at undersøge hvordan bestemmelserne skal forstås i praksis. Disse afgørelser er fra før Forordningen, men som tidligere nævnt, er der ikke tilsigtet en ændring i retspraksis med springet fra direktivet til Forordningen. Disse afgørelser er

[29] (EDPB, Retningslinjer 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse), s. 3

derfor stadig relevante og vil blive analyseret for at forstå den nuværende retstilstand. Alle relevante betragtninger vil blive inddraget, både i forhold til at vurdere hvorvidt man er dataansvarlig, men også de betragtninger der vedrører de begreber, der tidligere er gennemgået.

Wirtschaftsakademie

Sag C-210/16 indgivet af Bundesverwaltungsgericht (som er forbundstomstolen i forvaltningsretlige sager i Tyskland) omhandler Wirtschaftsakademie som udbyder uddannelse via en fanside på Facebook. Denne afgørelse omhandler fælles dataansvar. Det var ubestridt at Facebook naturligvis var dataansvarlig, da de behandlede personoplysninger, indsamlet igennem cookies. Et af spørgsmålene var i stedet, hvorvidt akademiet var fælles dataansvarlig i behandlingen af de besøgendes personoplysninger. Et af spørgsmålene var i denne forbindelse, hvorvidt en administrator af en Facebook-side, er med til at afgøre formål og hjælpemidler til den behandling af personoplysninger som foretages på brugerne af denne fanside. Behandlingen foretages igennem de cookies som en bruger af mediet accepterer ved oprettelsen af en bruger. I dag ville disse cookies skulle accepteres direkte ved besøg af hjemmesiden og ikke blot ved oprettelsen af brugeren. Disse cookies har til formål at lagre oplysninger om internetbrowsere og derved hjælpe med markedsføring for Facebook samt give administratoren mulighed for at få kendskab til de brugere, der besøger dennes fanside, med henblik på at kunne tilbyde dem mere relevant indhold og udvikle funktioner, som de kunne være mere interesserede i, jf. præmis 34.

Disse cookies lagres af Facebook hver gang en bruger besøger Facebook-tjenester, tjenester der leveres af andre Facebook-virksomheder og tjenester, der leveres af andre virksomheder, der bruger Facebook-tjenesterne, jf. præmis 33. Domstolen slår fast, at den omstændighed, at man blot benytter et socialt netværk som Facebook, ikke gør en til fælles dataansvarlig for netværkets behandling af personoplysninger, men at en administrator af en Facebook-side er med til at give muligheden for at placere cookies ved besøg af dennes side, jf. præmis 35. Selv uden en Facebook-profil, giver sideadministratoren Facebook mulighed for at placere cookies på brugerens computer, når denne besøger fansiden og denne situation synes at gøre administratorens behandling endnu vigtigere, jf. præmis 41. Derudover kan administratoren definere kriterierne som statistikkerne skal udarbejdes på grundlag af og angive kategorierne af personer, som der skal indsamles personoplysninger om, jf. præmis 36. Selvom disse personoplysninger er anonymiseret og Wirtschaftsakademie derfor ikke har adgang til disse, fastslår domstolen alligevel at Wirtschaftsakademie er med til at bestemme over formål og hjælpemidler for selve indsamlingen. Det er Wirtschaftsakademie der selv har oprettet

fansiden og dermed er med til at bestemme hjælpemidler og det er desuden også dem, der anvender disse personoplysninger til eksempelvis *"at foretage salgsfremstød eller arrangere begivenheder eller mere generelt bedre at målrette sit informationsudbud"*, jf. præmis 37. På baggrund af dette, fastslår domstolen at Wirtschaftsakademie er fælles dataansvarlig, men at dette ikke nødvendigvis medfører en lige fordeling af ansvaret. Ansvarsfordelingen skal vurderes ud fra de konkrete omstændigheder, jf. præmis 43. Det vil eksempelvis være mest nærliggende for Facebook at bære ansvaret om at sikre at opbevaringen af disse personoplysninger følger principperne i Forordningen, da Wirtschaftsakademie ikke selv har adgang til personoplysningerne.

Fashion-ID

Sag C-40/17 omhandler virksomheden Fashion ID GmbH, som sælger tøj online. På deres hjemmeside har de valgt at integrere en "synes godt om"-knap, som er linket til Facebook. Integrationen af denne knap, medfører at der indsamles personoplysninger fra alle besøgende på webstedet af Facebook. Indsamlingen finder sted selvom brugeren ikke interagere med knappen og selvom brugeren i øvrigt ikke er medlem af Facebook. Her udtalte domstolen, at Fashion ID *"Ved at integrere et sådant socialt modul på sit websted har Fashion ID desuden på afgørende vis indflydelse på indsamlingen",* jf. præmis 78. De lægger dertil til grund, at indsamlingen ikke ville have fundet sted, uden Fashion ID's integration af synes-godt-om-knappen. Ved selv at integrere eller være afgørende for at indsamlingen finder sted, vil man derfor have opfyldt kravet om at afgøre hjælpemidler. Fashion ID's formål med behandlingen var at behandle personoplysningerne til at optimere markedsføringen og gøre dem mere synlige på Facebook, på baggrund af dette blev det vurderet at Fashion ID var med til at bestemme formål og derfor var fælles dataansvarlig.

Det fremgår af præmis 74 at: *"Derimod og med forbehold for et eventuelt erstatningsansvar i henhold til national ret i denne henseende kan denne fysiske eller juridiske person ikke anses for at være den registeransvarlige som omhandlet i nævnte bestemmelse, for operationer, der indtræder før eller efter rækken af behandlinger, og vedrørende hvilke den pågældende hverken fastlægger formål eller hjælpemidler"*.

