Kandidatspeciale

Cloudleverandørernes udlevering af personoplysninger til amerikanske myndigheder

Disclosure of personal data by cloud providers to US authorities

Forfattere:

Julie Dahl Schneider, Studienr.: 20194081

Thilde Winther, Studienr.: 20195561

Vejleder: Tanja Kammersgaard Christensen

Anslag: 161.461

Indholdsfortegnelse

Abstract

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) entered into force on the 25th of May 2018.[1] This thesis examines the data protection issues that arise when US cloud providers may be required to disclose personal data to the US authorities under Foreign Intelligence Surveillance Act section 702 (FISA 702) and the Clarifying Lawful Overseas Use of Data (CLOUD Act).

To answer this question, the thesis examines what requirements the data processing agreement must fulfill to comply with the GDPR. In addition, the thesis examines how the data controller ensures that the processing of personal data is in accordance with the GDPR when using a cloud provider with sub-processors in the US. Finally, the thesis examines how the controller ensures that a US cloud provider does not disclose personal data as a result of a CLOUD Act request. The above is analyzed through GDPR, case law from the European Court of Justice, and case law from the Danish Data Protection Agency. Furthermore, guidelines and statements etc. from EDPB and the Danish Data Protection Agency are used in the analyzes.[2]

Finally, the thesis concludes that the data processing agreement must meet the minimum requirements set out in Article 28(3)(a)-(h) of the GDPR in order to comply with the GDPR. The thesis focuses in particular on the minimum requirements that have the greatest impact on whether the US authorities can access the personal data, cf. Article 28(3)(a), (c), (d) and (h) of the GDPR.[3]

If the cloud provider has a sub-processor in the US, Chapter V of the GDPR must be observed and in this connection a valid basis transfer must be ensured, cf. Article 44 of the GDPR. Article 46(2)(c) of the GDPR can be used as a valid basis for transfer in the absence of an adequacy decision but is conditional on there being an adequate level of protection. This means that it is a level of protection that essentially corresponds to the level in the EU/EEA. FISA 702 and E.O 12333 entails that the standard clauses under Article 46(2)(c) of the GDPR cannot be

[1] (Databeskyttelsesforordningen, 2016)
[2] Jf. nærmere herom i kapitel 2 angående specialets problemformulering
[3] (Databeskyttelsesforordningen, 2016), artikel 28, stk. 3 samt nærmere herom i kapitel 7 angående databehandleraftalen

applied without additional measures. Encryption can be used as an additional measure, but the encryption must be effective so that personal data in clear text is not transferred to the US.[4]

However, there is an adequacy decision, which means that the controller can also ensure compliance with the GDPR when using a cloud provider with sub-processors in the US by using data processors certified under the Data Privacy Framework. Another way the controller can ensure compliance with the GDPR when using a cloud provider is for the controller to completely opt out of allowing the cloud provider to use sub-processors in third countries. This must be clearly stated in the data processing agreement.[5]

The controller can ensure that a US cloud provider does not disclose personal data in response to a CLOUD Act request as a result of an instruction by removing the instruction in the data processing agreement. Based on the Danish Data Protection Agency's findings, the instruction will be removed by changing the wording in the data processing agreement to "required" to transfer by EU or the Member State law instead of instead of "as necessary" or "permitted" by the law or binding order from a governmental body if the data controller does not want a transfer to the US pursuant to a CLOUD Act request.[6]

Based on the Danish Data Protection Agency's findings, it can be inferred that the previous unclarity in the literature in relation to whether the data controller must clarify doubts of interpretation has been clarified. The Danish Data Protection Agency has clearly stated that doubts of interpretation in the data processing agreement should, as a general rule, be avoided. Thus, it can be concluded that the data controller can avoid that the cloud provider discloses personal data to the US authorities by developing a data processing agreement with clear and transparent provisions so that there is no doubt about interpretation. This doubt of interpretation can be avoided in the data processing agreement by ensuring that the wording of the provisions is identical.[7]

[4] (Schrems I C-362/14, 2015), (Schrems II C-311/18, 2020), (Datatilsynet, Journalnummer: 2020-431-0061, 2022)og (Databeskyttelsesforordningen, 2016), artikel 44 og 46, stk. 2, litra c. Nærmere herom i kapitel 9 angående cloudleverandører med underdatabehandlere i USA

[5] (Databeskyttelsesforordningen, 2016), artikel 28, stk. 3, litra d, jf. artikel 28, stk. 2

[6] Aktindsigten afsnit 2.2 (Bilag 1)

[7] Aktindsigten afsnit 2 og 2.2 (Bilag 1)

1. Indledning

Europa-Parlamentet og Rådets forordning (EU) 2016/679 (herefter "databeskyttelses-forordningen") trådte i kraft den 25. maj 2018.[8] Databeskyttelsesforordningen har til formål at beskytte fysiske personers personoplysninger, som er en grundlæggende rettighed efter Den Europæiske Unions (herefter "EU") charter om grundlæggende rettigheder (herefter "chartret") art. 8 samt Traktaten om Den Europæiske Unions funktionsmåde (herefter "TEUF") art. 16.[9] Retten til beskyttelse af personoplysninger er af særlig betydning i nyere tid, hvor teknologien udvikler sig eksplosivt, og globaliseringen spiller en stadig større rolle.[10] Den teknologiske udvikling har medført, at virksomheder får assistance til persondatabehandling af andre virksomheder i højere grad, fordi behandling af personoplysninger kan være komplekst og kræve mange ressourcer.[11]

De europæiske virksomheders anvendelse af cloudleverandører er steget markant de seneste år.[12] Dette skyldes formentlig, at anvendelsen af cloudleverandører giver fordele for virksomhederne, herunder både økonomiske fordele og fordele i form af mere sikker og effektiv teknologi.[13] Brugen af cloudleverandører kan dog være problematisk i henhold til databeskyttelsesforordningen, idet de fleste cloudleverandører er amerikansk ejet, og derfor kan der opstå tvivl om cloudleverandørens evne og vilje til at overholde databeskyttelsesforordningen.[14] Det danske datatilsyn (herefter "Datatilsynet") har flere gange udtalt sig i forbindelse med brugen af cloudleverandører. Allerede i år 2011 kom Datatilsynet med en udtalelse angående brugen af cloudleverandører. Dengang erklærede Datatilsynet, at der generelt var et gunstigt synspunkt på brugen af cloudleverandører, men Datatilsynet pointerede samtidig vigtigheden af de registreredes rettigheder og beskyttelsen heraf.[15] Cloudleverandører er stadig et relevant område at diskutere i forhold til databeskyttelsesret. Datatilsynet har senest udtalt kritik ved brugen af cloudleverandører, navnlig i forbindelse med Helsingør/Chromebook-sagen[16] (herefter "Chromebook-sagen"). Derudover har Datatilsynet

[8] (Databeskyttelsesforordningen, 2016), artikel 99
[9] (Databeskyttelsesforordningen, 2016) artikel 1, stk. 1 og præambelbetragtning nr. 4
[10] (Databeskyttelsesforordningen, 2016) præambelbetragtning nr. 6 og 7
[11] (Blume, Den nye persondatarets aktører, 2018), side 61 og (Motzfeldt, 2022), side 79
[12] (Blume, Den nye persondatarets aktører, 2018), side 62
[13] (Nielsen & Lotterup, 2020), side 656
[14] (Udsen, 2022), side 106
[15] (Nielsen & Lotterup, 2020), side 653 og (Datatilsynet, Journalnummer: 2010-52-0138, 2011)
[16] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)

udtalt sig vedrørende tilsigtet og utilsigtet overførsler til USA i forbindelse med en forespørgsel om brug af cloudleverandører fra KOMBIT (herefter "KOMBIT-sagen").[17]

De amerikanske cloudleverandører Amazon Web Service (herefter "AWS"), Google LLC (herefter "Google") og Microsoft Azure er de dominerende leverandører på markedet.[18] Fælles for disse cloudleverandører er, at deres moderselskab er placeret i USA, og deres datterselskaber er placeret i hele verden, heriblandt flere steder i Europa.[19] Den amerikanske lovgivning er derfor vigtig at holde sig for øje, navnlig Foreign Intelligence Surveillance Act section 702 (herefter "FISA 702") og Clarifying Lawful Overseas Use of Data Act (herefter "CLOUD Act"), idet disse lovgivninger kan påtvinge cloudleverandørerne til udlevere personoplysninger til de amerikanske myndigheder.[20] Den amerikanske overvågnings-lovgivning er problematisk, og FISA 702 har blandt andet været årsagen til, at de vedtagne tilstrækkelighedsafgørelser Safe Harbor og EU-US Privacy Shield (herefter "Privacy Shield") blev erklæret ugyldig i Schrems-dommene.[21] I skrivende stund eksisterer en gyldig tilstrækkelighedsafgørelse, såkaldt EU-US Data Privacy Framework (herefter "Data Privacy Framework"), og personoplysninger kan således overføres til USA med hjemmel heri.[22] Dog kan der reflekteres over, hvorvidt der er en risiko for, at der kommer en Schrems III i fremtiden.[23]

Med øget udlicitering af personoplysninger til amerikanske cloudleverandører er det vigtigt at have fokus på de komplekse databehandleraftaler, og risikoen for at personoplysningerne bliver genstand for overvågning i henhold til den amerikanske lovgivning. Netop databehandler-aftalen er et vigtigt element for at sikre, at behandlingen af personoplysningerne er i overens-stemmelse med databeskyttelsesforordningen.[24]

[17] (Datatilsynet, Journalnummer: 2022-212-3529, 2022)
[18] (Jensen, 2023) *"Tre leverandører sidder på 65 procent af markedet: Her er verdens største cloud-leverandører lige nu"* og (Hassan, Top 20 Cloud Computing Companies in USA, 2023)
[19] (Nasdaq, 2024)
[20] (U.S.C § 1881a) og (CLOUD Act, 2018), section 103
[21] (Schrems I C-362/14, 2015) og (Schrems II C-311/18, 2020)
[22] (Schrems I C-362/14, 2015), (Schrems II C-311/18, 2020) og (Datatilsynet, EU-U.S. Data Privacy Framework, 2024)
[23] (Olifent, Mens Biden og von der Leyen smiler, er Schrems III allerede i støbeskeen, 2022)
[24] (Databeskyttelsesforordningen, 2016), artikel 28

2. Problemformulering

I specialet analyseres de databeskyttelsesretlige problematikker, der opstår, når de amerikanske cloudleverandører kan blive underlagt at udlevere personoplysninger til de amerikanske myndigheder i henhold til FISA 702 og CLOUD Act.

For at besvare ovenstående problemformulering anvendes følgende underspørgsmål:

- Hvilke krav skal databehandleraftalen opfylde for at overholde databeskyttelsesforordningen?
- Hvordan sikrer den dataansvarlige, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen, når der anvendes en cloudleverandør med underdatabehandlere i USA?
- Hvordan sikrer den dataansvarlige, at en amerikansk cloudleverandør ikke udleverer personoplysninger som følge af en CLOUD Act-anmodning?

3. Afgrænsning

Specialet afgrænser sig først og fremmest til en specifik del af databeskyttelsesforordningen, navnlig kapitel V og art. 28. I kapitel V vil specialet være afgrænset til at beskæftige sig med art. 44, 45, 46, stk. 1-2, litra c, 48 og 49, stk. 1, litra d-f samt stk. 1, 2. pkt. Endvidere vil specialet henvise til andre bestemmelser i databeskyttelsesforordningen, såfremt det er relevant for besvarelsen af problemformuleringen. Databeskyttelsesloven bliver ikke belyst i nærværende speciale, idet der ikke er relevante nationale bestemmelser angående tredjelandsoverførsler og databehandleraftaler.

Specialet er afgrænset til EU-Domstolens- og Datatilsynets afgørelser, hvilket betyder, at afgørelserne fra de danske domstole ikke vil blive analyseret i nærværende speciale. Dette skyldes, at der er afsagt få domme, og disse domme har ikke relevans for specialets problemformulering. EU-Domstolens afgørelser, Schrems I og II, er afgrænset til udvalgte præmisser, som er relevante for besvarelsen af specialets problemformulering. I forbindelse med Schrems I vil databeskyttelsesdirektivet blive nævnt, men idet databeskyttelses-forordningen siden hen har erstattet denne, vil specialet ikke behandle databeskyttelses-direktivet yderligere. Endvidere er Chromebook-sagen ligeledes afgrænset til udvalgte problemstillinger, herunder problemstillingen angående tredjelandsoverførsler og amerikansk

lovgivning. Desuden vil afgørelser fra andre landes datatilsyn og andre landes domstole ikke blive analyseret i nærværende speciale, grundet specialets omfang.

Herudover vil specialet være afgrænset til USA, selvom begrebet *usikre tredjelande* tillige omfatter andre lande. Dette skyldes, at specialet har fokus på amerikanske cloudleverandører, der har moderselskab og/eller underdatabehandlere i USA. Desuden vil specialet være afgrænset til udvalgte amerikanske lovgivninger, herunder FISA 702, E.O. 12333, Presidential Policy Directive 28 (herefter "PPD-28") og CLOUD-Act som har særlig relevans for besvarelse af problemformuleringen. Specialet vil dog ikke uddybe nærmere retskildeværdien af disse lovgivninger samt rangfølge og lignende i USA. Dette skyldes, at det vil kræve et stort kendskab til det amerikanske retssystem.

Herudover vil specialet være afgrænset til bestemte cloudleverandører, navnlig AWS og Google. Der har været fokus på andre store amerikanske selskaber i nyere tid, herunder Meta, som har været kritiseret for manglende tilstrækkeligt beskyttelsesniveau af personoplysninger ved overførsler til USA.[25] Derudover har Den Europæiske Tilsynsførende for Databeskyttelse (herefter "EDPS") udsendt en pressemeddelelse, hvoraf det fremgår, at Europa-Kommissionen (herefter "EU-Kommissionen") har overtrådt databeskyttelsesforordningen ved brug af Microsoft.[26] For ganske nylig har Datatilsynet udtalt kritik af Telmore A/S' behandling af personoplysninger, herunder overførsel til USA, gennem Telmore A/S' brug af Meta Irland.[27] Disse sager er et udtryk for, at problematikken med de amerikanske selskaber er yderst relevant i nyere tid, men disse sager indgår ikke i specialet grundet specialets omfang.

Slutteligt er specialet afgrænset til retspraksis, lovgivning, udtalelser og lignende, der er offentliggjort inden den 15. maj 2024, hvor nærværende speciale er færdiggjort og afleveret.

[25] (Datatilsynet, Bøde på 1,2 milliarder euro til Meta Irland som følge af bindende afgørelse fra EDPB, 2023)
[26] (EDPS, 2024), "*European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies*"
[27] (Datatilsynet, Journalnummer: 2023-31-0007, 2024)

4. Metode og retskilder

Dette kapitel vil beskrive metoden, der er benyttet til at udarbejde specialet samt beskrive de anvendte retskilder.

4.1 Retsdogmatisk metode

For at besvare specialets problemformulering anvendes den retsdogmatiske metode. Fremgangsmåden ved den retsdogmatiske metode er at beskrive og analysere gældende ret, *de lege lata*.[28] Den retsdogmatiske metode anvender retskilderne med henblik på at klarlægge gældende ret.[29]

Metoden indebærer en fastlæggelse af relevant faktum, jus og resultat, hvilket gælder universelt.[30] Fastlæggelsen af disse, vil det ikke bero på en subjektiv holdning, men afhænger derimod af en række forhold. Det betegnes som en *retlig subsumption*, når de faktiske forhold henføres under en retsregel.[31]

Den retsdogmatiske metode benyttes i specialet til at fastlægge og beskrive retstilstanden. Mere specifikt benyttes metoden til at fastlægge og beskrive retstilstanden indenfor databeskyttelsesretten, navnlig i forbindelse med cloudleverandørers udlevering af personoplysninger til de amerikanske myndigheder. Et metodisk problem i specialet er, at Datatilsynets dialog med cloudleverandørerne og de dataansvarlige ikke altid offentliggøres. Der er opnået adgang til en relevant dialog gennem aktindsigt, som vil blive benyttet til at fastlægge og beskrive den gældende retstilstand.

4.2 Retskilder

Nærværende kapitel vil beskrive relevante retskilder, som benyttes i specialet. Retskilderne udgør autoritative kilder, hvoraf retten udspringer. Retskilder er bredt defineret, men det afgørende er, om retskilden har betydning for regelskabelsen.[32] Endvidere kan retskilderne

[28] (Munk-Hansen, 2018), side 10-11
[29] (Blume, Retssystemet og juridisk metode, 2020), side 277
[30] (Munk-Hansen, 2018), side 11
[31] Ibid., side 10
[32] Ibid., side 15

oplistes i et retskildehierarki - den såkaldte *retlige trinfølge*. Dette retskildehierarki kan illustreres nedenfor, hvoraf det fremgår, at EU-retten har forrang:[33]

Reguleringer:

1. EU's traktater, herunder chartret samt almindelige EU-retlige principper mv.
2. Forordninger, herunder databeskyttelsesforordningen, direktiver, love, konventioner
3. Bekendtgørelser, cirkulærer mv.