Fashion ID var udelukkende dataansvarlig for den behandling der blev foretaget i forbindelse med indsamling og videretransmission af personoplysningerne til Facebook. Derudover var det Fashion ID, og ikke Facebook, der skulle sørge for at der var samtykke til indsamlingen, jf. præmis 102. Dette er en betragtning der giver god mening i praksis, da det netop er Fashion ID der indsamler og

videregiver oplysningerne. Dette samtykke skal foreligge før indsamlingen finder sted og gælder kun på den del af behandlingen, som Fashion ID har afgjort formålet med.

3.3 Fælles dataansvar

Dette kapitel vil undersøge, hvornår der er tale om et fælles dataansvar. Det er relevant at undersøge dette, da et fælles dataansvar medfører forskellige forpligtelser for dem der indgår i dataansvaret. Disse forpligtelser vil også blive undersøgt i nærværende kapitel.

Det fælles dataansvar forudsætter at to dataansvarlige, i fællesskab, beslutter formål og hjælpemidlerne. Dette kan enten gøres igennem en fælles beslutning, eller det kan være et resultat af flere dataansvarliges konvergerende beslutninger om formål og væsentligste hjælpemidler.[30] Den konvergerende beslutning er en følge af EU-Domstolens retspraksis. Vurderingen af, hvorvidt der er tale om en konvergerende beslutning, foretages med hensyn til om behandlingen ville være umulig uden begge parters deltagelse i formål og hjælpemidler ved at hver parts behandling er uadskillelig, dvs. uløseligt forbundet.[31] Som tidligere nævnt, forudsætter det fælles dataansvar ikke at begge parter har adgang til personoplysningerne, jf. Wirtschaftsakademie, præmis 38.

EU-domstolen understregede i Jehovas Vidner-sagen at det ikke var nødvendigt for trossamfundet at udgive skriftlige retningslinjer eller anvisninger i forhold til behandlingen, men at det var tilstrækkeligt at trossamfundet koordinerede medlemmernes aktiviteter.

EU-domstolen fastslog også i Fashion ID-sagen at to dataansvarlige kun vil anses for fælles dataansvarlige for den behandling, hvor de sammen beslutter formål og hjælpemidler og at alt behandling der går forud eller følger dette, ikke vil involvere begge som dataansvarlige, jf. Fashion ID-sagen, præmis 74.

Når begge dataansvarlige forfølger et fælles formål, eller formål der er tæt forbundne, vil kravet om formål være opfyldt i forhold til om der er fælles dataansvar eller ej, som analyseret i Fashion ID afgørelsen, hvor det ikke var det samme formål Facebook og Fashion ID havde med indsamlingen, men hvor formålene var komplementære og gensidige.

[30] (EDPB, Retningslinjer 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse), s. 21
[31] IBID

Afgrænsningen af, hvorvidt der er tale om fælles dataansvar eller selvstændige dataansvarlige afspejles i to eksempler fra EDPB's vejledning om dataansvarlige. Det drejer sig om følgende eksempler:

Intet fælles dataansvar:

"Et rejsebureau sender sine kunders personlige oplysninger til flyselskabet og en række hoteller med henblik på at reservere en rejsepakke. Flyselskabet og hotellet bekræfter, at de ønskede sæder og værelser er ledige. Rejsebureauet udsteder rejsedokumenter og -kuponer til sine kunder. Hver af aktørerne behandler oplysningerne til at udføre deres egne aktiviteter og med deres egne hjælpemidler. I dette tilfælde er rejsebureauet, flyselskabet og hotellet tre forskellige dataansvarlige, der behandler oplysningerne til deres egne og separate formål, og der er intet fælles dataansvar."[32]

Fælles dataansvar

"Rejsebureauet, hotelkæden og flyselskabet beslutter derefter i fællesskab at deltage i oprettelsen af en internetbaseret fælles platform med det fælles formål at tilbyde pakkerejser. De er enige om de vigtigste hjælpemidler, der skal anvendes, f.eks. hvilke oplysninger der skal lagres, hvordan reservationerne vil blive fordelt og bekræftet, og hvem der kan få adgang til de lagrede oplysninger. Desuden beslutter de at dele deres kunders oplysninger med henblik på at gennemføre fælles markedsføringsaktiviteter. I dette tilfælde afgør rejsebureauet, flyselskabet og hotelkæden i fællesskab, hvorfor og hvordan personoplysninger om deres respektive kunder behandles, og vil derfor være fælles dataansvarlige med hensyn til behandlingen af den fælles internetbaserede reservationsplatform og de fælles markedsføringsaktiviteter. Men hver af dem ville stadig have enekontrol med hensyn til andre behandlingsaktiviteter uden for den internetbaserede fælles platform."[33]

Der vil i næste kapitel undersøges flere eksempler fra vejledningen, for generelt at fastslå hvornår man er selvstændigt dataansvarlig, fælles dataansvarlig og hvornår man slet ikke er dataansvarlig.

[32] (EDPB, Retningslinjer 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse), s. 23
[33] (EDPB, Retningslinjer 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse), s. 24

3.4 Datatilsynets vejledning

Det er vigtigt at identificere hvorvidt man er dataansvarlig eller databehandler, for at afgøre hvilke forpligtelser man er underlagt i forhold til databeskyttelsesforordningen. I en simpel databehandlerkonstruktion skal der udarbejdes en databehandleraftale, jf. Artikel 28, stk. 3, men der skal til gengæld ikke findes et selvstændigt hjemmelsgrundlag for overladelsen, da databehandleren behandler oplysningerne på vegne af den dataansvarlige. Hvis der derimod sker en overladelse af personoplysninger, kræver dette altså, at den anden dataansvarlige som overlades disse oplysninger skal kunne redegøre for sit eget behandlingsgrundlag.[34] Uanset om der er tale om en konstruktion med to fælles dataansvarlige efter artikel 26, eller om der er tale om den førnævnte overladelse af personoplysninger imellem to selvstændige, men samarbejdende dataansvarlige, eller om der er tale om overladelse fra en dataansvarlig til en databehandler, så er det afgørende at der er klarhed og åbenhed omkring ansvarsfordelingen for de registrerede, jf. Forordningens betragtning 79.[35]

Den simple databehandlerkonstruktion vil bestå af en dataansvarlig, som indsamler oplysninger og herefter skal have dem behandlet, f.eks. i en IT-løsning af databehandleren. Det vil her være den dataansvarlige som instruerer databehandleren i, hvordan disse oplysninger skal behandles og derved også den dataansvarlige som bestemmer formålet med behandlingen af disse, eksempelvis til personaleregister.

Definitionen indebærer at der kan være mere end én dataansvarlig i en behandling. Der er derfor ikke tale om en simpel udvælgelse af, hvem der bestemmer formål og instruks i størst omfang, men blot hvem der selvstændigt bestemmer formål og instruks. I enhver databehandlingssituation kan der derfor være både én, to og flere dataansvarlige, som hver især bestemmer formål og instruks for netop deres behandling og deraf også flere forskellige behandlinger. Datatilsynet har fremlagt en række eksempler på forskellige databehandlerkonstruktioner i deres vejledning om GDPR. Disse vil blive præsenteret her, for at give et kort indblik i de forskellige konstruktioner.

Dette første eksempel involverer et fitnesscenter A og en IT-virksomhed B. A ønsker en løsning til opbevaring af medlemmernes personoplysninger og i aftalen imellem dem, har A bestemt formål og instruks, som består i at B udelukkende skal opbevare disse oplysninger og altså ikke må bruge dem i videre omfang end det formål der er fastsat af A. Det er altså på A's præmisser at behandlingen

[34] (Lotterup & Nielsen, 2020), s. 273
[35] (Lotterup & Nielsen, 2020), s. 274

foregår og virksomhed B behandler ikke disse oplysninger yderligere. Dette er et klassisk eksempel på en simpel databehandlerkonstruktion.[36]

Datatilsynet har desuden et andet eksempel, hvor der ikke er tale om en klassisk databehandlerkonstruktion, men i stedet om to selvstændige dataansvarlige. Dette er vedrørende en revisor som skal udarbejde en selvangivelse for en mekaniker. Instruksen fra mekanikeren er blot, at selvangivelsen skal udarbejdes og derudover ikke yderligere instruks omkring behandlingen. Her fastslår datatilsynet at begge subjekter er selvstændigt dataansvarlige, også selvom mekanikeren reelt har givet instruks om, at behandlingen vedrører udarbejdelse af selvangivelsen. Datatilsynet lægger til grund at *"hvad revisoren skal gøre er bredt og generelt formuleret"* og at begge parter derfor er selvstændig dataansvarlige.[37] Det kræver altså en forholdsvis præcis formuleret instruks for at der er tale om en databehandlerkonstruktion. Hvis samme eksempel havde indeholdt en databehandleraftale med præcise formuleringer om, hvordan revisoren skulle behandle personoplysningerne, kunne der være tale om en databehandlerkonstruktion. Til dette eksempel lægges der dog yderligere vægt på, at det specifikt ved revisorer, er tvivlsomt hvorvidt de overhovedet kan efterleve en detaljeret instruks om udarbejdelsen af selvangivelsen, da revisorerne er underlagt professionelle forpligtelser.

I Datatilsynet og Justitsministeriets vejledning lægges der vægt på om en given ydelse – helt eller delvist - består i behandling af personoplysninger efter instruks. I dette tilfælde vil der sandsynligvis foreligge en databehandlerkonstruktion. Yderligere lægges der vægt på i vurderingen, hvem der træffer afgørelse om formål og hjælpemidler, som også er en central vurdering i ordlyden af artikel 4, nr. 7 samt de tidligere undersøgte afgørelser. Det kan være utvivlsomt hvem der træffer afgørelse omkring formål og hjælpemidler, eksempelvis kan dette være specifikt formuleret i en instruks i en databehandleraftale. Datatilsynet og Justitsministeriet fremlægger dog mulighed for at databehandler til dels kan bestemme over dele af behandlingen, eksempelvis tekniske og organisatoriske hjælpemidler, hvor det kan være mest nærliggende at databehandleren bestemmer disse. Der står følgende i vejledningen *"Det afgørende, for om der foreligger en instruks, og dermed en databehandlerkonstruktion, er, om en behandling af personoplysninger foretages af en anden part, mens du som dataansvarlig fortsat bestemmer over formålet og over de væsentligste behandlingsskridt, herunder indsamling, sletning, videregivelse og brug af eventuelle underdatabehandlere."* Dette indskrænker dermed det umiddelbare krav for, hvornår man er

[36] (Datatilsynet), s. 10
[37] (Datatilsynet), s. 10

dataansvarlig og det er derfor muligt at bestemme, i et mindre omfang, over selve behandlingen og stadig ikke ifalde rollen og de dertilhørende forpligtelser som dataansvarlig.