Praksis:

1. Retspraksis, administrativ praksis, herunder Datatilsynets praksis mv.
2. Retssædvane, branchekutyme, aftalepraksis
3. Almindelige retsgrundsætninger, fortolkningsprincipper[34]

4.2.1 Traktaten om Den Europæiske Unions funktionsmåde

EU-retten hviler på traktatretligt grundlag og er som udgangspunkt defineret som folkeret.[35] Som det fremgår af Grundlovens § 20, har Danmark delvist afgivet suverænitet.[36] EU-rettens retsdannelse er derfor supranational og retten skabes i EU's institutioner, hvor der fastlægges regler for medlemsstaterne og deres borgere.[37]

Traktaterne udgør et sæt aftaler mellem medlemsstaterne og EU-retsakterne har hjemmel i traktaterne. Endvidere indeholder traktaterne en række principper, og disse traktatfæstede principper har stor betydning ved fortolkning af retsakterne som EU's institutioner udsteder. Det er essentielt, at EU-rettens retsakter udfyldes og fortolkes i overensstemmelse med principperne, heriblandt solidaritetsprincippet, som indebærer, at medlemsstaterne er forpligtet til at implementere EU-retten loyalt.[38]

[33] (Munk-Hansen, 2018), side 17-18
[34] (Nielsen & Tvarnø, 2021), side 60 og (Munk-Hansen, 2018), side 17-18
[35] (Munk-Hansen, 2018) side 38-39
[36] (Grundloven, § 20)
[37] (Munk-Hansen, 2018), side 43
[38] Ibid., side 42-43

4.2.2 Den Europæiske Unions Charter om Grundlæggende Rettigheder

Chartret er som altid gældende i både EU-retten og nationalret.[39] Chartret har samme juridiske værdi som traktaterne.[40] Dermed defineres chartret som en del af EU's primærret og med vedtagelsen af Lissabontraktaten i 2009, blev chartret juridisk bindende for medlemsstaterne.[41] Databeskyttelsesforordningens art. 1, stk. 2-3 fastlægger formålene med forordningen, hvor det ene formål har relation til chartret. Det fremgår navnlig af databeskyttelsesforordningens art. 1, stk. 2, at ét af disse formål er at beskytte *"fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger."*[42] Det fremgår ligeledes af præambelbetragtning 4, at databeskyttelsesforordningen overholder de grundlæggende rettigheder, samt de frihedsrettigheder og principper, som fremgår af chartret.[43]

Det er dermed tydeliggjort i databeskyttelsesforordningen, at alle chartrets bestemmelser kan have en markant indvirkning i en databeskyttelsesretlig kontekst. Specialet vil have særlig fokus på de rettigheder som fremgår af henholdsvis chartrets art. 7, 8, 47 og 52.[44]

> Chartrets art. 7 omhandler beskyttelse af privatlivets fred, og chartrets art. 8 omhandler særskilt retten til beskyttelse af personoplysninger. Chartrets art. 47 vedrører retten til effektive retsmidler og til en upartisk domstol. Slutteligt har specialet tillige fokus på Chartrets art. 52, stk. 1, som indeholder et proportionalitetsprincip, hvilket medfører, at der kun kan indføres begrænsninger i rettighederne, hvis det er nødvendigt og har et formål som er anerkendt i Unionen.

Disse bestemmelser spiller en central rolle i EU-domstolens praksis i henhold til offentlige myndigheders adgang til personoplysninger.[45]

4.2.3 Databeskyttelsesforordningen

Databeskyttelsesforordningen erstattede databeskyttelsesdirektivet den 25. maj 2018.[46] Væsentligt for forordninger er, at disse er almengyldige.[47] Forordninger er dermed bindende i alle enkeltheder og gælder direkte for enhver medlemsstat og dennes borgere. Formålet med

[39] (Hamer & Schaumburg-Müller, 2020), side 277
[40] (EU-traktaten, artikel 6)
[41] (Udsen, 2022), side 41
[42] (Motzfeldt, 2022), side 30
[43] (Databeskyttelsesforordningen, 2016) præambelbetragtning nr. 4
[44] (Motzfeldt, 2022), side 30
[45] (Motzfeldt, 2022), side 30 ff.
[46] Ibid., side 34
[47] (TEUF), artikel 288

forordninger er at opnå en ensartet lovgivning indenfor EU.[48] En forordning er den stærkeste form for sekundærret,[49] og inden for databeskyttelsesretten er databeskyttelsesforordningen den centrale retskilde.[50] Som følge af forordningens universelle karakter, skal disse som udgangspunkt ikke implementeres i medlemsstaternes nationale ret. Dog kan medlemsstaterne supplere en forordning med national lovgivning, hvis forordningens regulering på enkelte områder ikke er entydige og fuldt ud anvendelig. Dette er tilfældet med databeskyttelses-forordningen, som suppleres af den danske databeskyttelseslov.[51]

Forordninger fra EU indledes med en præambel, og disse præambelbetragtninger angiver de overordnede hensyn, som medvirker til forståelsen af artiklerne.[52] Databeskyttelses-forordningen indeholder 173 præambelbetragtninger, hvoraf der kan udledes fortolknings-bidrag til artiklerne og retsaktens baggrund.[53]

Databeskyttelsesforordningens formål og de overordnede principper for behandling af personoplysninger er nogle af de forhold, som altid skal tages hensyn til, når databeskyttelses-forordningen fortolkes.[54] Udover det nævnte formål i afsnit 4.2.2, har databeskyttelses-forordningen tillige til formål at fremme fri udveksling af personoplysninger.[55] Formålene kan virke modstridende, men skal ikke anses som modsætninger. Formålene skal derimod afvejes, når databeskyttelsesforordningen skal fortolkes og anvendes.[56]

4.2.4 Databeskyttelsesloven

Som nævnt i afsnit 4.2.1 har Danmark i medfør af Grundlovens § 20 delvist overdraget lovgivningskompetence. Dette medfører, at EU-retten er en del af gældende dansk ret.[57] Databeskyttelsesforordningen forudsætter, at medlemsstaterne fastsætter nationale regler som supplerer forordningens artikler.[58] På den måde kan medlemsstaterne opretholde eksisterende

[48] (Hamer & Schaumburg-Müller, 2020), side 142
[49] (Blume, Retssystemet og juridisk metode, 2020), side 276
[50] (Hamer & Schaumburg-Müller, 2020), side 268
[51] Ibid., side 142 og 265
[52] (Blume, Retssystemet og juridisk metode, 2020), side 189 og 277
[53] (Blume, Retssystemet og juridisk metode, 2020), side 277 og (Nielsen & Lotterup, 2020), side 158
[54] Principperne fremgår af databeskyttelsesforordningens artikel 5
[55] (Databeskyttelsesforordningen, 2016) artikel 1, stk. 3
[56] (Nielsen & Lotterup, 2020), side 205
[57] (Munk-Hansen, 2018), side 43 og 44
[58] (Blume, Retssystemet og juridisk metode, 2020), side 276

særregulering og have mulighed for at indføre egne særregler.[59] Databeskyttelsesloven supplerer dermed databeskyttelsesforordningen og de to retsakter skal betragtes i sammenhæng.[60]

4.2.5 Retspraksis

En anden central retskilde inden for databeskyttelsesretten, som benyttes til at besvare specialet, er retspraksis fra EU-domstolen. EU-Domstolen afgør ultimativt fortolkningen af databeskyttelsesforordningen og deres retspraksis er retsskabende.[61] Det er gennem domstolspraksis, at reglerne inden for databeskyttelsesretten bliver udfyldt og præciseret.[62] I dette speciale udgør retspraksis inden for databeskyttelsesretten, både fra EU-Domstolen og Datatilsynet, et væsentligt fortolkningsbidrag. Gennem tiden har EU-Domstolen afsagt domme, som har betydelig indflydelse og bidraget til forståelsen af databeskyttelsesretten, navnlig i C-362/14 og C-311/18 (herefter "Schrems I" og "Schrems II").[63] I forbindelse med EU-Domstolens afgørelser, kan det bemærkes, at generaladvokatens forslag kan anvendes til at uddybe dommene afsagt af EU-Domstolen.[64]

Antallet af danske domme er begrænset, men vil formentlig stige i takt med flere præjudicielle forelæggelser for EU-Domstolen.[65] Medlemslandenes nationale datatilsyn kan ved fortolkningstvivl forelægge EU-Domstolen præjudicielle spørgsmål.[66] De afsagte domme fra EU-domstolen har en stor retskildemæssig værdi, da EU-domstolens afgørelser fastlægger, hvad gældende EU-ret er. Medlemsstaterne er forpligtet til at følge EU-domstolens retsopfattelse og er bindende for de nationale medlemsstater.[67]

4.2.6 Det Europæiske Databeskyttelsesråd og tilsynsafgørelser

Det Europæiske Databeskyttelsesråd (herefter "EDPB") er en gruppe, som består af EU-landenes ledere af datatilsynene, samt Den Europæiske Tilsynsførende for databeskyttelse

[59] (Udsen, 2022), side 43
[60] (Motzfeldt, 2022), side 36 og 37
[61] Ibid., side 32-33 og (Munk-Hansen, 2018), side 42
[62] (Udsen, 2022), side 43
[63] Ibid., side 48
[64] (Motzfeldt, 2022), side 33
[65] (Udsen, 2022), side 48 og 49
[66] Ibid., side 50
[67] (Blume, Retssystemet og juridisk metode, 2020), side 278

(herefter "EDPS") og en repræsentant fra EU-Kommissionen.[68] EDPB har erstattet den tidligere Artikel 29-gruppe. Medlemsstaterne blev pålagt efter det tidligere databeskyttelses-direktiv og nu databeskyttelsesforordningen at etablere en national uafhængig tilsyns-myndighed, hvilket tillige er en forpligtelse efter chartrets art. 8, stk. 3 og TEUF art. 16.[69] I Danmark udgør den nationale tilsynsmyndighed, Datatilsynet, som har en række opgaver og beføjelser i medfør af databeskyttelsesforordningen.[70] Datatilsynet har i medfør af databeskyttelsesforordningens art. 58 en række beføjelser, heriblandt at give kritik, udstede påbud om lovliggørelse af behandlingen, begrænse eller forbyde en behandling.[71] Datatilsynets praksis anses som administrativ praksis, men betragtes som en central retskilde inden for databeskyttelsesretten.[72] Afgørelser truffet af Datatilsynet er betydelig og disse bidrager til en mere generel fortolkning. Datatilsynet består af specialister på området og tillægges en stor vægt, da de danske domstole kun har truffet få afgørelser inden for databeskyttelsesretten.[73]

EDPB og Datatilsynets afgørelser er ikke autoritative og binder ikke domstolene. Derimod giver EDPB og Datatilsynet i deres afgørelser et bud på, hvorledes databeskyttelsesreglerne skal fortolkes. I henhold til databeskyttelsesforordningens art. 65, kan EDPB i få tilfælde træffe bindende afgørelser, hvorved disse afgørelser binder de involverede landes tilsynsmyndigheder. Afgørelser truffet af EDPB indeholder til tider fortolkninger af databeskyttelsesforordningens artikler, som kan tillægges en vægt.[74]

4.2.7 Vejledninger og retningslinjer

Vejledninger fra Datatilsynet og EDPB udgør ligesom afgørelser truffet af disse, ikke autoritative retskilder. Vejledninger og retningslinjerne er derfor ikke bindende for EU-Domstolen og de danske domstole.[75] Vejledningerne er dog i praksis en central retskilde inden for databeskyttelsesretten, fordi de dataansvarlige ofte følger dem. Endvidere bliver Datatilsynets afgørelser truffet i overensstemmelse med vejledningerne og en eventuel

[68] (Hamer & Schaumburg-Müller, 2020), side 270
[69] (Motzfeldt, 2022), side 34 og (Databeskyttelsesforordningen, 2016) artikel 51, stk. 1
[70] (Udsen, 2022), side 50-51. Databeskyttelsesforordningens artikel 57, stk. 1 og artikel 58 indeholder en liste af opgaver og beføjelser som tilsynsmyndighederne varetager
[71] (Databeskyttelsesforordningen, 2016), artikel 58, stk. 2 og (Udsen, 2022), side 53
[72] (Motzfeldt, 2022), side 34
[73] (Udsen, 2022), side 53
[74] Ibid., side 52
[75] (Motzfeldt, 2022), side 35

anfægtning overfor en afgørelse truffet af Datatilsynet kræver, at afgørelsen indbringes for domstolene.[76]

4.2.8 Juridisk litteratur

Der vil i specialet blive inddraget juridisk litteratur, såsom bøger og artikler. Den juridiske litteratur udgør ikke en retskilde. Det skyldes, at blot fordi en forfatter hævder noget i litteraturen, gøres dette ikke til retsregler - forstået på den måde, at en domstol og andre ikke skal træffe en afgørelse ud fra en forfatters holdning.[77] Imidlertid bliver litteraturen med tiden tillagt større betydning, da reguleringen hele tiden forandres.[78]

5. Struktur

Dette kapitel har til formål at skabe et overblik over specialets opbygning. Specialet har først og fremmest et abstract, som kort opsummerer specialets indhold. Kapitel 1 er specialets indledning, hvor emnet præsenteres, og det efterfølgende kapitel 2 er specialets problemformulering. I kapitel 3 afgrænses emnet, og i kapitel 4 beskrives metode samt retskilder. Specialet vil i kapitel 6 skitsere de grundlæggende begreber henholdsvis *den dataansvarlige* og *databehandleren* og *cloudleverandøren*.

Dernæst vil specialet i kapitel 7 beskrive kravene til en databehandleraftale i henhold til databeskyttelsesforordningens art. 28, hvorved første underspørgsmål til problemformulering besvares. I kapitel 8 vil specialet beskrive de databeskyttelsesretlige regler, navnlig databeskyttelsesforordningens kapitel V, som gælder ved tredjelandsoverførsler. Herefter vil specialet i kapitel 9 analysere problemstillingen ved at anvende en cloudleverandør med underdatabehandlere i USA. I den forbindelse vil den problematiske lovgivning i USA analyseres gennem Schrems I og II. Herefter vil problemstillingen med underdatabehandlere i USA blive analyseret gennem Chromebook-sagen.

Kapitel 10 vil herefter analysere den problemstilling, der kan opstå, hvis den amerikanske cloudleverandør og dennes underdatabehandlere er placeret i EU/EØS, og disse bliver mødt af en CLOUD Act-anmodning. I den forbindelse analyseres KOMBIT-sagen og herefter

[76] (Udsen, 2022), side 51
[77] (Munk-Hansen, 2018), side 74
[78] (Blume, Retssystemet og juridisk metode, 2020), side 32

inddrages pointer fra aktindsigten vedrørende KOMBIT-sagen. Slutteligt vil kapitel 11 være en perspektivering og kapitel 12 vil være en konklusion på specialets problemformulering.

6. Begrebsdefinitioner

I nærværende kapitel vil de databeskyttelsesretlige *pligtsubjekter* blive beskrevet. Efterfølgende vil kapitlet beskrive begrebet *cloudleverandør*, som er et centralt begreb i specialet. Inden for databeskyttelsesretten er der tre centrale aktører. På den ene side er de registrerede, *beskyttelsessubjekterne*, som har en række rettigheder i henhold til databeskyttelsesforordningen.[79] På den anden side er den dataansvarlige og databehandleren, *pligtsubjekterne*, som har en række forpligtelser og ansvar.[80]

6.1 Den dataansvarlige

Den dataansvarlige er defineret i legaldefinitionen i databeskyttelsesforordningens art. 4, nr. 7. Det fremgår heraf, at en dataansvarlig er *"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 [...]".*[81] Den dataansvarlige bestemmer således, hvorfor personoplysningerne skal behandles - det vil sige formålet med behandlingen. Derudover bestemmer den dataansvarlige, hvordan personoplysningerne skal behandles - det vil sige hjælpemidlerne til behandlingen.[82]

Den dataansvarlige skal sikre sig, at behandlingsprincipperne i databeskyttelsesforordningens art. 5, stk. 1, litra a-f overholdes. Ifølge Henrik Udsen er behandlingsprincipperne hjørnesten i databeskyttelsesretten og skal altid iagttages.[83] Endvidere følger det af ansvarlighedsprincippet, at den dataansvarlige skal kunne påvise, at behandlingsprincipperne overholdes.[84] Ansvarlighedsprincippet er ikke nærmere uddybet i databeskyttelsesforordningens præambelbetragtninger, men princippet afspejles også i databeskyttelsesforordningens art. 24 og 28. Det

[79] De registreredes rettigheder fremgår af databeskyttelsesforordningens art. 12-23
[80] (Udsen, 2022), side 89
[81] (Databeskyttelsesforordningen, 2016) artikel 4, nr. 7
[82] Ibid., og (Udsen, 2022), side 91
[83] (Udsen, 2022), side 126
[84] (Databeskyttelsesforordningen, 2016), artikel 5, stk. 2 og (Databeskyttelsesforordningen, 2016), præambelbetragtning nr. 74

er som udgangspunkt den dataansvarlige som er pålagt ansvarlighedsprincippet, men i visse tilfælde påhviler det også databehandleren.[85]

6.2 Databehandler og underdatabehandler

Begrebet *databehandler* er defineret i legaldefinitionen i databeskyttelsesforordningens art. 4, nr. 8. Det fremgår heraf, at databehandleren er *"en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne."*[86] Databehandleren skal handle på vegne af den dataansvarlige, hvilket betyder, at databehandleren skal tjene den dataansvarliges interesser samt formål og behandle personoplysningerne efter instruks fra den dataansvarlige. Såfremt databehandleren handler uden for instruks, vil databehandleren blive selvstændig dataansvarlig for den del af behandlingen. Databehandleren handler uden for instruks i det tilfælde, at personoplysningerne behandles til egne formål og hjælpemidler.[87]

Inden for databeskyttelsesretten findes endnu en aktør, navnlig *underdatabehandleren*. Der findes ingen legaldefinition på underdatabehandler i databeskyttelsesforordningen, men er i litteraturen beskrevet som en aktør, der behandler personoplysninger på vegne af den oprindelige databehandler.[88]

6.3 Cloudleverandør

Flere virksomheder vælger at få støtte til persondatabehandling af andre virksomheder i højere grad, fordi behandling af personoplysninger kan være komplekst og kræve mange ressourcer.[89] I den forbindelse vælger nogle virksomheder at benytte cloudleverandører som databehandler, hvor deres personoplysninger herved lagres i *skyen* fremfor at lagre personoplysninger på en lokal server.[90] Cloudleverandørerne tilbyder såkaldt *Cloud Computing*. Ifølge Datatilsynets kan *Cloud Computing* defineres som *"en model til at tilvejebringe standardiserede it-ressourcer, typisk på større decentrale samlinger af servere, der tilgås via internettet"*.[91]

---

[85] (EDPB's Retningslinjer 07/2020 , 2021), side 9
[86] (Databeskyttelsesforordningen, 2016) artikel 4, nr. 8
[87] (Databeskyttelsesforordningen, 2016) artikel 28, stk. 10 og (EDPB's Retningslinjer 07/2020 , 2021), side 28
[88] (Udsen, 2022), side 112 og 113
[89] (Blume, Den nye persondatarets aktører, 2018), side 61 samt (Motzfeldt, 2022), side 79
[90] (Diamond, 2020) (Diamond, 2020), *"Skylager kontra servere i det lokale miljø: Ni ting, som du bør være opmærksom på,"* afsnit 2
[91] (Datatilsynets Vejledning om cloud, 2022), side 4

Der findes flere cloudleverandører på markedet, og de dominerende leverandører er henholdsvis AWS, Microsoft Azure, Alibaba og Google.[92] Specialet har særligt fokus på AWS og Google.