4. Køber og producent som dataansvarlig

Det er blevet fastslået hvornår der er tale om et fælles dataansvar og med udgangspunkt i dette, er det relevant at kigge på nogle af de grænsetilfælde der er i forhold til at placere dataansvaret. I denne forbindelse vil dataforholdet, der er imellem en privat køber og en producent blive undersøgt. Producenten er som udgangspunkt ikke dataansvarlig, når denne fratræder sit produkt. Der opstår dog en problemstilling, når producenten fortsat er med til at bestemme over formål og hjælpemidler, eksempelvis ved løbende at kunne opdatere produktet eller afholde køberen fra at kunne vælge, hvordan personoplysningerne behandles. Det fremgår af præambelbetragtning 78 at:

"Når producenter af produkter, tjenester og applikationer udvikler, designer, udvælger og bruger applikationer, tjenester og produkter, der er baseret på behandling af personoplysninger eller behandler personoplysninger, for at udføre deres opgaver, bør de tilskyndes til at tage højde for retten til databeskyttelse i forbindelse med udvikling og design af sådanne produkter, tjenester og applikationer og til under behørig hensyntagen til det aktuelle tekniske niveau at sørge for, at de dataansvarlige og databehandlerne er i stand til at opfylde deres databeskyttelsesforpligtelser. Der bør også tages hensyn til principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i forbindelse med offentlige udbud."

Spørgsmålet er, hvorvidt producenten dermed er forpligtet til at efterleve Forordningens regler eller blot er tilskyndet, som formuleret i præambelbetragtningen. Det må i denne forbindelse udledes, at så længe producenten ikke er omfattet af Forordningens anvendelsesområde, vil denne ikke skulle efterleve kravene, men bliver blot tilskyndet til dette – hvilket ikke har nogen praktisk betydning. Dette synspunkt synes dog at blive udfordret af moderne produkter, hvor producentens rolle efter salgstidspunktet stiger i forhold til tidligere. Smartphones er efterhånden ikke nye længere, og er i lang tid blevet opdateret efter produktet egentlig har forladt producenten. Ved disse opdateringer og den generelle indgriben fra producenten, har dette medført et dataansvar, fordi producenten netop stadig behandler oplysninger med egne formål og hjælpemidler. Dertil kan der være situationer, hvor producenten og køberen er fælles dataansvarlige, dette forudsætter at de begge er medbestemmende til den samme behandling. Samme problematik vokser indenfor bilbranchen, hvor flere og flere

moderne biler begynder at ligne smartphones i deres anvendelse. Især elbiler som Tesla opdateres præcis som en telefon og nogle af funktionerne i bilen har aktivt behandlet og videregivet oplysningerne til Tesla, uden at brugeren har haft mulighed for at vælge dette fra eller til.

Tidligere har brugen af telefoner, biler og andre apparater betydet en lokal behandling af ens personoplysninger. F.eks. har alle telefonens data tidligere, udelukkende ligget lokalt på telefonen og bilens kørerutiner m.m. har ligeså været lagret lokalt i bilens systemer. Producenten har altså ikke haft adgang til disse oplysninger, men personoplysningerne i de selvsamme eksempler bliver nu opbevaret i en "cloud-løsning" som producenten tilbyder. Denne cloud-løsning er egentlig en separat ydelse, som ikke direkte vedrører den behandling som foretages af bilen. Eksempel på personoplysninger, som stadig behandles lokalt, er fingeraftryk. Disse ligger gemt lokalt på telefonen og behandles derfor ikke af producenten. Uagtet om køberen, som privat person, falder indenfor databeskyttelsesforordningen, er producenten sandsynligvis stadig, efter præambelbetragtning 18, indenfor forordningens anvendelsesområde. Det er formuleret således:

"Denne forordning gælder dog for dataansvarlige eller databehandlere, som tilvejebringer midlerne til behandling af personoplysninger til sådanne personlige eller familiemæssige aktiviteter."

Formuleringen er bred og synes at indfange alle apparater, som kan behandle data, leveret af producenten. Omfanget af betragtningens anvendelsesområde er dog uklar. EDPB har udgivet en vejledning om tilsluttede biler, hvori de henviser til denne præambelbetragtning. Heri fastslår de, at tilsluttede biler altså er indenfor betragtningens anvendelsesområde og at producenten derfor skal efterleve kravene om privacy-by-default og privacy-by-design, når de udvikler løsningerne til bilen, såfremt de er dataansvarlige eller databehandler. Som en anbefaling i forhold til principperne om privacy-by-default og privacy-by-design, anbefales det desuden at producenten indfører en sikker, lokal "in-car" platform, som er adskilt fra clouden og derved ikke er afhængig af cloud-løsningen – og at producenten i øvrigt indfører lokal databehandling i det omfang, det er muligt.[38]

Det er altså ikke blevet fastslået, hvorvidt lokal behandling af en lokal person, som ellers falder rimelig tydeligt udenfor forordningens anvendelsesområde, medfører et ansvar for producenten.

[38] (EDPB, Retningslinjer 1/2020 om behandling af personoplysninger i forbindelse med opkoblede køretøjer og mobilitetsrelaterede anvendelser), s. 19

I tilfælde af, at producenten er den eneste dataansvarlige, vil køberen være en typisk registrerede, som defineret i Forordningen. Det medfører at producenten ifalder alle de forpligtelser, som en almindelig dataansvarlig har og at køberen derudover også vil have de rettigheder, som tidligere fastslået. Såfremt den registreredes behandling falder udenfor forordningens anvendelsesområde, vil den registrerede fortsat forbeholde sig de rettigheder, som forordningen medfører, og kan derfor gøre indsigelse mod producenten på baggrund af disse rettigheder, såfremt producenten er dataansvarlig.

Det bliver noget sværere at fastslå konsekvenserne af producenten som databehandler. For hvis producenten er databehandler, må den dataansvarlige modsat være den dataansvarlige, og i stedet for at kunne gøre indsigelse på baggrund af de registreredes rettigheder, vil rettighederne, eller "magten" i stedet ligge i at bestemme formål og hjælpemidler. Det næste afsnit vil undersøge denne problemstilling og mulige konsekvenser heraf.

Hvis producenten er databehandler, besværliggør dette pludselig køberens rettigheder. Den registreredes rettigheder kan kun udøves overfor den dataansvarlige, og databehandlerens forpligtelser ligger, i denne forbindelse, blot i at bistå den dataansvarlige i opfyldelsen af eventuelle udøvede rettigheder. Derudover er forpligtelserne om privacy-by-design og privacy-by-default kun gældende for dataansvarlige, jf. artikel 25. Dette er ellers en forpligtelse, som er helt central for en producent ved udviklingen af produktet eller løsningen.

4.1 Robotstøvsugere

Det er blevet fastslået hvornår der er tale om et fælles dataansvar. Det vil nu blive undersøgt, i hvilke tilfælde en privat køber og en producent kan være dataansvarlige – og hvorvidt disse vil være fælles dataansvarlige.

I denne forbindelse vil en række scenarier blive undersøgt, for at vurdere hvornår henholdsvis en køber og en producent vil være dataansvarlige. Der vil tages udgangspunkt i et reelt produkt som anvender kameraer, men der vil også opstilles en række fiktive scenarier, baseret på dette produkt. Disse scenarier gør sig sandsynligvis gældende på allerede eksisterende produkter. Formålet er at undersøge, i hvilke tilfælde køberen og producenten vil være dataansvarlige. Der tages udgangspunkt i en moderne robotstøvsuger med produktnavnet "Dreame D10s Pro" af mærket Dreametech. Denne robotstøvsuger anvender laser til dens navigation, men er samtidig udstyret med kameraer, hvis formål er at overvåge hjemmet og dens funktioner indeholder blandt andet muligheden for at optage et klip af realtidsovervågningen eller bede støvsugeren om at køre hen til en person i hjemmet.

Forskellige fiktive scenarier, som kan være relevante i forhold til andre robotstøvsugere, vil blive diskuteret, herunder:

- Formålet med kameraet: overvågning eller navigation?
- Placering af robotstøvsugeren: i hjemmet eller på offentligt område?
- Opbevaring af oplysningerne: Lokalt eller på cloud?

Ud fra ovenstående scenarier, vil det i de konkrete scenarier, blive vurderet om Forordningen finder anvendelse, hvem der er dataansvarlig for behandlingen af personoplysninger, hvorvidt principperne for lovlig behandling af personoplysninger er overholdt samt delingen af de lagrede personoplysninger.

Strukturen for undersøgelsen vil være opdelt efter ovenstående vurderinger og scenarierne vil blive inddraget for hver vurdering, når disse er relevante. Til slut vil det blive vurderet hvilket scenarie, der er det mest relevante i forhold til Forordningen og dette scenarie vil undersøges yderligere.

4.1.1 Forordningens anvendelsesområde

Som tidligere defineret er anvendelsesområdet bredt og det er blevet konkluderet at optagelser eller billeder af identificerbare personer er indeholdt i definitionen af personoplysninger. (Se afsnit 1.1.2) Da det underliggende software i robotstøvsugeren er edb, er der også tale om automatisk behandling (Afsnit 1.2.3). Optagelserne fra robotstøvsugeren vil derfor falde ind under Forordningens anvendelsesområde, såfremt der er tale om oplysninger om en identificerbar (eller identificeret) person. Det er ikke blot personer, som kan optræde på videooptagelserne der vil være henregnet som personoplysninger, men også andre oplysninger, herunder nummerplader som er fastslået til at være en personoplysning.[39] Robotstøvsugeren vil i nogen tilfælde, måske slet ikke behandle oplysninger. Dette ville navnligt ske, hvis der ikke var kamera installeret eller kameravinklen peger nedad, som derved gør det umuligt at opfange personoplysninger. Dette ville dog være en konkret vurdering og undviger ikke nødvendigvis Forordningens anvendelsesområde, da tatoveringer, indgraverede smykker m.m. sandsynligvis vil gå ind under definitionen af personoplysninger ved at være en ”identifikator”. Behandlingen af personoplysninger i forbindelse med lagring i cloud-løsning vil utvivlsomt også være omfattet. Der vil senere blive skelnet imellem hvorvidt oplysninger opbevares. Heraf også om de opbevares lokalt eller i en cloud-løsning. Vedrørende anvendelsesområdet er det dog ikke relevant, da behandling ikke forudsætter at oplysningerne lagres. Dette nævnes i ”Retningslinjer 3/2019 om brug af videoudstyr til behandling af personoplysninger” hvortil det også

[39] Retningslinjer 3/2019 om brug af videoudstyr til behandling af personoplysninger

nævnes at realtidsovervågning kan være mere indgribende end lagring, der slettes efter en bestemt periode, da realtidsovervågningen kan iagttages af en person, hvorimod optagelsen ville kunne lagres med henblik på, kun at gennemgå optagelserne ved særlige omstændigheder, såsom hærværk. Dette vil diskuteres yderligere.

Dreamebot D10s giver mulighed for realtidsovervågning, men lagrer ikke optagelserne. Det er dog muligt, med appens funktioner, at optage videoer igennem realtidsovervågningen.

Angående spørgsmålet om det territorielle anvendelsesområde, afhænger dette af de tidligere nævnte kriterier fra kapitel 1.3. Kriterierne vil kort blive gennemgået med udgangspunkt i Dreamebot D10s.

Dreametech der producerer støvsugeren er oprindeligt en asiatisk virksomhed, som sælger til forhandlere i hele Europa. I Danmark er forhandlerne Power og Elgiganten. Vurderingen er derfor ikke helt den samme, som blev fastlagt i det tidligere kapitel 1.3. Dreametech har selv en hjemmeside på dansk med dertilhørende support af deres produkter, som er tilkoblet et dansk nummer. I den forbindelse må det anslås, at Dreametech er etableret i Danmark og derudover også i resten af Europa, da de har hjemmesider og support på tysk, fransk, norsk, svensk, spansk m.m. Dreametech er derfor omfattet af det territorielle anvendelsesområde gældende deres produkt og dens behandling, jf. Forordningens art. 3, stk. 1. Såfremt produkterne produceres i Kina, vil behandlingen stadig være omfattet af det territorielle anvendelsesområde.