6.4 Rollefordelingen ved brug af en cloudleverandør

Sondringen mellem den dataansvarlig og databehandleren kan i praksis give anledning til tvivl og det er blevet vanskeligere over tid grundet ny kompleks teknologi. Ved fastlæggelsen af aktørernes roller skal der lægges vægt på deres faktiske rolle og ikke den formelle udnævnte rolle i en databehandleraftale. Dette skyldes, at begreberne dataansvarlig og databehandler er funktionelle og dermed skal begreberne fastlægge ansvarsfordelingen ud fra den reelle rolle, som aktørerne har påtaget sig.[93]

Cloudleverandøren behandler personoplysninger på vegne af virksomheden, og derfor er cloudleverandøren databehandler, og virksomheden som anvender cloudleverandøren er dataansvarlig.[94] I praksis kan der dog opstå en situation, hvor cloudleverandøren påbegynder behandling af personoplysninger til egne formål, hvorved cloudleverandøren vil anses som dataansvarlig for den del af behandlingen.[95] Datatilsynet har i en afgørelse fra 2024 anført, at databehandleren Google skal anses som selvstændig dataansvarlig for den behandling, som de foretager til egne formål, herunder brug af personoplysninger til udvikling af Googles applikationer.[96]

6.5 Sammenfatning

På baggrund af kapitel 6 kan det udledes, at der er to pligtsubjekter i databeskyttelses-forordningen henholdsvis den dataansvarlige og databehandleren.[97] Specialet vil i de øvrige kapitler anvende legaldefinitionerne for disse aktører. Som udgangspunkt vil virksomheden være dataansvarlig og cloudleverandøren vil være databehandler, idet cloudleverandøren behandler personoplysninger på vegne af virksomheden.[98] Anvendelsen af en cloudleverandør

[92] (Jones, 2023) *"Cloud markedsandel: et kig på cloud økosystemet i 2024"*
[93] (EDPB's Retningslinjer 07/2020 , 2021), side 10
[94] (Vejledning til anvendelse af cloud, 2020), side 25 og (Nielsen & Lotterup, 2020), side 655
[95] (Databeskyttelsesforordningen, 2016) artikel 28, stk. 10 og (EDPB's Retningslinjer 07/2020 , 2021), side 28
[96] (Datatilsynet Journalnummer: 2023-431-0001, 2024)
[97] (Udsen, 2022), side 89
[98] (Nielsen & Lotterup, 2020), side 655

som databehandler, skal naturligvis være i overensstemmelse med databeskyttelses-forordningen.

7. Databehandleraftalen

Formålet med dette kapitel er at belyse databeskyttelsesforordningens krav til en data-behandleraftale og dermed besvare problemformuleringens første underspørgsmål.[99] AWS og Google har udarbejdet standard-databehandleraftaler, som er ens for alle, der anvender cloudleverandøren, medmindre de formår at forhandle med de langt mere ressourcestærke cloudleverandører.[100]

7.1 Databeskyttelsesforordningens krav

Det følger af databeskyttelsesforordningen, at der skal udarbejdes en databehandleraftale, når en dataansvarlig benytter en databehandler.[101] Før den dataansvarlige påbegynder brugen af en databehandler, skal den dataansvarlige vurdere, hvorvidt den påtænkte databehandler kan og agter at opfylde kravene i databeskyttelsesforordningen.[102] Det er en konkret vurdering, som skal foretages af den dataansvarlige, og hvis der opstår en tvivl i forhold til, hvorvidt databehandleren overholder af databeskyttelsesforordningen, skal den dataansvarlige afklare denne tvivl. Ved brugen af amerikanske cloudleverandører, som databehandler, kan der opstå en tvivl i forhold til udlevering af oplysninger til de amerikanske myndigheder som følge af den amerikanske lovgivning. Ifølge Henrik Udsen skal den dataansvarlige *nok* få afklaret denne tvivl, og dette gælder særligt, når cloudleverandørens vilkår indeholder en tvivl om udleveringen til USA, jf. nærmere herom i kapitel 10.[103]

Kravene til databehandleraftalen fremgår af databeskyttelsesforordningens art. 28, stk. 3, hvor det først og fremmest fremgår, at databehandleraftalen skal: *"fastsætte genstanden for og varigheden for behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorier samt den dataansvarliges forpligtelser og rettigheder".*[104] Minimumskravene til

[99] Databeskyttelsesforordningens krav til indholdet af en databehandleraftale fremgår af databeskyttelsesforordningens artikel 28, stk. 3
[100] (Blume, Den nye persondatarets aktører, 2018), side 66
[101] (Databeskyttelsesforordningen, 2016) artikel 28, stk. 3, 1. pkt.
[102] (Nielsen & Lotterup, 2020), side 610, (Databeskyttelsesforordningen, 2016) præambelbetragtning nr. 81 og (Udsen, 2022), side 105-106
[103] (Udsen, 2022), side 105-106 og (Databeskyttelsesforordningen, 2016) artikel 28, stk. 1
[104] (Databeskyttelsesforordningen, 2016) artikel 28, stk. 3, 1. pkt.

databehandleraftalen fremgår af databeskyttelsesforordningens art. 28, stk. 3, litra a-h. Såfremt databehandleraftalen ikke opfylder ét eller flere af kravene, vil aftalen ikke anses som en gyldig databehandleraftale.[105] Dette ses tillige i en afgørelse fra Datatilsynet, hvor Odense Kommune havde udarbejdet en databehandleraftale, som ikke havde angivet minimumskravet i litra a og derfor kunne aftalen ikke betragtes som en gyldig databehandleraftale.[106]

I de nedenstående afsnit vil specialet fokusere på udvalgte minimumskrav til databehandleraftalen, navnlig databeskyttelsesforordningens art. 28, stk. 3, litra a, c, d og h, idet de har særlig relevans i forhold til at undgå, at cloudleverandøren udleverer personoplysninger til amerikanske myndigheder.

7.1.1 Instruks

I henhold til databeskyttelsesforordningens art. 28, stk. 3, litra a, skal det fremgå af databehandleraftalen, at databehandleren kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, og dette gælder også overførsel til tredjelande.[107] Endvidere skal databehandleraftalen fastsætte, at når *"det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt"*[108] er kravet om instruks ikke er gældende. I dette tilfælde skal databehandleren dog inden databehandlingen underrette den dataansvarlige herom, undtagen hvis underretningen forbydes af den pågældende ret grundet hensyn til vigtige samfundsmæssige interesser.[109]

Desuden følger pligten til at handle efter instruks af databeskyttelsesforordningens art. 29. I henhold til bestemmelsen, må personoplysningerne kun behandles efter instruks fra den dataansvarlige. Kravet om at personoplysningerne udelukkende må behandles efter instruks, gælder for databehandleren og enhver, der behandler personoplysninger for den dataansvarlige eller databehandleren.[110] Instruksen bør være individualiseret til den specifikke databehandling fremfor at have et generaliseret indhold.[111]

[105] (Blume, Den nye persondatarets aktører, 2018), side 66
[106] Datatilsynet, Journal nr. 2016-623-0061 og (Høilund, 2022), side 144
[107] (Nielsen & Lotterup, 2020), side 612
[108] (Databeskyttelsesforordningen, 2016) artikel 28, stk. 3, litra a
[109] Ibid.
[110] (Databeskyttelsesforordningen, 2016) artikel 29 og (Nielsen & Lotterup, 2020), side 619 og 620
[111] (Blume, Den nye persondatarets aktører, 2018), side 68

Såfremt databehandleren behandler personoplysninger uden for instruksen, bliver databehandleren selvstændig dataansvarlig for den del af behandlingen.[112] Det betyder derfor, at databehandleren - som har overtrådt databeskyttelsesforordningen - nu anses som dataansvarlig og skal i den forbindelse overholde databeskyttelsesforordningens krav til en dataansvarlig. Dog er den oprindelige dataansvarlig fortsat ansvarlig efter databeskyttelsesforordningens art. 82-84, og dette skyldes, at det skal sikres, at den dataansvarlige udvælger en databehandler, som kan efterleve databeskyttelsesforordningens krav.[113] Datatilsynet har i en afgørelse fra 2022 udtalt alvorlig kritik, idet underdatabehandleren handlede uden for sin instruks, ved ikke at ville udlevere kundeoplysninger til den dataansvarlige, og hertil anførte Datatilsynet, at underdatabehandleren skulle anses for selvstændig dataansvarlig for den del af behandlingen.[114]

7.1.2 Behandlingssikkerhed

Det følger af databeskyttelsesforordningens art. 28, stk. 3, litra c, at databehandleraftalen skal fastsætte, at databehandleren skal iværksætte de i art. 32 benævnte foranstaltninger. I henhold til databeskyttelsesforordningens art. 32, stk. 1, skal såvel den dataansvarlige som databehandleren sikre at efterleve forordningens krav til behandlingssikkerhed. I den forbindelse skal der foretages en vurdering af rette sikkerhedsniveau ud fra en risikobaseret tilgang. Behandlingssikkerheden skal derfor modsvare de risici, der er ved den pågældende behandling.[115] Det betyder, at jo højere risici, jo strengere krav er der til behandlingssikkerheden.[116] Det er den dataansvarlige, som har ansvaret for at kunne påvise samt dokumentere, at der er tilstrækkeligt behandlingssikkerhed. Derfor skal den dataansvarlige undersøge de mulige risici, der kan opstå for de registrerede som følge af behandlingen og hertil foretage foranstaltninger, som kan dokumenteres. Dette ansvar hænger tillige sammen med databeskyttelsesforordningens art. 5, stk. 2 samt art. 24.[117]

Behandlingssikkerheden kan sikres vha. organisatoriske- og tekniske foranstaltninger, og databeskyttelsesforordningens art. 32, stk. 1, litra a-d oplister nogle sikkerhedsforanstaltninger.

[112] (Databeskyttelsesforordningen, 2016) artikel 28, stk. 10
[113] (Nielsen & Lotterup, 2020), side 617 og 618
[114] (Datatilsynets Journalnummer: 2022-431-0167, 2022)
[115] (Nielsen & Lotterup, 2020), side 634 og 635
[116] Ibid., side 638
[117] Ibid., side 635

Dette er blot eksempler, hvorfor andre foranstaltninger tillige kan benyttes.[118] Bestemmelsen anfører for det første, at en foranstaltning kan være pseudonymisering og kryptering af personoplysningerne.[119] Kryptering opstår, når personoplysninger omsættes til en kode, og kryptering kan benyttes som en foranstaltning til at minimere risikoen for manglende sikkerhed, hvis krypteringen er effektiv.[120] Henning Mortensen skriver i sin artikel om behandlingssikkerhed, at personoplysninger kan krypteres med en krypteringsnøgle og på den måde sikre, at det kun er personer med adgang til dekrypteringsnøglen, som kan læse personoplysningerne. Endvidere anfører Henning Mortensen, at det er væsentligt, at dekrypterringsnøglen ikke er lettilgængelig for uvedkommende, og i den forbindelse kan der overvejes en længere krypteringsnøgle, idet nøglelængden er afgørende for, hvor let det er for uvedkommende at få adgang til at dekryptere dataen. Derudover understreger Henning Mortensen, at der ikke skal være såkaldte *indbygget bagdøre* i krypteringen, da udviklere af de *indbyggede bagdøre* har mulighed for at bryde krypteringen.[121] Kasper Bjerre Hendrup Andersen skriver om krypteringsnøgler i sin artikel, hvor han anfører, at Microsoft og AWS giver deres kunder mulighed for at kryptere deres personoplysninger, hvor kunderne har dekrypteringsnøglen. I den situation vil det ikke være muligt for Microsoft og AWS, at dekryptere dataene og desuden har cloudleverandørerne som udgangspunkt ikke lovlig adgang til at genidentificere personoplysningerne med dekrypteringsnøglen i henhold til databehandleraftalen.[122]

7.1.3 Underdatabehandlere

I henhold til databeskyttelsesforordningens art. 28, stk. 3, litra d skal databehandleraftalen fastsætte, at databehandleren skal opfylde betingelserne for at gøre brug af en under-databehandler.[123]

I henhold til databeskyttelsesforordningens art. 28, stk. 2 må databehandleren ikke benytte en underdatabehandler uden forudgående specifik eller generel skriftlig godkendelse fra den dataansvarlige. Datatilsynet har i en afgørelse fra 2019 udtalt alvorlig kritik, idet Herning

[118] Ibid., side 640
[119] (Databeskyttelsesforordningen, 2016) artikel 32, stk. 1, litra a
[120] (Nielsen & Lotterup, 2020), side 645-646
[121] (Mortensen, 2018), *"Sikkerhedsforanstaltninger – i henhold til databeskyttelsesforordningen"* RR.5.2018.32
[122] (Andersen, 2023), *"Hvornår er en fysisk person "identificeret eller identificerbar" i GDPR's forstand?, 2023",* afsnit 3.1
[123] (Databeskyttelsesforordningen, 2016) artikel 28, stk. 2 og 4

Kommune ikke havde givet forudgående godkendelse til, at databehandleren EG anvendte ServiceNow som underdatabehandler. EG blev derfor selvstændig dataansvarlig for den del af behandlingen.[124]

Endvidere følger det af databeskyttelsesforordningens art. 28, stk. 2, at databehandleren skal underrette den dataansvarlige om ændring, erstatning eller tilføjelse af underdatabehandlere, således at den dataansvarlige kan gøre indsigelse mod dette.[125] Såfremt databehandleren benytter en underdatabehandler, skal der udarbejdes en databehandleraftale mellem databehandleren og underdatabehandleren og videre ned i databehandlerkæden. I den forbindelse skal de vilkår, som den dataansvarlige og databehandleren har indgået i databehandleraftalen, videreføres i databehandleraftalen mellem databehandleren og underdatabehandleren. Vilkårene må således ikke være mildere for underdatabehandleren, men kan være strengere.[126]

7.1.4 Revision og inspektion

I henhold til databeskyttelsesforordningens art. 28, stk. 3, litra h, skal databehandleraftalen indeholde oplysninger om, hvor hyppigt og på hvilken måde udvekslingen af oplysninger mellem databehandleren og den dataansvarlige skal foregå. Dette sikrer, at den dataansvarlige er fuldt informeret om behandlingsaktiviteterne, således at det er muligt at påvise overholdelse af forpligtelserne i databeskyttelsesforordningens art. 28.[127] Derudover pålægges databehandleren at give den dataansvarlige mulighed for at foretage revisioner, herunder inspektioner hos databehandleren og bidrage til sådanne revisioner. Det er dog ikke et eksplicit krav efter databeskyttelsesforordningens art. 28, stk. 3, litra h, at den dataansvarlige skal føre kontrol med databehandleren. Forpligtelsen til at føre løbende tilsyn udspringer derimod af princippet i databeskyttelsesforordningens art. 5, stk. 2, hvorefter den dataansvarlig er ansvarlig for at kunne påvise, at de generelle principper i databeskyttelsesforordningens art. 5, stk. 1 overholdes.[128] Princippet om ansvarlighed lægges til grund i flere afgørelser fra Datatilsynet. Dette illustreres navnlig i en afgørelse fra Datatilsynet i år 2022, hvor Datatilsynet gav kritik, fordi Styrelsen for International Rekruttering ikke førte tilsyn med sine to databehandlere og

[124] (Datatilsynet Journalnummer: 2019-442-3996, 2019)
[125] (Databeskyttelsesforordningen, 2016) artikel 28, stk. 2
[126] (Databeskyttelsesforordningen, 2016) artikel 28, stk. 4 samt (Nielsen & Lotterup, 2020), side 610-611 og 615
[127] (Databeskyttelsesforordningen, 2016), artikel 28, stk. 3, litra h
[128] (Udsen, 2022), side 115 ff.