Hvis Dreametech anvendte en cloud-løsning til deres robotstøvsuger ville denne anses som en service der udbydes til registrerede i Unionen ud fra samme overvejelser og selvom støvsugeren er produceret udenfor EU, vil producenten stadig være omfattet af det territorielle anvendelsesområde, jf. Forordningens art. 3, stk. 2.

Kapitel 4.1.2 Privatreglen

Privatreglen, som er den tidligere gennemgået undtagelse af Forordningens anvendelsesområde, er relevant i forhold til at vurdere, hvorvidt den private køber er dataansvarlig. Med dens krav om ”*fysiske personer”* vil den ikke være relevant i forhold til producenten som dataansvarlig og ej heller for køberen, hvis dette er en virksomhed. I afsnit 1.2 blev det fastlagt at videoovervågning, der dækker et offentligt område – også selvom dette kun er delvist, ikke er dækket af bestemmelsens krav om at behandlingen foretages i *”personlig eller familiemæssig”* sammenhæng. I tilfælde af, at robotstøvsugeren blot anvendes i hjemmet, vil køberens behandling være undtaget, jf. privatreglen.

Dette vil dog ikke undtage producentens forpligtelser, hvis denne er dataansvarlig. Det er dog relevant at diskutere hvor grænsen går, i forhold til at filme offentligt. Det klare scenarie er robotstøvsugeren der kun filmer inde i huset og derved ikke filmer på offentligt område eller robotstøvsugeren, der tages med ud på en gåtur og derfor uden tvivl filmer på offentligt område, men mere tvivlsomt bliver det, hvis eksempelvis en robotstøvsuger kører rundt i en privat kælder, hvor vinduernes placering og robottens kameravinkel medfører at robotstøvsugeren filmer ud på offentligt område. I praksis ville dette dog sandsynligvis ikke medføre behandling af identificerbar eller identificerede personer, da kamerakvaliteten næppe ville være god nok, til at kunne genkende en person på afstand – og igennem et vindue. Her vil den konkrete situation skulle vurderes ud fra, hvorvidt der behandles personoplysninger ude på det offentlige område, hvis ikke dette er tilfældet, er privatreglen ikke relevant, da der slet ikke er tale om personoplysninger og man derfor ikke er indenfor Forordningens anvendelsesområde i første omgang. Ansigter eller nummerplader, der er tydelige nok til at kunne identificeres er indenfor anvendelsesområdet og kan ikke undtages af privatreglen, da behandling på offentligt område ikke falder ind under undtagelsen. Det er tidligere blevet fastlagt, at det ikke er et krav at kameraet er placeret på offentligt område, men derimod tilstrækkeligt, at det blot filmer ud på offentligt område, jf. František Ryneš-sagen. Privatreglen vil sandsynligvis ikke undtage behandlingen fra Forordningens anvendelsesområde og køberen vil derfor være dataansvarlig for behandlingen.

Privatreglen vil altså kunne undtage fysiske personer fra forordningens anvendelsesområde, såfremt der IKKE filmes på offentligt område og den dataansvarlige vil ikke falde ind under Forordningens anvendelsesområde, hvis der ikke behandles personoplysninger på dette offentlige område (eksempelvis pga. afstanden og/eller kvalitet af optagelsen). Alle de andre scenarier vil være omfattet af Forordningens anvendelsesområde og det vil derfor også antages i de efterfølgende scenarier, at støvsugeren ikke anvendes i et hjem, hvor der ikke er risiko for at filme ud på offentligt område. Det mest nærliggende vil derfor være, at der i scenarierne antages at kameraet er anvendt på et offentligt område.

Med udgangspunkt i de tidligere kapitler omkring, hvornår man er dataansvarlig, vil følgende kapitel gennemgå de forskellige scenarier og fastslå, hvornår køberen og producenten hver især er dataansvarlige, ud fra de tidligere undersøgelser.

Som tidligere fastslået, skal der i vurderingen om man er dataansvarlig, kigges på om man er med til at bestemme hvorfor (formål) og hvordan (hjælpemidler) behandlingen skal foregå.

I det nævnte eksempel har kameraet ikke et formål der er knyttet til selve støvsugningen, men fungerer i stedet funktionelt som et (støvsugende) sikkerhedskamera og det vil derfor i det konkrete scenarie, blive behandlet som et sikkerhedskamera. Andre robotstøvsugere bruger dog kameraet som navigation og dette scenarie vil også blive behandlet.

I dette fiktive scenarie, antager vi at kameraets primære formål ikke er at behandle personoplysninger, men at dette sker indirekte ved at optimere støvsugerens navigation og at de indsamlede personoplysninger i øvrigt behandles af producenten, til at forbedre navigationen.

Problemstillingen her, er at det er producenten der bestemmer over denne funktion og medmindre kameraet understøttes af en anden form for navigationssystem, kan dette næppe slås fra af køberen. Her vil producenten bestemme over formålet, hvorimod køberen vil være den der styrer støvsugeren og derfor står for selve behandlingen af personoplysningerne. Problemstillingen er derfor om de vil være fælles dataansvarlige, selvstændige dataansvarlige eller om en af parterne alene vil være dataansvarlig.

Som tidligere fastslået, er det muligt at have flere dataansvarlige for samme behandling, hvis disse i fællesskab bestemmer formål og hjælpemidler. De tidligere fastsatte hjælpemidler vil derfor blive gennemgået.