dermed ikke kunne dokumentere, at principperne i databeskyttelsesforordningens art. 5, stk. 1 overholdes. I den henseende anførte Datatilsynet, at det var i strid med databeskyttelses-forordningens art. 5, stk. 2.[129]

7.2 Sammenfatning

Opsummerende kan det udledes, at i det tilfælde, hvor en dataansvarlig benytter en cloudleverandør som databehandler, skal der udarbejdes en databehandleraftale.[130] I den forbindelse skal den dataansvarlige foretage en vurdering af, hvorvidt cloudleverandøren kan og vil opfylde kravene i databeskyttelsesforordningen. Såfremt den dataansvarlige sår tvivl om cloudleverandøren vil udlevere personoplysningerne til de amerikanske myndigheder som følge af den amerikanske lovgivning, skal den dataansvarlige *nok* afklare denne tvivl.[131]

Databeskyttelsesforordningens art. 28, stk. 3 indeholder en række krav til databehandleraftalen. Databeskyttelsesforordningens art. 28, stk. 3, litra a fastlægger, at databehandleraftalen skal præcisere, at cloudleverandøren kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, og dette gælder også overførsel til tredjelande medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt.[132] Såfremt cloudleverandøren handler uden for instruksen, bliver cloudleverandøren selvstændig dataansvarlige for denne del af behandlingen.[133] Endvidere følger det af databeskyttelsesforordningens art. 28, stk. 3, litra c, at databehandleraftalen skal fastsætte, at databehandleren skal iværksætte de i databeskyttelsesforordningens art. 32 benævnte foranstaltninger. Dette kan eksempelvis være kryptering, som kan minimere risikoen for manglende sikkerhed.[134] I henhold til databeskyttelsesforordningens art. 28, stk. 3, litra d skal databehandleraftalen fastsætte, at databehandleren skal opfylde betingelserne for at gøre brug af en underdatabehandler, herunder at databehandleren ikke må benytte en underdatabehandler uden forudgående specifik eller generel skriftlig godkendelse fra den dataansvarlige. Derudover skal vilkårene i databehandleraftalen tillige være vilkårene for underdata-

[129] (Datatilsynet Journalnummer: 2021-421-0102, 2021)
[130] (Databeskyttelsesforordningen, 2016), artikel 28, stk. 3, 1. pkt.
[131] (Udsen, 2022), side 105-106
[132] (Databeskyttelsesforordningen, 2016) artikel 28, stk. 3, litra a og (Nielsen & Lotterup, 2020), side 612
[133] (Databeskyttelsesforordningen, 2016) artikel 28, stk. 10
[134] (Databeskyttelsesforordningen, 2016), artikel 32, stk. 1, litra a

behandleren.[135] Slutteligt skal den dataansvarlige føre tilsyn med dennes databehandlere for at kunne dokumentere, at databeskyttelsesforordningen overholdes.[136]

8. Tredjelandsoverførsler

Nærværende kapitel vil først og fremmest klarlægge de centrale begreber databeskyttelses-forordningens kapitel V. Herefter vil kapitlet fastlægge databeskyttelsesforordningens krav i forbindelse med tredjelandsoverførsler.

8.1. Centrale begreber

Databeskyttelsesforordningens kapitel V regulerer overførsler af personoplysninger til tredjelande eller internationale organisationer.

Der skal først og fremmest være tale om en *overførsel*. Der findes ingen legaldefinition af begrebet *overførsel* i databeskyttelsesforordningen. Overførselsbegrebet er en samlet betegnelse for henholdsvis videregivelse til tredjemand, overladelse og intern anvendelse.[137] EDPB anfører i deres retningslinjer, at der er tre kumulative krav, som skal være opfyldt førend der er tale om en overførsel og det er følgende: at 1) den dataansvarlige eller databehandleren, som benævnes *eksportør*, foretager en behandling som er omfattet af databeskyttelses-forordningen, 2) *eksportøren* videregiver personoplysninger, eller på en anden måde stiller personoplysninger til rådighed for en anden dataansvarlig, databehandler eller fælles dataansvarlig, som benævnet *importør* og 3) *importøren* befinder sig i et tredjeland, og dette gælder uanset om *importørens* behandling af personoplysningerne er omfattet af databeskyttelsesforordningen.[138]

Begrebet *tredjeland* er ikke defineret i databeskyttelsesforordningen, men det er defineret i litteraturen ved en negativ afgrænsning, således det er alle andre lande end EU/EØS-lande.[139]

[135] (Databeskyttelsesforordningen, 2016), artikel 28, stk.4
[136] (Databeskyttelsesforordningen, 2016) artikel 5, stk. 2
[137] (Udsen, 2022), side 334
[138] (EDPB's Retningslinjer 05/2021, 2023), side 7 og (Udsen, 2022), side 332
[139] (Udsen, 2022), side 342

8.2 Artikel 44

Databeskyttelsesforordningens art. 44 fastlægger det generelle princip for overførsel til tredjelande. Princippet i databeskyttelsesforordningens art. 44 fastslår, at både betingelserne i kapitel V skal overholdes samt de øvrige bestemmelser indeholdt i databeskyttelses-forordningen, herunder at der er behandlingsgrundlag i databeskyttelsesforordningens art. 6 og eventuelt art. 9.[140] Databeskyttelsesforordningens art. 45-49 er en udtømmende og prioriteret liste over overførselsgrundlag til modtagere der er placeret uden for EU/EØS.[141]

8.3 Artikel 45

Databeskyttelsesforordningens art. 45 omhandler overførsler baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet. Det er kun EU-Kommissionen, som med bindende virkning kan beslutte, hvorvidt et tredjeland har et tilstrækkeligt beskyttelsesniveau.

Beskyttelsesniveauet vil anses som tilstrækkeligt, når det i det væsentligste svarer til det niveau, som der er sikret i EU/EØS som følger af databeskyttelsesforordningen.[142] Såfremt EU-Kommissionen vurderer, at tredjelandet har et tilstrækkeligt beskyttelsesniveau, kan EU-Kommissionen fastslå, at tredjelandet er et såkaldt *sikkert tredjeland.*[143] EU-Kommissionen kan godkende et område i et tredjeland, en eller flere specifikke sektorer i et tredjeland eller hele tredjelandet. I skrivende stund har EU-Kommissionen godkendt, at der kan overføres til USA, såfremt modtageren er certificeret under Data Privacy Framework.[144] Såfremt der ikke er en tilstrækkelighedsafgørelse, kan der ske overførsel til et tredjeland, i henhold til databeskyttelsesforordningens art. 46 eller art. 49.[145]

8.4 Artikel 46

Såfremt EU-Kommissionen ikke har vedtaget en tilstrækkelighedsafgørelse, kræver det fornødne garantier før der kan ske overførsel til tredjelandet.[146] Disse garantier kompenserer

[140] (Nielsen & Lotterup, 2020), side 773 og 774 og (Databeskyttelsesforordningen, 2016) præambelbetragtning nr. 101 og (Motzfeldt, 2022), side 264
[141] (Nielsen & Lotterup, 2020), side 774
[142] (Schrems I C-362/14, 2015), præmis 73, (Udsen, 2022), side 342, (Nielsen & Lotterup, 2020), side 782 og (Databeskyttelsesforordningen, 2016) præambelbetragtning nr. 104
[143] (Databeskyttelsesforordningen, 2016), artikel 45, stk. 3
[144] (Datatilsynets Vejledning, 2024), side 14
[145] (Datatilsynets Vejledning, 2024), side 16 og 27
[146] (Databeskyttelsesforordningen, 2016), artikel 46

for den manglende beskyttelse af personoplysninger.[147] Foruden kravet om fornødne garantier, er det også et krav, at de registreredes rettigheder kan håndhæves og der er effektive retsmidler for den registrerede. Det er både den dataansvarlige og databehandleren som skal sikre fornødne garantier ved overførsel af personoplysninger til et tredjeland.[148] I henhold til databeskyttelsesforordningens art. 46, stk. 2, litra c, kan der ske overførsel til et tredjeland på grundlag af EU-kommissionens standardbestemmelser.

8.5 Artikel 48

Af databeskyttelsesforordningens art. 48 fremgår det, at enhver dom og afgørelse truffet af myndigheder og domstole i tredjelandet, kan anerkendes og håndhæves, såfremt de bygger på en international aftale mellem tredjelandet og landet i EU/EØS. En international aftale kan være en traktat om gensidig retshjælp. Domme og afgørelser truffet af myndigheder og domstole i tredjelandet kan ikke stå alene, hvorfor der ikke kan overføres på baggrund heraf medmindre der også er en international aftale. Såfremt der er en international aftale, kan personoplysningerne udleveres gennem traktaterne, hvor de tiltrådte parter er forpligtet til at hjælpe hinanden.[149]

8.6 Artikel 49

I henhold til databeskyttelsesforordningens art. 49 kan der overføres personoplysninger til tredjelande i de situationer, hvor hverken databeskyttelsesforordningens art. 45 og 46 kan udgøre et overførselsgrundlag.[150] Databeskyttelsesforordningens art. 49 kræver ikke et tilstrækkeligt beskyttelsesniveau, som nævnt i art. 45 og 46, og karakteriseres derfor som en undtagelsesbestemmelse.[151] I henhold databeskyttelsesforordningens art. 49, stk. 1 kan der overføres personoplysninger, hvis overførslen er omfattet af én af de oplistede betingelser som fremgår af litra a-g. Specialet har som benævnt afgrænset sig til databeskyttelsesforordningens art. 49, stk. 1, litra d, e og f, idet disse er relevante for besvarelsen af problemformuleringen.

I henhold til databeskyttelsesforordningens art. 49, stk. 1, litra d, kan en overførsel finde sted, hvis den er nødvendig af hensyn til vigtige samfundsinteresser. Disse samfundsinteresser skal

[147] (Databeskyttelsesforordningen, 2016) præambelbetragtning nr. 108
[148] (Nielsen & Lotterup, 2020), side 791, (Databeskyttelsesforordningen, 2016) præambelbetragtning nr. 108 og 114 og (Databeskyttelsesforordningen, 2016) artikel 46, stk. 1
[149] (Udsen, 2022), side 375 samt (Nielsen & Lotterup, 2020), side 805 og 806
[150] (Motzfeldt, 2022), side 279
[151] (Udsen, 2022), side 370

være anerkendt af EU-retten eller medlemsstaternes nationale ret, som den europæiske dataansvarlige er underlagt.[152]

Endvidere følger det af databeskyttelsesforordningens art. 49, stk. 1, litra e, at der kan ske overførsel til et tredjeland i medfør af denne bestemmelse, såfremt overførslen er nødvendig for at et retskrav kan fastlægges, gøres gældende eller forsvares. Endvidere skal overførslen kun forekomme lejlighedsvist.[153]

Derudover følger det af databeskyttelsesforordningens art. 49, stk. 1, litra f, at der kan ske overførsel, såfremt overførslen er nødvendig for at beskytte den registreredes eller andre personers vitale interesse i det tilfælde, hvor den registrerede ikke selv er i stand til at give samtykke.[154]

Såfremt undtagelserne i særlige situationer nævnt i databeskyttelsesforordningens art. 49, stk. 1, litra a-g ikke kan benyttes som overførselsgrundlag, indeholder art. 49, stk. 1, 2. pkt. en interesseafvejningsregel. En overførsel til et tredjeland i henhold til interesseafvejningsreglen kræver at overførslen ikke gentages, og at overførslen kun må vedrøre et begrænset antal registrerede. Desuden skal overførslen være nødvendig af hensyn til vægtige legitime interesser. De registreredes interesser og rettigheder må ikke vægte tungere end interessen for at overføre. Vurderingen af disse interesser skal inddrage alle faktiske omstændigheder, således at der kan stilles passende garantier for de registrerede.[155]

9. Cloudleverandører med underdatabehandlere i USA

I dette kapitel vil specialet analysere den problematiske lovgivning i USA gennem Schrems I og II. Herefter belyses den nuværende tilstrækkelighedsafgørelse, Data Privacy Framework, som giver hjemmel til overførsel til USA. Desuden vil en analyse af Chromebook-sagen belyse problematikken ved at benytte en cloudleverandør med underdatabehandlere i USA. Slutteligt vil specialet på baggrund af analysen besvare problemformuleringens andet underspørgsmål angående, hvordan den dataansvarlige sikrer, at behandlingen af personoplysninger sker i

[152] (Databeskyttelsesforordningen, 2016) artikel 49, stk. 1, litra d og artikel 49 stk. 4 og (Udsen, 2022), side 372
[153] (Databeskyttelsesforordningen, 2016) præambelbetragtning nr. 111
[154] (Databeskyttelsesforordningen, 2016) art. 49, stk. 1, litra f og præambelbetragtning nr. 112
[155] (Motzfeldt, 2022), side 280, (Databeskyttelsesforordningen, 2016) artikel 49, stk. 1, 2. pkt. og præambelbetragtning nr. 113

overensstemmelse med databeskyttelsesforordningen, når der anvendes en cloudleveandør med underdatabehandlere i USA.

9.1 Overførselsgrundlag til USA - historik

De amerikanske cloudleverandører har selskaber placeret i EU/EØS, men deres moderselskab er beliggende i USA. Som følge heraf kan der forekomme overførsler af personoplysninger fra EU/EØS til USA. Igennem tiden har EU/EØS og USA indgået forskellige certificeringsordninger for at sikre et tilstrækkeligt beskyttelsesniveau. Nedenfor vil Safe Harbor og Privacy Shield blive belyst gennem Schrems I og II. I den henseende har specialet fokus på den problematiske lovgivning, som har medført at certificeringsordningerne er blevet erklæret ugyldig. Slutteligt vil den nye certificeringsordning, Data Privacy Framework, blive belyst.

9.1.1 Safe Harbor

I år 2000 traf EU-Kommissionen beslutningen om, at certificeringsordningen kaldet Safe Harbor, sikrede et tilstrækkeligt beskyttelsesniveau i forhold til de dagældende regler om databeskyttelse.[156] Safe Harbor var en certificeringsordning, som amerikanske virksomheder havde mulighed for at tilslutte sig, hvis de ønskede, at der skulle ske overførsel af personoplysninger fra EU/EØS til USA. Ved at tilslutte sig Safe Harbor forpligtede de amerikanske virksomheder sig til at efterleve nogle principper til behandling af personoplysningerne, og på den måde opnåede de et tilstrækkeligt beskyttelsesniveau.[157] Safe Harbor blev af EU-domstolen erklæret ugyldig i den 6. oktober 2015 i Schrems I, jf. nærmere herom i nedenstående afsnit.[158]

9.1.2 Schrems I

Sagen udsprang af en klage fra Maximilian Schrems, en østrigsk statsborger, som benyttede Facebook. Ved anvendelse af Facebook skulle der indgås en aftale med Facebook Irland, der er datterselskab af Facebook Inc., som er beliggende i USA. Det betød, at Facebook-brugernes personoplysninger blev overført til USA, hvor der skete behandling af personoplysningerne. Facebook benyttede Safe Harbor som overførselshjemmel til USA. Maximillian Schrems besluttede derfor at klage til det irske datatilsyn, idet han hævdede, at USA ikke sikrede

[156] (Europa-Parlamentet og Rådets direktiv 95/46/EF, 1995), artikel 25, stk. 1 (nu forordningens art. 45), (Nielsen & Lotterup, 2020), side 775-776 og (Kommissionens beslutning af 26. juli 2000, 2000)
[157] (Kommissionens beslutning af 26. juli 2000, 2000) og (Udsen, 2022), side 344
[158] (Nielsen & Lotterup, 2020), side 775

tilstrækkelig beskyttelse af personoplysninger - herunder ikke tilstrækkelig sikkerhed mod de offentlige myndigheders overvågning set i lyset af Edward Snowdens afsløringer.[159]

> I år 2013 afslørede Edward Snowden NSA's globale masseovervågning samt teknikker til overvågning, henholdsvis PRISM og Upstream. Endvidere blev det afsløret, at NSA overvågede uden en dommerkendelse, og overvågningen kunne ske uden der nødvendigvis var en mistanke om en specifik kriminel handling.

9.1.2.1 Spørgsmålet om gyldigheden af tilstrækkelighedsafgørelsen

EU-domstolen behandler spørgsmålet om, hvorvidt tilstrækkelighedsafgørelsen vedrørende Safe Habour er gyldig. Det anføres først og fremmest, at databeskyttelsesdirektivet forbyder overførsel til tredjelande, såfremt tredjelandet ikke har et tilstrækkeligt beskyttelsesniveau.[160] Databeskyttelsesdirektivet fastslog ikke en definition af et *tilstrækkeligt* beskyttelsesniveau, men fastsatte vurdering af beskyttelsesniveauet skulle ske på grundlag af samtlige forhold, som har indvirkning på videregivelsen.[161] Endvidere skal vurderingen foretages på grundlag af den nationale lovgivning og internationale forpligtelser med henblik på at vurdere, hvorvidt denne lovgivning beskytter de grundlæggende rettigheder samt frihedsrettigheder.[162] General-advokaten har i forslaget til afgørelsen fremsat følgende angående kravet om et tilstrækkelig beskyttelsesniveau: [163]

"[...]et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, på grundlag af artikel 25, stk. 6, i direktiv 95/46, hvis den efter en helhedsvurdering af gældende ret og praksis i det pågældende tredjeland kan fastslå, at dette tredjeland sikrer et beskyttelsesniveau, som i alt væsentligt svarer til det, der sikres ved dette direktiv, selv om de nærmere vilkår for denne beskyttelse kan adskille sig fra dem, der normalt gælder inden for EU."