- Typen af personoplysninger, der behandles
- Varigheden af behandlingen
- Kategorierne af modtagere
- Hvilke personers oplysninger behandles

Producenten bestemmer hvilke typer af personoplysninger der behandles ved at installere kameraerne. Dette vil være kameraoptagelserne. Producenten bestemmer desuden hvem der har adgang til disse, når de selv anvender disse oplysninger til at forbedre deres navigation. Det er også producenten, der har valgt placeringen og anvendelsen af kameraet og bestemt formålet med kameraet (bedre navigation). Varigheden af behandlingen vælges dog af køberen, da det er denne der vælger, hvornår robotstøvsugeren skal køre og til dels også typen af personoplysninger, da det er denne der vælger hvor robotstøvsugeren skal køre.

I det nuværende scenarie bestemmer de ikke i fællesskab både formål og hjælpemidler, men køberen bestemmer hjælpemidler og producenten bestemmer formålet. Denne konvergerende beslutning er, som tidligere fastlagt, tilstrækkelig til at fastslå et fælles dataansvar. Kravet om at behandlingen ikke

ville være mulig uden begge parters deltagelse i formål og hjælpemidler og derved er uløselig forbundet er tydelig i scenariet, hvor producenten har udstyret støvsugeren med et kamera og den er designet således at den automatisk behandler personoplysninger. Med henblik på Fashion-ID dommen, blev der lagt vægt på at Fashion-ID selv havde installeret deres synes godt om-knap i vurderingen om, hvorvidt de var med til at bestemme formål. Det kan derfor have betydning, hvorvidt køberen selv kan slå funktionen til eller fra, eksempelvis i det scenarie, hvor kameranavigationen er understøttet af en anden form for navigation, der ikke behandler personoplysninger. Her vil køberen være med til at bestemme en del af formålet. Det er desuden værd at nævne igen, at manglende adgang til personoplysningerne ikke fratager en fra dataansvaret og producenten behøver derfor ikke have adgang til disse oplysninger. Det er i denne sammenhæng derfor ikke relevant, om cloud-løsningen anvendes eller om der er tale om lokal-behandling (eksempelvis et memory-kort i støvsugeren). Producenten vil dog næppe opnå en gensidig fordel ved denne behandling og da køberen selv bestemmer, hvorvidt funktionen er slået fra eller til, vil denne sandsynligvis være selvstændig dataansvarlig. Problemstillingen kan sammenlignes med køb af et GoPro-kamera, eller et dash-kamera til en bil. Her vil producenten have udviklet produktet, og dermed være medbestemmende i formålet, men vil sandsynligvis ikke bestemme over hjælpemidlerne, da det udelukkende er køberen der vælger at tænde eller slukke det og derudover selv bestemmer hvor kameraet skal optage.

I det udvalgte produkt lagres optagelserne ikke. Det er i stedet realtidsovervågning og på producentens hjemmeside står der følgende:

"Med videofjernovervågning kan du holde øje med din bolig, dine kæledyr og børn, hvorend du er henne. Se it hjem med robottens blik for at få et helt nyt perspektiv, eller se om noget er faldet under dine møbler med blot et par tryk på din telefon."

Det fungerer igennem en app, hvor man med telefonen kan få adgang til realtidsovervågningen og selv starte en videooptagelse.

Ved brug af en form for memory-kort vil producenten kun have bestemt formålet, men ikke hjælpemidlerne til den behandling der foregår i forbindelse med lagringen af optagelserne. Med udgangspunkt i det primære eksempel, er formålet med kameraet at overvåge huset og at kunne køre hen til en bestemt person. Dette er formuleret på producentens hjemmeside og medfører muligvis et medansvar i bestemmelsen af formålet.

Hvis producenten var dataansvarlig, ville denne skulle fastlægge formålet og sikre sig, at indsamlingen ikke går ud over, hvad der er nødvendigt for at opnå dette formål. I relation til dette, er der en anden robotstøvsuger med et infrarødt-kamera fremfor et RGB-kamera, netop for at imødekomme hensynet til privatlivet. Udskiftningen af kameraet kan dog have betydning for støvsugerens navigationsevne, men hvorvidt RGB-kameraet er nødvendigt for at opnå robotstøvsugerens formål, kan ikke endeligt konkluderes, men den lille forbedring som RGB-kameraet medfører, vil sandsynligvis ikke være proportionel med risikoen for beskyttelse af privatlivet. Med anvendelse af kameraet og den dertilhørende behandling for at forbedre navigationen, vil producenten skulle efterleve principperne i Forordningen. Udover kravet om formål og formålsbegrænsning, betyder dette blandt andet også at producenten skal gøre det klart, at der behandles personoplysninger, og i øvrigt hvilke personoplysninger der behandles. Dette vil muligvis kræve en form for skiltning på produktet, uanset om dette er en robotplæneklipper eller en robotstøvsuger, som gør det klart overfor registrerede, at der optages. Dette ville næppe være nødvendigt ved et opsat kamera og er heller ikke nævnt i František Ryneš-sagen. Det ville derudover også skulle fremgå af producentens hjemmeside, hvad formålet med kameraet er og præcis hvilke personoplysninger, der viderebehandles til formålet om at forbedre navigationsevnen.

På baggrund af ovenstående, vil det nu vurderes ud fra de oprindeligt fastlagte scenarier, hvornår privatpersonen og producenten kan være dataansvarlige.

Formålet med kameraet: overvågning eller navigation?

Hvis formålet er overvågning og producenten ikke har adgang til de lagrede personoplysninger og at køberen derudover kan slå denne funktion fra eller til, vil producenten sandsynligvis ikke være dataansvarlig. Hvis formålet i stedet er navigation og at kameraet ikke kan slås fra, og den dataansvarlige behandler disse oplysninger med henblik på at forbedre navigationen, bestemmer producenten over både formål og hjælpemidler og vil sandsynligvis være selvstændig dataansvarlig.