EU-domstolen tilslutter sig generaladvokatens holdning i forslaget og fastslår, at kravet om *tilstrækkeligt* beskyttelsesniveau ikke er et krav om et identisk niveau af beskyttelse som i

[159] (Udsen, 2022), side 344 og (Schrems I C-362/14, 2015), præmis 26-28, (noyb, Data Transfers) og (Allingstrup, 2016), *"Snowdens kæmpelæk: Afslørede USA's massive overvågning"*
[160] (Schrems I C-362/14, 2015), præmis 68
[161] (Europa-Parlamentet og Rådets direktiv 95/46/EF, 1995) artikel 25, stk. 2, og (Schrems I C-362/14, 2015) præmis 70
[162] (Europa-Parlamentet og Rådets direktiv 95/46/EF, 1995) artikel 25, stk. 6 og (Schrems I C-362/14, 2015) præmis 70 og 71
[163] (Generaladvokat, Y. Bot, 2015), punkt 141

EU/EØS, men derimod blot et niveau, som i det *væsentlige* svarer til niveauet i EU/EØS. Det betyder, at der er et krav om, at tredjelandets nationale lovgivning eller internationale forpligtelser sikrer, at personernes grundlæggende rettigheder og frihedsrettigheder er beskyttet på et niveau, der svarer til beskyttelsesniveauet i EU/EØS i medfør af databeskyttelses-direktivet og chartret. Dette krav sikrer, at der ikke sker omgåelse ved at overføre personoplysningerne til tredjelande.[164] Det er et krav, at EU-Kommissionen skal undersøge indholdet af reglerne i tredjelandet samt vurdere, hvorvidt tredjelandets lovgivning også i praksis er effektiv i forhold til beskyttelse af personoplysninger. Undersøgelse af beskyttelsesniveauet skal ske med regelmæssigt mellemrum for at sikre at beskyttelsesniveauet stadig er tilstrækkeligt, og særligt når der opstår tvivl i forhold til beskyttelsesniveauets tilstrækkelighed.[165]

EU-Domstolen anfører herefter, at anvendelsen af en certificeringsordning ikke i sig selv er i strid med kravene i databeskyttelsesdirektivet, men at pålideligheden til certificerings-ordningen afhænger af tilstedeværelsen af effektive kontrolmekanismer.[166] Principperne i Safe Harbor skulle kun efterleves af de certificerede virksomheder, og de amerikanske myndigheder skulle dermed ikke efterleve dem.[167] Af beslutning 2000/520 er der anført en begrænsning i forhold til efterlevelse af principperne i Safe Harbor af hensyn til den amerikanske stats-sikkerhed. Denne begrænsning gælder navnlig, når amerikanske love, andre administrative bestemmelser eller retspraksis tilsiger, at udlevering af personoplysninger er nødvendige af legitime grunde. Endvidere fremgår det af beslutningen, at uanset om de amerikanske virksomheder har tilsluttet sig Safe Harbor, skal de overholde den amerikanske lovgivning i tilfælde af modstridende forpligtelser.[168] EU-domstolen fastslår i den henseende, at det betyder, at amerikansk lovgivning har forrang for principperne i Safe Harbor.[169] Be-grænsningen i beslutningen angående efterlevelse af kravene til statens sikkerhed eller efterlevelse af amerikansk lovgivning, kan give anledning til, at der sker et indgreb i de grundlæggende rettigheder for de personer, der får videregivet sine personoplysninger til

[164] (Schrems I C-362/14, 2015), præmis 73 og 74
[165] (Schrems I C-362/14, 2015), præmis 75 og 76
[166] (Schrems I C-362/14, 2015), præmis 81
[167] (Schrems I C-362/14, 2015), præmis 82
[168] (Kommissionens beslutning af 26. juli 2000, 2000), afsnit B i bilag IV og (Schrems I C-362/14, 2015), præmis 84 og 85
[169] (Schrems I C-362/14, 2015), præmis 86

USA.[170] Beslutningen fastlægger ikke, hvorvidt reglerne af statslig karakter i USA sikrer en begrænsning i forhold til indgreb i de grundlæggende rettigheder og fastlægger heller ikke, hvilke indgreb de statslige myndigheder må foretage, når de ønsker at forfølge legitime mål. Derudover fremgår det heller ikke, hvorvidt der er en effektiv domstolsbeskyttelse for så vidt angår indgreb fra de statslige myndigheder.[171]

EU-Kommissionen har tillige forholdt sig til Safe Harbors svagheder efter Edward Snowdens afsløringer og udtrykt sin bekymring i deres meddelelse.[172] Heri anfører EU-Kommissionen, at det er en bekymring, at det ikke er alle de certificerede virksomheder, der i praksis overholder de anførte principper i Safe Harbor. Dette medfører konsekvenser for EU-borgernes rettigheder samtidig med, at virksomhederne i EU/EØS og de amerikanske virksomheder som overholder principperne, er ringere stillet end de amerikanske virksomheder, som ikke overholder principperne. EU-Kommissionen betvivler, hvorvidt den omfattende indsamling af personoplysninger, som de amerikanske myndigheder foretager, har et rimeligt omfang og hvorvidt det er nødvendigt, idet myndighederne kan behandle personoplysninger udover det strengt nødvendige.[173]

EU-Domstolen pointerer, at såfremt en lovgivning medfører indgreb i de grundlæggende rettigheder[174], skal rækkevidden heraf være klart og præcist fastlagt.[175] Desuden skal en begrænsning fra reglerne om beskyttelsen af personoplysninger holdes til det strengt nødvendige.[176] Da de amerikanske myndigheders adgang til personoplysninger ikke afgrænses, holdes det således ikke til det strengt nødvendige.[177] Endvidere anses det som et indgreb i retten til privatliv, når en lovgivning giver generel adgang til elektronisk kommunikation.[178] Desuden opfylder den amerikanske lovgivning ikke chartrets art. 47, idet lovgivningen ikke giver adgang til effektive retsmidler.[179]

[170] (Schrems I C-362/14, 2015), præmis 87
[171] (Schrems I C-362/14, 2015), præmis 88 og 89
[172] (MEDDELELSE FRA KOMMISSIONEN, 2013)
[173] (MEDDELELSE FRA KOMMISSIONEN, 2013), punkt 2, 3.2 og 4 og (Schrems I C-362/14, 2015), præmis 15
[174] (Den Europæiske Unions charter , 2009), artikel 7 og 8
[175] (Den Europæiske Unions charter , 2009), artikel 52, stk. 1
[176] (Schrems I C-362/14, 2015), præmis 91 og 92
[177] (Schrems I C-362/14, 2015), præmis 93
[178] (Den Europæiske Unions charter , 2009), artikel 7
[179] (Schrems I C-362/14, 2015), præmis 94 og 95

EU-domstolen konstaterer slutteligt, at EU-Kommissionen i sin beslutning ikke har anført, hvorvidt USA sikrer et tilstrækkeligt beskyttelsesniveau på grundlag af den amerikanske lovgivning eller internationale forpligtelser. EU-domstolen kunne således erklære Safe Harbor for ugyldig uden at vurdere indholdet af principperne i Safe Harbor.[180]

9.1.3 Privacy Shield

Den 12. juli 2016 kom der en erstatning for Safe Harbor, idet EU-kommissionen traf beslutningen om, at Privacy Shield sikrede et tilstrækkeligt beskyttelsesniveau.[181] Privacy Shield var ligesom Safe Harbor også en certificeringsordning. I forbindelse med EU-Kommissionens vedtagelse af Privacy Shield undersøgte de begrænsningerne og garantierne i henhold til amerikansk ret vedrørende de amerikanske myndigheders adgang til og brug af personoplysninger fra EU/EØS. Privacy Shield forsøgte at afdække manglerne i Safe Harbor ved, at den amerikanske regering i forbindelse med Privacy Shield implementeret en ny tilsynsmekanisme, ombudsmanden, hvis rolle var at fungere som et uafhængigt tilsynsorgan, hvilket var en mangel ved Safe Harbor.[182]

9.1.3.1 Schrems II

Maximilian Schrems indgav en ny klage den 1. december 2015 til det irske datatilsyn, hvori han anførte, at Facebook Inc. i USA i henhold til amerikansk ret skal stille personoplysninger til rådighed for amerikanske myndigheder. Endvidere påpegede Maximilian Schrems, at personoplysningerne blev benyttet til forskellige overvågningsprogrammer, som var i strid med strid med chartrets art. 7, 8 og 47, og brugen af standardbestemmelser kunne ikke begrunde overførslerne til USA.[183]

Det irske datatilsyn opfattede Maximilian Schrems klage som et spørgsmål om gyldigheden af standardbestemmelserne, og det irske datatilsyn indbragte derfor sagen for High Court med henblik på, at spørgsmålet skulle forelægges EU-Domstolen. High Court forelagde herefter spørgsmålet for EU-Domstolen.[184]

[180] (Schrems I C-362/14, 2015), præmis 98 og 107
[181] (KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2016, 2016)
[182] (Schrems II C-311/18, 2020), præmis 43
[183] (Schrems II C-311/18, 2020), præmis 55
[184] (Schrems II C-311/18, 2020), præmis 57

EU-domstolen blev forelagt 11 præjudicielle spørgsmål, og finder det også relevant at undersøge gyldigheden af Privacy Shield.[185] Specialet har udvalgt de spørgsmål som bidrager til forståelsen af problematikken med den amerikanske lovgivning.

Først og fremmest konstaterer EU-domstolen, at i det tilfælde, hvor tredjelandets myndigheder under eller efter overførslen behandler personoplysningerne af hensyn til den offentlige sikkerhed, forsvaret og statens sikkerhed, vil det være omfattet af databeskyttelses-forordningens anvendelsesområde.[186]

9.1.3.2 Spørgsmål angående tilstrækkeligt beskyttelsesniveau

EU-Domstolen forholder sig til, hvilket beskyttelsesniveau der er krævet ved overførsel til tredjelande i medfør af standardbestemmelserne. Derudover bedes EU-Domstolen om præcision af, hvilke elementer der skal overvejes i forbindelse med en afgørelse om tilstrækkeligt beskyttelsesniveau i et tredjeland.[187]

Indledningsvist fastslår EU-Domstolen, at såfremt der ikke er vedtaget en tilstrækkelighedsafgørelse, må der kun overføres til tredjelande med hjemmel i databeskyttelsesforordningens art. 46, såfremt betingelser stk. 1 er opfyldt.[188] Hertil bemærker EU-Domstolen, at databeskyttelsesforordningens art. 46 er anført i forordningens kapitel V og skal således ses i lyset af databeskyttelsesforordningens art. 44, som er det generelle princip, der sikrer overholdelse af kapitel V og resten af forordningen for at sikre et tilstrækkeligt beskyttelsesniveau.[189]

I henhold til databeskyttelsesforordningens art. 45 kan der ske overførsel til et tredjeland, såfremt EU-Kommissionen har truffet en afgørelse om tilstrækkeligt beskyttelsesniveau. Som tidligere anført i Schrems I, vil det være et *tilstrækkeligt* beskyttelsesniveau, når tredjelandets lovgivning i det *væsentlige* svarer til niveauet af beskyttelse i EU/EØS. Beskyttelsesniveauet behøver således ikke at være identisk med beskyttelsen i EU/EØS.[190] I den henseende påpeger

[185] (Schrems II C-311/18, 2020), præmis 68 og 151
[186] (Schrems II C-311/18, 2020), præmis 86 og 89
[187] (Schrems II C-311/18, 2020), præmis 68 og 90
[188] (Schrems II C-311/18, 2020), præmis 91
[189] (Schrems II C-311/18, 2020), præmis 92
[190] (Schrems I C-362/14, 2015), præmis 73 og (Schrems II C-311/18, 2020), præmis 94

EU-Domstolen, at det fremgår af præambelbetragtning 107, at overførsel til tredjelandet bør forbydes, hvis der ikke er et tilstrækkeligt beskyttelsesniveau medmindre kravene i databeskyttelsesforordningen art. 46 eller art. 49 er opfyldt. Endvidere fremgår det af præambelbetragtning 108, at hvis der ikke foreligger en tilstrækkelighedsafgørelse, skal den dataansvarlige eller databehandleren *"kompensere for den manglende databeskyttelse i et tredjeland"*[191] ved at træffe passende foranstaltninger, herunder fornødne garantier, for at sikre overholdelse af forordningen og dermed sikrer et beskyttelsesniveau, som i det væsentlige svarer til det i EU/EØS.[192]

Dernæst undersøger EU-Domstolen spørgsmålet om, hvilke elementer der skal overvejes i forbindelse med en afgørelse om tilstrækkeligt beskyttelsesniveau i et tredjeland. Her nævner EU-Domstolen, at databeskyttelsesforordningens art. 46 ikke oplister de elementer, der skal tages i betragtning. Dog er det specificeret i bestemmelsens stk. 1, at der skal være *fornødne garantier, rettigheder, som kan håndhæves* og *effektive retsmidler*.[193] EU-Domstolen påpeger, at kontraktvilkår mellem den dataansvarlige eller databehandleren i EU/EØS og modtageren i tredjelandet skal tages i betragtning. I forbindelse med vurderingen af et tilstrækkeligt beskyttelsesniveau i et tredjeland skal det undersøges, hvorvidt tredjelandets myndigheder kan få adgang til personoplysninger.[194]

Opsummerende kan det udledes, at i de tilfælde, hvor EU-Kommissionen ikke har truffet en tilstrækkelighedsafgørelse, kan der overføres på baggrund af databeskyttelsesforordningens art. 46, som skal ses i lyset af databeskyttelsesforordningens art. 44. Herudover kan det udledes, at databeskyttelsesforordningens art. 46 stk. 1 stiller krav om, at der skal være *fornødne garantier, rettigheder, som kan håndhæves* og *effektive retsmidler*, men at disse elementer ikke er uddybet i databeskyttelsesforordningen. Dog fastslår EU-Domstolen, at kontraktsvilkår samt tredjelandets lovgivning skal tages i betragtning, når beskyttelsesniveauet skal vurderes.[195]

[191] (Databeskyttelsesforordningen, 2016) præambelbetragtning 108
[192] (Schrems II C-311/18, 2020), præmis 95 og 96
[193] (Schrems II C-311/18, 2020), præmis 103
[194] (Schrems II C-311/18, 2020), præmis 104
[195] (Schrems II C-311/18, 2020), præmis 104

9.1.3.3 Spørgsmål angående gyldigheden af standardbestemmelserne

EU-Domstolen tager stilling til gyldigheden af standardbestemmelserne sammenholdt med chartret art. 7, 8 og 47.[196] Årsagen til det præjudicielle spørgsmål var, at der var opstået en tvivl angående beskyttelsesniveauet ved overførsel af personoplysninger til tredjelande på baggrund af standardbestemmelser, idet disse ikke er bindende for tredjelandets myndigheder.[197] Det er kun parterne i kontrakten, som er bundet af disse standardbestemmelser, navnlig afsenderen i EU/EØS og modtageren i tredjelandet.[198] EU-Domstolen fastslår, at der var en problemstilling i det tilfælde, hvor tredjelandets lovgivning muliggør, at tredjelandets myndigheder kan få adgang til personoplysningerne.[199] EU-Domstolen skulle derfor tage stilling til, hvorvidt EU-Kommissionens afgørelse om standardbestemmelser var ugyldig, eftersom de kun var gældende for kontraktparterne, og derfor ikke indeholdte garantier i forhold til de offentlige myndigheder.[200]

EU-Domstolen anfører, at såfremt der er ikke er truffet en tilstrækkelighedsafgørelse, kan der kun ske overførsel til tredjelandet, hvis 1) der er stillet de fornødne garantier, 2) de registreredes rettigheder kan håndhæves og 3) der er effektive retsmidler.[201] De fornødne garantier kan i henhold til databeskyttelsesforordningens art. 46, stk. 2, litra c, sikres gennem EU-Kommissionens standardbestemmelser.[202] EU-Kommission har ikke en pligt til at undersøge trejdelandets lovgivning, når EU-Kommissionen træffer en afgørelse om standard-bestemmelser. Dette skyldes, at standardbestemmelserne ikke er møntet på et specifikt tredjeland, område eller sektorer og kan anvendes generelt.[203] Som nævnt fastslår EU-Domstolen, at standardbestemmelserne ikke binder tredjelandets myndigheder, og derfor kan det være nødvendigt at supplere garantierne i standardbestemmelserne. I den forbindelse anfører EU-Domstolen, at den dataansvarlige har mulighed for at supplere med yderligere garantier.[204] På den måde opretholdes et tilstrækkeligt beskyttelsesniveau.[205] EU-Domstolen

[196] (Schrems II C-311/18, 2020), præmis 122
[197] (Schrems II C-311/18, 2020), præmis 123
[198] (Schrems II C-311/18, 2020), præmis 125
[199] (Schrems II C-311/18, 2020), præmis 126
[200] (Schrems II C-311/18, 2020), præmis 127
[201] (Schrems II C-311/18, 2020), præmis 131 og (Databeskyttelsesforordningen, 2016), præambelbetragtning nr. 108 og 114
[202] (Schrems II C-311/18, 2020), præmis 128
[203] (Schrems II C-311/18, 2020), præmis 130
[204] (Databeskyttelsesforordningen, 2016), præambelbetragtning nr. 109
[205] (Schrems II C-311/18, 2020), præmis 132 og 133

fastslår, at ansvaret påhviler den dataansvarlige eller dennes databehandlere, og hvis nødvendigt rådfører sig med modtageren i tredjelandet. Det betyder, at den dataansvarlige eller dennes databehandlere skal undersøge, hvorvidt tredjelandets lovgivning sikrer tilstrækkelig beskyttelse og give yderligere garantier ved behov.[206] Hvis det ikke er muligt at give yderligere garantier, skal den dataansvarlige eller dennes databehandlere eller tilsynsmyndigheden suspendere eller indstille overførslen af personoplysninger. Dette vil være tilfældet, såfremt lovgivningen i tredjelandet tillader de offentlige myndigheder at få adgang til personoplysningerne.[207] Hertil bemærker EU-Domstolen, at selvom standardbestemmelserne ikke er bindende for myndighederne i tredjelandet, vil dette ikke alene have indvirkning på afgørelsens gyldighed.[208] Gyldigheden er derimod betinget af, hvorvidt afgørelsen efterlever databeskyttelsesforordningens art. 46, stk. 1 og art. 46, stk. 2, litra c sammenholdt med chartret art. 7, 8 og 47, samt at overførslen til tredjelandet suspenderes eller forbydes, hvis bestemmelserne ikke kan overholdes.[209]

I henhold til standardbestemmelserne udarbejdet af EU-Kommissionen skal den dataansvarlige i EU/EØS og modtageren i tredjelandet gensidigt forpligte sig til, at personoplysningerne behandles i overensstemmelse med databeskyttelsesforordningen.[210] Såfremt modtageren i tredjelandet ikke kan efterleve sine forpligtelser, skal den dataansvarlige i EU/EØS underrettes herom, uagtet tredjelandets lovgivning forbyder underretningen grundet fortrolighed ved efterretningsaktiviteter. Desuden skal modtageren i tredjelandet bekræfte, at der ikke er grund til at tro, at tredjelandets lovgivning vil være en hindring i forhold til at efterleve kontraktens forpligtelser.[211] Såfremt modtageren i tredjelandet ikke overholder sine forpligtelser, skal den dataansvarlige i EU/EØS suspendere overførslen og/eller ophæve kontrakten for at overholde kravene fastsat i standardbestemmelserne.[212] EU-Domstolen bemærker, at den dataansvarlige i EU/EØS og modtageren i tredjelandet inden overførslen har en forpligtelse til at undersøge, hvorvidt tredjelandets lovgivning muliggør modtagerens overholdelse af kontrakten. Såfremt

[206] (Schrems II C-311/18, 2020), præmis 134
[207] (Schrems II C-311/18, 2020), præmis 135
[208] (Schrems II C-311/18, 2020), præmis 136
[209] (Schrems II C-311/18, 2020), præmis 137
[210] (Schrems II C-311/18, 2020), præmis 138
[211] (Schrems II C-311/18, 2020), præmis 139
[212] (Schrems II C-311/18, 2020), præmis 140 og 142

lovgivningen i tredjelandet ikke er mere omfattende end nødvendigt for at sikre statens sikkerhed, forsvaret og offentlig sikkerhed, vil det ikke i strid med standardbestemmelserne.[213]

EU-domstolen konkluderede derfor, at gyldigheden af afgørelse om standardbestemmelser ikke er påvirket af, at standardbestemmelser kun er bindende for kontraktparterne, og ikke de offentlige myndigheder i tredjelandet, så længe tredjelandets lovgivning er proportionel i forhold til formålet med at sikre staten mv.[214]

9.1.3.4 Spørgsmål angående gyldigheden af Privacy Shield

Maximillian Schrems havde klaget over overførslen af personoplysninger til USA med påstanden om manglende tilstrækkeligt beskyttelsesniveau.[215] Men idet Privacy Shield blev vedtaget efterfølgende, fortolkes spørgsmålene til EU-Domstolen således, at der blev rejst tvivl om Privacy Shields gyldighed.[216]

Indholdet af afgørelsen om Privacy Shield

EU-Domstolen gennemgår først tilstrækkelighedsafgørelsens indhold. Her anføres, at EU-Kommissionen har vurderet, at Privacy Shield sikrer et tilstrækkeligt beskyttelsesniveau. Privacy Shield består af en række principper,[217] men EU-Domstolen pointerer herefter, at den modtagende virksomhed i USA i visse tilfælde skal tilsidesætte principperne i Privacy Shield, hvis det er i strid med amerikansk lovgivning, som sikrer den nationale sikkerhed, den offentlige interesse eller retshåndhævelsen. Dermed understreger EU-domstolen ligesom i Schrems I, at amerikansk lovgivning har forrang.[218] Denne tilsidesættelse af principperne i Privacy Shield muliggør, at de amerikanske myndigheder kan få adgang til personoplysninger overført fra EU/EØS til en modtager i USA, hvis det sker af hensyn til national sikkerhed, offentlig interesse eller amerikansk retshåndhævelse. Denne adgang kan de amerikanske myndigheder få via. FISA 702 samt E.O. 12333, jf. nærmere herom i nedenstående afsnit.[219]

[213] (Schrems II C-311/18, 2020), præmis 141
[214] (Schrems II C-311/18, 2020), præmis 149 og (Den Europæiske Unions charter , 2009), artikel 52, stk.1
[215] (Schrems II C-311/18, 2020), præmis 159
[216] (Schrems II C-311/18, 2020), præmis 160-161
[217] (Schrems II C-311/18, 2020), præmis 163
[218] (Schrems II C-311/18, 2020), præmis 164
[219] (Schrems II C-311/18, 2020), præmis 165 og 166

Konstateringen vedrørende tilstrækkeligheden af beskyttelsesniveauet

EU-Domstolen stiller spørgsmålstegn ved, hvorvidt amerikansk ret har et tilstrækkeligt beskyttelsesniveau set i lyset af chartrets art. 7, 8 og 47. EU-Domstolen finder ikke, at amerikansk lovgivning indeholder nødvendige begrænsninger og garantier for, at de europæiske borgere er sikret deres rettigheder, som fremgår af chartrets art. 7, 8 og 47. Det nye uafhængige tilsynsorgan i USA, ombudsmanden, som blev implementeret i forbindelse med Privacy Shield, finder EU-Domstolen ikke sammenlignelig med rettigheden i chartrets art. 47, som sikrer, at enhver har ret til en uafhængig og upartisk domstol.[220]

EU-domstolen fastslår, at det vil være et indgreb i de grundlæggende rettigheder, såfremt tredjelandets myndigheder får adgang til, opbevarer eller får videregivet personoplysninger.[221] Såfremt de grundlæggende rettigheder og frihedsrettighederne begrænses, skal dette fremgå af lovgivningen.[222] Endvidere kan begrænsninger kun anvendes, hvis de er nødvendige og svarer til det formål der er angivet i EU-retten.[223] EU-Domstolen pointerer herefter, at begrænsninger skal angives i lovgivningen, hvoraf rækkevidden og anvendelsen af begrænsningen defineres klart og præcist samt opstille mindstekrav, herunder betingelser for at begrænsningen kan finde sted. Dette skyldes, at de registrerede skal råde over tilstrækkelige garantier.[224]

Herefter stiller EU-Domstolen spørgsmålstegn ved EU-Kommissionens afgørelse om Privacy Shield, fordi EU-domstolen er i tvivl om, hvorvidt FISA 702 og EO 12333 er underlagt proportionalitetsprincippet.[225] EU-Domstolen tager først stilling til FISA 702. I den forbindelse konstaterer EU-Domstolen, at The United States Foreign Intelligence Surveillance Court (herefter "FISC") fører kontrol af overvågningsprogrammer i henhold til FISA 702 for at undersøge, hvorvidt disse er i overensstemmelse med formålet om at indhente oplysningerne til brug for efterretningsaktiviteter. Dog kontrollerer FISC ikke, om personoplysningerne er velegnede mål for indsamlingen.[226]

[220] (Schrems II C-311/18, 2020), præmis 168 og 190
[221] (Schrems II C-311/18, 2020), præmis 171
[222] (Den Europæiske Unions charter , 2009), artikel 52, stk. 1, 1. pkt.
[223] (Den Europæiske Unions charter , 2009) artikel 52, stk. 1, 2. pkt. og (Schrems II C-311/18, 2020), præmis 174
[224] (Schrems II C-311/18, 2020) præmis 175 og 176
[225] (Schrems II C-311/18, 2020), præmis 178 og (Den Europæiske Unions charter , 2009), artikel 52, stk. 1
[226] (Schrems II C-311/18, 2020), præmis 179

Herefter pointerer EU-Domstolen, at FISA 702 ikke indeholder begrænsninger for de amerikanske myndigheder til at gennemføre overvågning. Derudover indeholder FISA 702 ikke garantier for *non-US persons*.[227] FISA 702 fastsætter ikke rækkevidden af begrænsningen med klare og præcise regler, og FISA 702 er således ikke i overensstemmelse med proportionalitetsprincippet.[228]

EU-Kommissionen har konstateret, at ved overvågning i henhold til FISA 702 skal kravene i PPD-28 overholdes, og disse krav er de amerikanske myndigheder forpligtet til at overholde. Dog har den amerikanske regering imidlertid udtalt, at PPD-28 ikke giver de registrerede de rettigheder, som de er sikret i chartret, navnlig kan de registrerede ikke påberåbe deres rettigheder overfor de amerikanske myndigheder ved domstolene. EU-Domstolen fastslår på den baggrund, at PPD-28 ikke kan sikre et tilstrækkeligt beskyttelsesniveau.[229]

Udover FISA 702 undersøger EU-Domstolen ligeledes EO 12333 sammenholdt med PPD-28. I den forbindelse anfører EU-Domstolen, at E.O. 12333 er et præsidentielt dekret, som giver NSA mulighed for adgang til personoplysninger. Denne adgang vedrører personoplysninger *"der er i »transit« til USA, ved at tilgå de undersøiske kabler, der ligger på havbunden i Atlanterhavet."*[230] Når personoplysningerne er fremme i USA gælder FISA's bestemmelser, men med E.O. 12333 kan NSA indsamle personoplysninger allerede inden de er fremme i USA.[231] EU-Domstolen fastslår, at hverken FISA 702 og E.O. 12333 er begrænset til indgreb, der er strengt nødvendige og dermed ikke er i overensstemmelse med proportionalitets-princippet i chartret art. 52, stk. 1.[232]

Det fremgår af chartret art. 47, at hvis der sker krænkelse af rettigheder eller friheder, skal de registrerede have adgang til effektive retsmidler for en domstol.[233] EU-Domstolen pointerer, at *"selve eksistensen af en effektiv domstolsbeskyttelse, som skal sikre overholdelsen af de EU-retlige bestemmelser, uløseligt forbundet med eksistensen af en retsstat"*, og såfremt der ikke

[227] Ikke amerikanske personer
[228] (Schrems II C-311/18, 2020), præmis 180
[229] (Schrems II C-311/18, 2020), præmis 181
[230] (Schrems II C-311/18, 2020), præmis 63
[231] Ibid.
[232] (Schrems II C-311/18, 2020), præmis 184 og 185
[233] (Den Europæiske Unions charter , 2009), artikel 47 og (Schrems II C-311/18, 2020), præmis 186

er en effektiv domstolsbeskyttelse, vil det være i strid med chartrets art. 47.[234] EU-Domstolen rejser tvivl angående EU-Kommissionen vurdering af et tilstrækkeligt beskyttelsesniveau, idet ombudsmanden ikke kan afhjælpe manglerne i forhold til domstolsbeskyttelse, som var en af de problematikker, som blev rejst i Schrems I.[235] Ombudsmanden udgør ikke en uafhængig og upartisk domstol, idet ombudsmanden var en del af det amerikanske udenrigsministerium.[236] Endvidere var ombudsmanden ikke bemyndiget til at træffe bindende afgørelser vedrørende amerikanske efterretningstjenester.[237]

På baggrund af ovenstående erklærede EU-Domstolen, at Privacy Shield var ugyldig, fordi der ikke er sikret et *tilstrækkeligt* beskyttelsesniveau som krævet i henhold til databeskyttelses-forordningens art. 45, stk. 1 set i lyset af chartrets art. 7, 8 og 47.[238]

9.1.4 Overførsel til USA efter Schrems II

Efter Schrems II var der usikkerhed i forhold til brugen af amerikanske cloudleverandører, idet der ikke forelå en tilstrækkelighedsafgørelse. Personoplysningerne kunne således ikke overføres til USA i medfør af Privacy Shield, og derfor skulle de dataansvarlige i EU/EØS finde et andet overførselsgrundlag i databeskyttelsesforordningens kapitel V, indtil der kom en ny aftale på plads. I 2023 blev Data Privacy Framework vedtaget, hvilket betyder, at personoplysningerne lovligt kan overføres til USA, såfremt modtageren i USA er certificeret under ordningen. De fleste cloudleverandører, herunder AWS og Google, er certificerede, hvilket betyder, at der gerne må overføres til USA, men kun hvis der er en instruks hertil.[239]

Data Privacy Framework indeholder principper om databeskyttelse, som de certificerede virksomheder er forpligtet til at iagttage.[240] På baggrund af principperne samt de nye retssikkerhedsgarantier for EU-borgere, har EU-Kommissionen vurderet, at Data Privacy Framework giver et tilstrækkeligt beskyttelsesniveau.[241]

[234] (Schrems II C-311/18, 2020), præmis 187
[235] (Schrems II C-311/18, 2020), præmis 190
[236] (Schrems II C-311/18, 2020), præmis 195
[237] (Schrems II C-311/18, 2020), præmis 196
[238] (Schrems II C-311/18, 2020), præmis 201
[239] (Data Privacy Framework, 2024)
[240] (EU-Kommissionen, 2023), spørgsmål 3
[241] (Datatilsynet, EU-U.S. Data Privacy Framework, 2024) ”*EU-U.S Data Privacy Framework*”

Præsidenten i USA, Joe Biden, har i 2022 vedtaget Executive Order 14086 (herefter "E.O 14086"), som imødekommer de problemer, som EU-Domstolen rejste i Schrems II. E.O 14086 sikrer, at efterretningsaktiviteter er underlagt passende sikkerhedsforanstaltninger, som skal sikre de registreredes grundlæggende rettigheder og frihedsrettigheder.[242] Blandt andet kan der udelukkende foretages efterretningsaktiviteter, hvis det vurderes, at det er nødvendigt, legitimt og proportionalt for efterretningsaktiviteten. Proportionalitetsafvejningen skal ses i lyset af de registreredes grundlæggende rettigheder.[243]

Derudover er de amerikanske efterretningstjenesters aktiviteter underlagt et forbedret tilsyn i forhold til at sikre overholdelse af begrænsninger for overvågningsaktiviteter.[244] Slutteligt er der i forbindelse med vedtagelse af E.O 14086 etableret en ny klageordning, hvor en uafhængig og bindende myndighed håndterer klager fra enhver person, hvis personoplysninger er blevet overført fra EU/EØS til virksomheder i USA. De europæiske borgere skal ikke påvise, at deres personoplysninger er blevet indsamlet af de amerikanske efterretningstjenester, men blot indgive en klage til deres nationale tilsynsmyndighed, som herefter sikre, at klagen viderebehandles korrekt. Disse klager vil efterfølgende blive videresendt til USA af EDPB. Klagen vil herefter blive undersøgt af Civil Liberties Protection Officer (herefter "CLPO"), som er ansvarlig for at sikre, at amerikanske efterretningstjenester overholder de grundlæggende rettigheder. Såfremt en EU-borger er utilfreds med beslutningen fra CLPO, kan denne klage til den nyoprettede Data Protection Review Court (herefter "DPRC"). I modsætning til den tidligere tilsynmekanisme, ombudsmanden, er medlemmerne af DPRC ikke en del af den amerikanske regering og kan ikke modtage instrukser fra regeringen. DPRC fungerer således som en uafhængig klagemekanisme og kan træffe bindende afgørelser, hvis de finder, at personoplysningerne er blevet indsamlet i strid med E.O 14086.[245]

9.2 FISA 702

Ud fra analysen af Schrems I og II står det klart, at der er bekymring for de amerikanske myndigheders overvågning. Nedenfor vil overvågning i henhold til FISA 702 blive nærmere belyst.

[242] (Executive Order 14086, 2022), Section 2 (a)(ii)
[243] (Executive Order 14086, 2022), Section 2 (a)(ii)(A) og Section 2 (a)(ii)(B)
[244] (Executive Order 14086, 2022), Section 2 (a)(ii)(B)(iii)
[245] (EU-Kommissionen, 2023), spørgsmål 5, (Executive Order 14086, 2022), Section 5 (h) og (Datatilsynet, Nye klageformularer vedrørende overførsler til USA, 2024)

FISA 702 er implementeret i den amerikanske lov 50 U.S.C § 1881a. Som det fremgår af bestemmelsen og som nævnt i Schrems II giver FISA 702 de amerikanske myndigheder mulighed for at få adgang til personoplysninger fra amerikanske virksomheder til brug for efterretningsaktiviteter.[246] Det er et krav i henhold til FISA 702, at oplysningerne omhandler *non-U.S persons*. Endvidere er det et krav, at personerne, der indsamles oplysninger om, med rimelighed kan antages at være placeret uden for USA. I den forbindelse kan det bemærkes, at en dataansvarlig i EU/EØS, som benytter en cloudleverandør placeret i USA eller som har underdatabehandlere i USA, skal være opmærksom på, at der behandles oplysninger om *non-U.S persons*, og dermed kan være omfattet af FISA 702.