Placering af robotstøvsugeren: i hjemmet eller på offentligt område?

Hvis placeringen er i hjemmet, vil køberen som udgangspunkt ikke være dataansvarlig. Producenten kan dog blive dataansvarlig, afhængigt af de samme betragtninger, som er nævnt ovenfor. Køberen vil dog i alle situationer, blive ansvarlig for den behandling der sker, i forbindelse med deling af personoplysningerne på internettet. Hvis køberen derfor vælger at uploade billeder eller videoer af en indbrudstyv i hjemmet, vil køberen altså være dataansvarlig for denne behandling.

Opbevaring af oplysningerne: Lokalt eller på cloud?

Hvis optagelserne lagres lokalt og den private i øvrigt har fuld kontrol over hjælpemidlerne hertil, vil det udelukkende være køberen der kan være dataansvarlig. Ved cloud-løsningen kan producenten blive dataansvarlig, men der skelnes mellem cloud-løsningen og produktet. Disse vil sandsynligvis medføre to forskellige behandlinger, som skal adskilles.

Dreamebot D10s

Producenten af Dreamebot D10s vil sandsynligvis ikke være dataansvarlig for de personoplysninger, som robotstøvsugeren behandler. Robotstøvsugeren fungerer primært som et sikkerhedskamera, som kan slås til og fra af køberen. Det vil derfor være køberen der er dataansvarlig for behandlingen af personoplysninger. Det er dog ikke usandsynligt at Dreametech vil være dataansvarlig for den behandling, som foretages af deres app, som bruges i forbindelse med realtidsovervågningen.

Kapitel 5. Konklusion

For at være dataansvarlig, som defineret i Forordningen, kræver det at den behandling man foretager sig, er inden for Forordningens anvendelsesområde. Dette kræver at man behandler personoplysninger ved hjælp af automatisk databehandling eller anden ikkeautomatisk behandling af personoplysninger, der vil blive indeholdt i et register. Det kræver desuden at behandlingen finder sted indenfor Unionen, som defineret i det territorielle anvendelsesområde. Det territorielle anvendelsesområde er bredt. En dataansvarlig uden for Unionen vil i mange tilfælde behandle oplysninger indenfor anvendelsesområdet, hvis denne behandling vedrører fysiske personer indenfor Unionen.

Som privatperson kan man dog være undtaget fra dette anvendelsesområde, hvis behandlingen udelukkende foretages som led i rent personlige eller familiemæssige aktiviteter. Specialet har afgrænset disse aktiviteter og det kan konkluderes at behandling, hvis formål er at gøre personoplysninger tilgængelige for et ubestemt antal personer, eller når denne aktivitet endda – om end kun delvist – omfatter det offentlige rum, ikke er omfattet af denne undtagelse. Fysiske personer, som behandler personoplysninger ved at dele disse på internettet, eller ved at optage offentlige rum, kan derfor blive dataansvarlige.

Det kan herefter konkluderes, at de afgørende elementer i vurderingen af, om man er dataansvarlig eller ej, er hvorvidt man er med til at bestemme formål og hjælpemidler. Det er i denne forbindelse

ikke nødvendigt at man bestemmer både formål og hjælpemidler og det er heller ikke nødvendigt at man alene bestemmer disse, da der kan være flere dataansvarlige for den samme behandling af personoplysninger og beslutningen om formål og hjælpemidler godt kan være konvergerende. Det er derudover heller ikke nødvendigt for begge dataansvarlige at have adgang til de indsamlede oplysninger, for at være dataansvarlige.

Til sidst er disse principper og analysen af retstilstanden blevet anvendt på en konkret case, hvor det kan konkluderes at producenten af den undersøgte robotstøvsuger, der funktionelt fungerer som et sikkerhedskamera, ikke vil være dataansvarlig for den behandling, som robotstøvsugeren foretager, selvom det er producenten der har bestemt formål med behandlingen. Producenten kan dog være dataansvarlig for behandlingen der foretages af deres app eller hvis producenten i øvrigt indsamler oplysningerne, med det formål at forbedre navigationsevnen. Det afgørende er, om producenten er med til at bestemme formål og hjælpemidler i en væsentlig grad.

Den private køber af et produkt vil ikke være dataansvarlig medmindre denne anvender produktet på en måde, der resulterer i at det offentlige rum bliver filmet. Heri ligger der dog en vurdering af den konkrete situation og såfremt produktet udelukkende er i hjemmet, vil behandling af personoplysninger igennem vinduet og ud på vejen ikke betyde at den private er dataansvarlig. Hvis kameraet dog i stedet var placeret på en robotplæneklipper, et sikkerhedskamera udendørs eller personen gik tur med sin robotstøvsuger, vil den private køber dog være dataansvarlig og vil i den forbindelse skulle iagttage forpligtelserne i Forordningen, herunder sikre sig at der er et behandlingsgrundlag og at principperne i øvrigt er overholdt.

Bibliografi

- Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)
- Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger

Datatilsynet. (u.d.). *Vejledning om dataansvarlige og databehandlere.* Hentet fra Datatilsynet.dk.

EDPB. (u.d.). *Retningslinjer 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse.* Hentet fra edpb.europa.eu: https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_da.pdf

EDPB. (u.d.). *Retningslinjer 1/2020 om behandling af personoplysninger i forbindelse med opkoblede køretøjer og mobilitetsrelaterede anvendelser.* Hentet fra edpb.europa.eu: https://www.edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_da.pdf

Lotterup, A., & Nielsen, K. K. (2020). *Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udgave.*

Munk-Hansen, C. (2018). *Retsvidenskabsteori 2. udgave.*

Udsen, H. (2022). *Databeskyttelsesret.* Hentet fra https://databeskyttelsesret.dk/.