Endvidere er det et krav i henhold til FISA 702, at indhentning af disse personoplysninger skal være med henblik på at få adgang til *foreign intelligence information*. Det betyder at personoplysningerne skal være relevante for efterretningsaktiviteten.[247] Proceduren for indhentelsen af personoplysninger er, at den amerikanske justitsminister og direktøren for den nationale efterretningstjeneste starter med at sende en skriftlig certificering til godkendelse ved FISC. FISC godkender og fører tilsyn med den udenlandske efterretningsaktivitet, og i den forbindelse vurderer, hvorvidt den konkrete overvågning er korrekt i henhold til FISA 702. Herefter udsteder den amerikanske justitsminister og direktøren for den nationale efterretningstjeneste direktiver om udlevering af personoplysninger til de såkaldte *electronic communications service providers.*[248] En *electronic communications service provider* er defineret bredt, hvilket betyder, at en cloudleverandør derfor kan være omfattet af denne definition.[249] Derudover kræver indsamlingen i henhold til FISA 702, at efterretningstjenesterne har en såkaldt *selector*, hvilket eksempelvis er en e-mailadresse eller telefonnummer, som kommunikationen er enten til eller fra.[250]

9.3 Sammenfatning

Opsummerende kan det konstateres, at der har været behov (og stadig er) for at overføre personoplysninger til USA fra EU/EØS, hvorfor der af flere omgange har været

[246] (Schrems II C-311/18, 2020), præmis 61
[247] (U.S.C § 1881a) og (Schrems II C-311/18, 2020), præmis 61
[248] (U.S.C § 1881a)(a)
[249] (U.S.C § 1881a)(b)(4)
[250] (Datatilsynets Vejledning om cloud, 2022), side 21 ff.

certificeringsordninger, som lovliggjorde denne overførsel henholdsvis Safe Harbor, Privacy Shield og den nugældende Data Privacy Framework. Som nævnt i afsnit 8.3 er det EU-Kommissionen, som træffer tilstrækkelighedsafgørelser, såfremt de finder, at det pågældende tredjeland har et tilstrækkeligt beskyttelsesniveau, hvilket er et beskyttelsesniveau som i det væsentligste svarer til niveauet i EU/EØS.[251] EU-Domstolen har i Schrems I og II foretaget en vurdering af EU-Kommissionens tilstrækkelighedsafgørelse for så vidt angår Safe Harbor og Privacy Shield.

I Schrems I foretog EU-Domstolen en vurdering af, hvorvidt Safe Harbor sikrede et tilstrækkeligt beskyttelsesniveau. I den forbindelse fastlagde EU-Domstolen, at EU-Kommissionen skulle iagttage tredjelandets nationale lovgivning og internationale forpligtelser.[252] Problemet med Safe Harbor var, at amerikansk lovgivning havde forrang i forhold til principperne i Safe Harbor, hvilket betød, at de registreredes rettigheder i visse tilfælde blev undermineret, hvilket er i strid med både databeskyttelsesforordningen og chartrets art. 7, 8 og 47.[253] Når der er et indgreb i de grundlæggende rettigheder, skal rækkevidden af indgrebet være præcist og klart fastlagt, og begrænsningerne skal holdes til det strengt nødvendige.[254] EU-Kommissionen havde i deres vurdering af tilstrækkeligt beskyttelsesniveau i USA ikke undersøgt den nationale lovgivning i USA og derfor erklæres afgørelsen ugyldig uden at undersøge principperne i Safe Harbor.[255]

EU-Domstolens konklusion er i overensstemmelse med databeskyttelsesforordningens art. 45, idet EU-Kommissionen er forpligtet til at undersøge national lovgivning i forbindelse med vedtagelse af en tilstrækkelighedsafgørelse.[256] Derudover havde de registrerede ikke ret til domstolsprøvelse.[257] Safe Harbor blev erklæret ugyldig og derfor var retstilstanden fra den 6. oktober 2015, at overførselsgrundlaget ikke kunne findes i en tilstrækkelighedsafgørelse i medfør af databeskyttelsesforordningens art. 45.[258] Derfor skulle der findes et andet overførselsgrundlag i kapitel V, jf. databeskyttelsesforordningens art. 46 eller 49.

[251] (Schrems I C-362/14, 2015), præmis 73 og (Schrems II C-311/18, 2020), præmis 94
[252] (Schrems I C-362/14, 2015), præmis 70 og 71
[253] (Schrems I C-362/14, 2015), præmis 86 og 87
[254] (Den Europæiske Unions charter , 2009), artikel 52, stk. 1
[255] (Schrems I C-362/14, 2015), præmis 98 og 107
[256] (Schrems I C-362/14, 2015), præmis 75 og 76
[257] (Schrems I C-362/14, 2015), præmis 94 og 95
[258] (Schrems I C-362/14, 2015), præmis 98 og 107

Efterfølgende blev Privacy Shield vedtaget af EU-Kommissionen, jf. databeskyttelses-forordningens art. 45.[259] USA havde forsøgt at afdække manglerne i Safe Harbor, og dermed overholde chartret.[260] EU-Domstolen anfører, at såfremt der ikke er vedtaget en tilstrækkelighedsafgørelse, må der kun overføres personoplysninger, hvis der er givet de fornødne garantier og på betingelse af, at rettigheder som kan håndhæves og effektive retsmidler er tilgængelige for de registrerede.[261] Såfremt der skal ske overførsel i henhold til en tilstrækkelighedsafgørelse, skal der være et tilstrækkeligt beskyttelsesniveau i tredjelandet. Hvis der ikke er en tilstrækkelighedsafgørelse, skal databehandleren eller den dataansvarlige kompensere for den manglende databeskyttelse i tredjelandet. Dette kan ske ved at stille fornødne garantier som nævnt i afsnit 8.4.

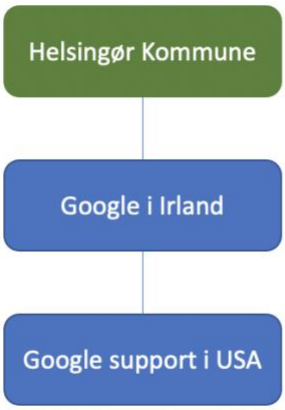
9.4 Chromebook-sagen

I nærværende afsnit vil der foretages en analyse af Chromebook-sagen, hvor specialet vil analysere Datatilsynets afgørelse sammenholdt med databeskyttelsesforordningen, chartret, amerikansk lovgivning samt tidligere retspraksis fra EU-Domstolen og Datatilsynet. På baggrund af analysen vil specialet fastlægge den gældende retstilstand og besvare problemformuleringens andet underspørgsmål angående, hvordan den dataansvarlige sikrer, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelses-forordningen, når der anvendes en cloudleveandør med underdatabehandlere i USA.

9.4.1 Sagens faktum

En række kommuner har indgået en databehandleraftale med Google om brugen af ChromeBooks, hvor Google behandler elevernes personoplysninger på vegne af kommunerne. Det betyder, at kommunerne i denne henseende er dataansvarlige og Google Irland er databehandler. Endvidere benytter Google Irland en underdatabehandler, som er en supportfunktionen i USA.[262] Nedenfor illustreres databehandlerkonstruktionen:

[259] (KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2016, 2016)
[260] (Schrems II C-311/18, 2020), præmis 43
[261] (Databeskyttelsesforordningen, 2016), artikel 46
[262] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)



Figur: Databehandlerkonstruktion

Chromebook-sagen startede den 11. december 2019, hvor en forælder klagede til Datatilsynet over, at hans barn fik oprettet en YouTube-konto, som skulle benyttes i folkeskolens undervisning. Mere specifikt blev børnenes fulde navn, skolenavn og klassetrin oplyst i forbindelse med oprettelse af kontoen. Forældrene var ikke informeret om, at deres børn fik oprettet denne konto, men en forælder opdagede, at barnets oplysninger blev offentliggjort på Youtube, når eleven lavede et opslag eller kommenterede et opslag.[263]

I 2020 anmeldte kommunen hændelsen som et brud til Datatilsynet. Nærværende afsnit vil belyse den del af sagen, som omhandler supportfunktionen i USA.[264] Første afgørelse adresserer ikke problematikken om tredjelandsoverførsler uddybende, men Datatilsynet pointerer blot, at databeskyttelsesforordningens kapitel V skal overholdes ved tredjelandsoverførsler. Anden afgørelse fra 2022 mod Helsingør Kommune behandler problemstillingen om overførsel af personoplysninger til tredjelande, herunder USA, hvorfor det er denne sag, der tages udgangspunkt i.[265]

9.4.2 Instruks til brug af underdatabehandlere

Dette afsnit vil belyse problemstillingen angående Helsingør Kommunes instruks til brug af underdatabehandlere.

[263] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[264] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[265] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)

Helsingør Kommune og Google Irland har udarbejdet en databehandleraftale, hvilket er et krav i henhold til databeskyttelsesforordningens art. 28, stk. 3. Af databehandleraftalen fremgår følgende af punkt 10.1:[266]

> *"10.1 Data Storage and Processing Facilities. Subject to Google's data location commitments under the Service Specific Terms and to the remainder of this Section 10 (Data Transfers), Customer Data may be processed in any country in which Google or its Subprocessors maintain facilities. [...]"*

Det betyder, at personoplysninger kan behandles både inden- og uden for EU/EØS af underdatabehandlere, når der skal ydes support. Ifølge Datatilsynets afgørelse, skal kommunen (som dataansvarlig) ved support i et tredjeland sikre sig, at personoplysningerne ikke overføres til tredjelande, medmindre der er givet instruks hertil.[267]

Datatilsynets udtalelse er i overensstemmelse med databeskyttelsesforordningens art. 28, stk. 3, litra a og art. 29, om at en databehandler kun må behandle personoplysninger efter instruks fra den dataansvarlige. Således må en databehandler kun overføre oplysninger til en underdatabehandler, hvis den dataansvarlige har instrueret databehandleren hertil. Såfremt databehandleren handler uden for instruks og benytter en underdatabehandler, der ikke er givet instruks til, vil databehandleren blive selvstændig dataansvarlig for denne del af behandlingen.[268] Datatilsynet har i en tidligere afgørelse vedrørende ServiceNow, udtalt, at en databehandler (EG) bliver selvstændig dataansvarlig, da EG handler uden for den instruks der er fastsat i databehandleraftalen ved at anvende en underdatabehandler (ServiceNow) uden godkendelse.[269]

Det kan heraf udledes, at en cloudleverandør, som databehandler, kun må handle inden for instruks, herunder kun benytte underdatabehandlere der er givet instruks til i databehandleraftalen. Såfremt cloudleverandøren handler uden for instruks, ved at overføre personoplysninger til en underdatabehandler, der ikke er givet instruks til, vil cloudleverandøren være selvstændig dataansvarlig herfor. Det betyder, at cloudleverandøren

[266] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[267] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[268] (Databeskyttelsesforordningen, 2016), artikel 28, stk. 10
[269] (Datatilsynet Journalnummer: 2019-442-3996, 2019) og (Databeskyttelsesforordningen, 2016), artikel 28, stk. 10

skal overholde databeskyttelsesforordningens krav som selvstændig dataansvarlig. Dog slipper den oprindelige dataansvarlige ikke for ansvar i medfør af databeskyttelsesforordningens art. 82-84, selvom det er cloudleverandøren, der handler i strid med instruksen og benytter en underdatabehandler, der ikke er instrueret i. Dette ansvar hænger sammen med, at den dataansvarlige skal vælge en cloudleverandør, som kan efterleve forordningen.[270]

9.4.3 Godkendelse af underdatabehandlere

Nærværende afsnit vil belyse databeskyttelsesforordningens krav om godkendelse af underdatabehandlere i relation til Chromebook-sagen.

Af databehandleraftalen mellem Helsingør Kommune og Google Irland fremgår følgende af punkt 11.1:[271]

> *"11.1 Consent to Subprocessor Engagement. Customer specifically authorizes the engagement as Subprocessors of those entities listed as of the Amendment Effective Date at the URL specified in Section 11.2 (Information about Subprocessors). [...]"*

Det vil sige, at Helsingør Kommune giver specifik tilladelse til brug af de underdatabehandlere, der er henvist til i punkt 11.2 i databehandleraftalen, herunder supportfunktionen i USA.[272] I denne afgørelse pointerer Datatilsynet, at Helsingør Kommune dermed har godkendt brugen af underdatabehandlere, der fremgår af databehandleraftalen, herunder godkendt og instrueret benyttelse af underdatabehandlere i USA.[273]

Formuleringen i databehandleraftalens punkt 11.1 vedrørende godkendelse af under-databehandlere, er i overensstemmelse med databeskyttelsesforordningens art. 28, stk. 2, som tilsiger, at en databehandler kun må gøre brug af underdatabehandlere ved forudgående specifik eller generel skriftlig godkendelse fra den dataansvarlige. Såfremt den dataansvarlige ikke har givet godkendelse til brug af underdatabehandlere, vil det være i strid med databeskyttelses-forordningens art. 28, stk. 2. I den fornævnte sag vedrørende ServiceNow, udtalte Datatilsynet,

[270] (Udsen, 2022), side 119 og (Databeskyttelsesforordningen, 2016), artikel 28, stk. 1
[271] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[272] (Google Workspace, 2024)
[273] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)

at idet databehandleren (EG) ikke havde fået en godkendelse til brug af en ny under-databehandler, handlede EG i strid med databeskyttelsesforordningens art. 28, stk. 2.[274]

På baggrund af ovenstående kan det udledes, at en dataansvarlig skal godkende cloudleverandørens underdatabehandlere ved generel specifik godkendelse eller forudgående godkendelse. Såfremt der i denne godkendelse fremgår underdatabehandlere i USA, vil det betyde, at den dataansvarlige giver instruks til brug af en underdatabehandler i USA. Konsekvensen ved at den dataansvarlige godkender og instruerer til brug af en underdatabehandler i USA, er at den dataansvarlige skal iagttage databeskyttelses-forordningens kapitel V, jf. nærmere herom i nedenstående afsnit.[275]

9.4.4 Overførsler til tredjelande

I nærværende afsnit analyseres Datatilsynets afgørelse i Chromebook-sagen i relation til databeskyttelsesforordningens kapitel V, navnlig databeskyttelsesforordningens art. 44 og 46, stk. 1, litra c. Herefter analyseres Datatilsynets udtalelse vedrørende den amerikanske overvågningslovgivning samt de supplerende foranstaltninger, som kan anvendes.

9.4.4.1 Databeskyttelsesforordningens art. 44

Som nævnt fremgår det af databehandleraftalen, at Google Irland må anvende underdatabehandlere i blandt andet USA. I den forbindelse nævner Datatilsynet i afgørelsen, at det vil være en tilsigtet overførsel, hvis Google Irland overfører til USA, da databehandleren som nævnt ovenfor, har fået instruks gennem databehandleraftalen til at anvende de godkendte underdatabehandlere.[276] Det følger ligeledes af Datatilsynets vejledning om tredjelands-overførsler, at hvis databehandleren handler inden for instruksen i databehandleraftalen, vil det være en tilsigtet overførsel.[277] Endvidere har Datatilsynet tidligere udtalt, at sådan en situation vil udgøre en tilsigtet overførsel, jf. nærmere herom i kapitel 10 vedrørende KOMBIT-sagen. Det kan således konstateres, at Datatilsynet fastholder deres synspunkt.

[274] (Datatilsynet Journalnummer: 2019-442-3996, 2019)
[275] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[276] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[277] (Datatilsynets Vejledning, 2024), side 12

Herefter anfører Datatilsynet i Chromebook-sagen, at der skal være et gyldigt overførselsgrundlag i medfør af databeskyttelsesforordningens kapitel V.[278] Datatilsynets vurdering er i overensstemmelse med databeskyttelsesforordningens art. 44, hvorved det fremgår, at overførsler til tredjelande omfattes af kapitel V. Begrebet *tredjelande* er ikke defineret i databeskyttelsesforordningen, men det er alle lande udenfor EU/EØS. Idet USA er et land uden for EU/EØS, er USA et tredjeland, og dermed omfattet af kapitel V, jf. afsnit 8.1. Endvidere følger det af databeskyttelsesforordningens art. 44, at der kun kan ske overførsel til et tredjeland, hvis der foreligger et overførselsgrundlag i kapitel V samtidig med, at den resterende del af forordningens bestemmelser overholdes.

I den forbindelse nævner Datatilsynet i afgørelsen, at databeskyttelsesforordningens art. 44 er en forpligtelse, som gælder for både den dataansvarlige og databehandleren. Datatilsynet mener derfor, at såvel Helsingør Kommune som Google Irland har en pligt til at tilvejebringe et effektivt overførselsgrundlag.[279] Denne holdning er Henrik Udsen enig i, idet han pointerer, at databehandleren er et selvstændigt pligtsubjekt i visse af forordningens bestemmelser, herunder *formentlig* art. 44. Endvidere anfører Henrik Udsen, at konsekvensen heraf vil være, at databehandleren også skal sikre at bestemmelsen efterleves.[280]

Datatilsynet hævder herefter i Chromebook-sagen, at forpligtelsen til at sikre et overførselsgrundlag, gælder ligeledes, når det er Google Irland, som indgår standardbestemmelser med underdatabehandlere i tredjelande efter databeskyttelsesforordningens art. 46, stk. 2, litra c. Endvidere anfører Datatilsynet, at Helsingør Kommune i disse tilfælde skal kunne sikre samt påvise, at Google Irland har tilvejebragt et fornødent overførselsgrundlag, som er effektivt. Datatilsynets opfattelse er i overensstemmelse med databeskyttelsesforordningens art. 5, stk. 2, hvoraf det fremgår, at den dataansvarlige er ansvarlig for at forordningen overholdes.[281]

[278] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[279] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[280] (Udsen, 2022), side 112
[281] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)

9.4.4.2 Databeskyttelsesforordningens art. 46, stk. 2, litra c

Datatilsynet anfører i Chromebook-sagen, at et gyldigt overførselsgrundlag eksempelvis er indgåelse af en standardbestemmelser, som EU-Kommissionen har vedtaget.[282] Netop dette overførselsgrundlag er benyttet mellem databehandleren og underdatabehandleren i Chromebook-sagen. Datatilsynets udtalelse er i overensstemmelse med databeskyttelses-forordningen, idet tilstrækkelighedsafgørelsen angående Privacy Shield var erklæret ugyldig i Schrems II, hvorved der på dette tidspunkt ikke var et overførselsgrundlag i henhold til databeskyttelsesforordningens art. 45, og derfor kan databeskyttelsesforordningens art. 46, stk. 2, litra c benyttes som et gyldigt overførselsgrundlag.[283]

Datatilsynet henviser til EU-domstolens præmisser i Schrems II, hvor det fremgår, at standardbestemmelserne kræver, at der kan sikres et beskyttelsesniveau i tredjelandet som i det *væsentligste* svarer til niveauet af beskyttelse i EU/EØS.[284] Databeskyttelsesforordningen definerer ikke, hvad der er et *tilstrækkeligt* beskyttelsesniveau, men det fremgår af præamblen, at de fysiske personers grundlæggende rettigheder og frihedsrettigheder ikke må undermineres som følge af utilstrækkeligt beskyttelsesniveau.[285] Datatilsynets udtalelse er således i overensstemmelse med EU-Domstolens afgørelse og præamblen.

Opsummerende kan det udledes, at såfremt en cloudleverandør i EU/EØS overfører til USA, skal der sikres et gyldigt overførselsgrundlag i henhold til kapitel V. Denne forpligtelse gælder formentlig både for den dataansvarlige og cloudleverandøren, jf. databeskyttelses-forordningens art. 44.[286] Denne forpligtelse gælder uagtet, at det er cloudleverandøren som har indgået en standardbestemmelser med en underdatabehandler i et tredjeland.[287] Endvidere kan det fastslås, at databeskyttelsesforordningens art. 46, stk. 2, litra c er et gyldigt overførselsgrundlag. I den henseende er det fastslået i Schrems I og II, at databeskyttelses-forordningens art. 46 kræver, at der er sikret et tilstrækkeligt beskyttelsesniveau, som i det væsentlige svarer til niveauet af beskyttelse i EU/EØS.[288]

[282] (Databeskyttelsesforordningen, 2016), artikel 46, stk. 2, litra c
[283] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[284] (Datatilsynet, Journalnummer: 2020-431-0061, 2022), (Schrems II C-311/18, 2020), præmis 101 og 105
[285] (Databeskyttelsesforordningen, 2016), præambelbetragtning nr. 101
[286] (Udsen, 2022), side 112 og (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[287] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[288] (Datatilsynet, Journalnummer: 2020-431-0061, 2022) og (Schrems II C-311/18, 2020), præmis 101 og 105

9.4.4.3 Amerikansk overvågningslovgivning

I Chromebook-sagen henviser Datatilsynet til Schrems II, hvor det fremgår, at standard-bestemmelser ikke vil være tilstrækkelig i forhold til at sikre effektiv beskyttelse af personoplysninger, hvis tredjelandets lovgivning giver tilladelse til, at myndighederne kan gøre indgreb i de registreredes grundlæggende rettigheder.[289] Underdatabehandleren befinder sig i nærværende sag i USA, hvorfor det er den amerikanske lovgivning, som skal tages i betragtning for at vurdere, hvorvidt lovgivningen giver myndighederne mulighed for at gøre indgreb i de registrerede grundlæggende rettigheder og dermed ikke udgør et tilstrækkeligt beskyttelses-niveau i henhold til EU-retten. Den amerikanske lovgivning som EU-Domstolen henviser til i Schrems II, og Datatilsynet henviser til i Chromebook-sagen, er henholdsvis FISA 702, E.O. 12333 og PPD-28.[290]

I nærværende afgørelse hævder Helsingør Kommune, at kommunens personoplysninger ikke omhandler *U.S.-persons* og dermed ikke er omfattet af FISA 702. Imidlertid pointerer Data-tilsynet, at FISA 702 finder anvendelse på *non-U.S persons*, hvorfor Helsingør Kommunes underdatabehandler er omfattet af FISA 702 og dermed kan blive pålagt udlevering af personoplysningerne.[291]

Det følger af U.S.C § 1881a, at personoplysningerne skal omhandle en *non-U.S persons* som med rimelig sandsynlighed ikke befinder sig i USA. Desuden fremgår det, at personoplysninger skal indsamles hos en *electronic communication service provider*. Datatilsynet hævder i Chromebook-sagen, at Google kan defineres som en *electronic communication service provider*. Datatilsynets udtalelse er i overensstemmelse med ordlyden i U.S.C § 1881 (b)(4), som er bred, og dermed kan en cloudleverandør være omfattet heraf. Datatilsynet er af den opfattelse, at FISA 702 finder anvendelse i sagen angående Chromebook, og at ingen personoplysninger er omfattet af de fastsatte begrænsninger i U.S.C. § 1881 a(b). I henhold til U.S.C. § 1881a(b) kan FISA 702 begrænses, hvis personoplysninger omhandler en amerikansk statsborger eller personoplysninger omhandler en person, som med rimelighed befinder sig i USA. I Chromebook-sagen omhandler personoplysningerne EU-borgere, og disse borgere befinder sig i Danmark, hvorfor Datatilsynets opfattelse er i overensstemmelse med bestemmelsen i U.S.C. § 1881 a(b) sammenholdt med afgørelsens faktum.

[289] (Schrems II C-311/18, 2020), præmis 126
[290] (Datatilsynets Journalnummer: 2022-431-0167, 2022) og (Schrems II C-311/18, 2020), præmis 60-63
[291] (Datatilsynets Journalnummer: 2022-431-0167, 2022)

I Chromebook-sagen nævner Datatilsynet, at E.O. 12333 giver de amerikanske myndigheder mulighed for adgang til personoplysninger, der er i transit. Herved kan de amerikanske myndigheder få adgang til personoplysningerne, inden de befinder sig i USA, og herefter kan omfattes af FISA 702.[292] Datatilsynets udtalelse angående FISA 702 og E.O 12333 er i overensstemmelse med EU-Domstolen udtalelse i Schrems II, beskriver anvendelsesområdet for FISA 702 og E.O 12333.[293] EU-Domstolen fastslog herefter i Schrems II, at disse amerikanske lovgivninger, sammenholdt med PPD-28, ikke er i overensstemmelse med chartrets art. 52. Dette skyldes, at disse lovgivninger ikke er begrænset til det strengt nødvendige. Derudover fastslog EU-Domstolen, at disse amerikanske lovgivninger ikke er i overensstemmelse med chartrets art. 47.[294]

Hernæst anfører Datatilsynet i Chromebook-sagen, at i og med Helsingør Kommunes underdatabehandler, Google i USA, er omfattet af FISA 702 og E.O. 12333, vil standard-bestemmelserne som overførselsgrundlag, ikke sikre et tilstrækkeligt beskyttelsesniveau. Hertil anfører Datatilsynet, at der derfor skal etableres supplerende foranstaltninger. Datatilsynets opfattelse stemmer overens med EU-Domstolens opfattelse i Schrems II, hvor de har anført, at standardbestemmelserne kun er bindende for kontraktparterne og ikke bindende for de amerikanske myndigheder,[295] og derfor kan det være nødvendigt med supplerende foranstaltninger for at opretholde et tilstrækkeligt beskyttelsesniveau, som er krævet i henhold til EU-retten.[296]

På baggrund af ovenstående kan det udledes, at FISA 702 finder anvendelse, hvis der er tale om personoplysninger om *non-US persons*, og personoplysningerne befinder sig hos en *electronic communication service provider*, som er bredt defineret. Det kan formentlig konstateres, at Google i USA vil være omfattet af dette begreb ud fra Datatilsynets udtalelse i Chromebook-sagen sammenholdt med den brede definition af begrebet i U.S.C §1881(b)(4). Derudover kan det udledes, at E.O. 12333 giver de amerikanske myndigheder adgang til personoplysninger, når de er i transit. I og med at disse amerikanske lovgivninger ikke er begrænset til det strengt nødvendige, er de i strid med chartrets art. 52. Desuden vil EU-

[292] (Datatilsynets Journalnummer: 2022-431-0167, 2022) og (Schrems II C-311/18, 2020), præmis 61 og 63
[293] (Schrems II C-311/18, 2020), præmis 61 og 63
[294] (Schrems II C-311/18, 2020), præmis 181, 182 og 184
[295] (Schrems II C-311/18, 2020), præmis 125-127
[296] (Schrems II C-311/18, 2020), præmis 132 og (Databeskyttelsesforordningen, 2016), præambelbetragtning nr. 109

borgerne ikke kunne håndhæve deres rettigheder overfor de amerikanske myndigheder ved en domstol, hvilket er i strid med chartrets art. 47. Da det er konstateret, at personoplysningerne kan være genstand for FISA 702 og E.O. 12333 skal der anvendes supplerende foranstaltninger, jf. nærmere herom i nedenstående afsnit.

9.4.4.4 Supplerende foranstaltninger

Datatilsynet anfører i Chromebook-sagen, at Helsingør Kommune anvender kryptering som en supplerende foranstaltning både i transit og i hvile. Dog oplyses det i sagen, at support-funktionen i USA i visse tilfælde har adgang til personoplysninger i klartekst. Endvidere oplyses det, at det er Google Irland, der opbevarer dekrypteringsnøglen og ikke Google i USA. Datatilsynets anerkender, at kryptering kan være en effektiv supplerende foranstaltning til standardbestemmelserne, der kan være med til at sikre et tilstrækkeligt beskyttelsesniveau. Datatilsynets opfattelse af, at kryptering kan være en effektiv supplerende foranstaltning, er i overensstemmelse med databeskyttelsesforordningens art. 32, stk. 1, litra a, hvoraf det fremgår at kryptering af personoplysninger kan anvendes som foranstaltning til at sikre et tilstrækkeligt beskyttelsesniveau.

I nærværende afgørelse finder Datatilsynet dog ikke, at krypteringen er en effektiv supplerende foranstaltning, som er med til at sikre et tilstrækkeligt beskyttelsesniveau. Dette skyldes, at supportfunktionen i USA kan få adgang til personoplysninger i klartekst, og dermed kan personoplysningerne blive genstand for FISA 702. Hertil konkluderer Datatilsynet, at brugen af cloudleverandøren med underdatabehandlere i USA i den konkrete situation ikke er i overensstemmelse med databeskyttelsesforordningens art. 44, jf. art. 46, stk. 2, litra c.[297] Datatilsynets opfattelse er i overensstemmelse med EDPB's opfattelse vedrørende kryptering. EDPB har anført, at adgangen i klartekst i USA kan medføre, at krypteringen ikke er en effektiv supplerende foranstaltning, som sikrer et tilstrækkeligt beskyttelsesniveau.[298] EDPB har udarbejdet anbefalinger angående supplerende foranstaltninger. Heri anfører EDPB, at de supplerende foranstaltninger skal være effektive i forhold til den konkrete overførsel, og dermed effektiv til at forhindre myndigheder i tredjelandet at få adgang til person-oplysningerne.[299]

[297] (Datatilsynets Journalnummer: 2022-431-0167, 2022)
[298] (Datatilsynets Vejledning om cloud, 2022), side 22 og 23
[299] (EDPB Henstilling nr. 01/2020, 2021), side 23 og 24

Endvidere er Datatilsynets konklusion i overensstemmelse med databeskyttelsesforordningens bestemmelser, idet databeskyttelsesforordningens art. 46, stk. 2, litra c giver hjemmel til overførsel til USA. Dog er standardbestemmelserne kun bindende for kontraktparterne, og ikke de amerikanske myndigheder. Standardbestemmelserne skal derfor suppleres med foranstaltninger, såsom kryptering, for at sikre et tilstrækkeligt beskyttelsesniveau. Krypteringen i Chromebook-sagen er ikke effektiv, fordi der er adgang til personoplysningerne i klartekst i USA. Der er derfor ikke tilvejebragt et gyldigt overførselsgrundlag i art. 46, stk. 2, litra c, og dermed er det i strid med art. 44, som kræver, at der er en hjemmel til overførsel i kapitel V samtidig med at den resterende del af forordningen overholdes.[300]

Opsummerende kan det udledes af nærværende afsnit, at kryptering kan være en effektiv supplerende foranstaltning til databeskyttelsesforordningens art. 46, stk. 2, litra c. Dog vil krypteringen ikke være en effektiv supplerende foranstaltning, såfremt USA har adgang til personoplysningerne i klartekst, fordi de amerikanske myndigheder herved kan få adgang til personoplysningerne i henhold til FISA 702. Dette vil være i strid med databeskyttelses-forordningens art. 44 og 46, stk. 2, litra c.[301]

9.4.5 Retstilstanden i dag

På baggrund af ovenstående analyse kan retstilstanden i dag fastlægges. Følgende kapitel vil gennemgå retstilstanden i dag ved anvendelse af en cloudleverandør, der er certificeret under Data Privacy Framework. Desuden vil retstilstanden i dag ved anvendelse af en cloudleverandør, der ikke er certificeret blive belyst. Datatilsynet har endnu ikke forholdt sig yderligere til problemstillingen angående tredjelandsoverførsler i Chromebook-sagen, hvorfor nedenstående pointer er fremsat på baggrund af specialets indledende kapitler.

9.4.5.1 Overførselsgrundlag til ikke certificerede cloudleverandører

Nærværende afsnit er relevant i dag, såfremt en europæisk dataansvarlig vil overføre personoplysninger til USA gennem en cloudleverandør, som ikke er certificeret under Data Privacy Framework. Derudover vil pointerne nedenfor gøre sig gældende, såfremt tilstrækkelighedsafgørelsen erklæres ugyldig i fremtiden, jf. nærmere herom i perspektivering.

[300] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[301] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)

Standardbestemmelserne og kryptering

For at overførslen til USA er i overensstemmelse med databeskyttelsesforordningens art. 44 og art. 46, stk. 2, litra c, skal en europæisk dataansvarlig, som benytter sig af en cloudleverandør med underdatabehandleren i USA træffe effektive supplerende foranstaltninger, som eksempelvis kryptering. Denne kryptering skal være effektiv, således at underdatabehandleren i USA ikke har adgang til personoplysninger i klartekst.[302] Chromebook-sagen klarlægger ikke, hvorvidt denne kryptering kan blive effektiv, men EDPB har som nævnt udtalt, at kryptering kan være en effektiv foranstaltning, såfremt risikoen for uautoriseret adgang, herunder de amerikanske myndigheders adgang, forhindres.[303]

Henning Mortensen og Kasper Bjerre Hendrup Andersen har i deres artikler belyst kryptering, og dennes effektivitet. Ifølge Henning Mortensen er det væsentligt, at dekrypteringsnøglen ikke er tilgængelig for uvedkommende, samt at en længere dekrypteringsnøgle vil gøre det sværere at dekryptere dataene.[304] Endvidere bemærker Kasper Bjerre Hendrup Andersen, at flere cloudleverandører giver mulighed for at kunderne selv opbevarer dekrypteringsnøglen, og på den måde vil det ikke være muligt for cloudleverandøren at dekryptere dataene. For at sikre at den effektive kryptering gennemføres, skal databehandleraftalen fastsætte at cloud-leverandøren skal benytte kryptering som foranstaltning.[305] Det vil således ikke være lovligt for cloudleverandøren at dekryptere personoplysninger i medfør af databehandleraftalen. [306]

Instruks

En anden måde at sikre overholdelse af databeskyttelsesforordningen og chartret er ved, at den dataansvarlige helt fravælger, at den amerikanske cloudleverandør benytter en underdatabehandler i USA. Dette skal klart fremgå af databehandleraftalen. Det er et krav i henhold til databeskyttelsesforordningens art. 28, stk. 3, at den dataansvarlige og cloudleverandøren udarbejder en databehandleraftale. I Chromebook-sagen bemærker Datatilsynet, at den europæiske dataansvarlig ikke kan fraskrive sig ansvar i henhold til databeskyttelsesforordningen med den begrundelse, at der benyttes en standard-databehandleraftale udarbejdet af cloudleverandøren. Den dataansvarlige skal efterleve

[302] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[303] (EDPB Henstilling nr. 01/2020, 2021), side 31
[304] (Mortensen, 2018), "*Sikkerhedsforanstaltninger – i henhold til databeskyttelsesforordningen*" RR.5.2018.21
[305] (Databeskyttelsesforordningen, 2016), artikel 28, stk. 3, litra c
[306] (Andersen, 2023), "*Hvornår er en fysisk person "identificeret eller identificerbar" i GDPR's forstand?"* afsnit 3.1 og (EDPB Henstilling nr. 01/2020, 2021), side 33

forordningens krav uanset, om der benyttes cloudleverandører med høj forhandlingsstyrke grundet dens markedsposition.[307]

I databehandleraftalen skal det klart fremgå, hvad cloudleverandøren har instruks til at foretage, idet cloudleverandøren kun må behandle personoplysningerne efter instruks.[308] På den måde sikrer den dataansvarlige, at cloudleverandøren bliver ansvarlig for manglede overholdelse af instruksen. I den henseende bliver cloudleverandøren selvstændig dataansvarlig for den del af behandlingen, som der ikke er instruks til.[309] Dette vil formentlig afskrække cloudleverandøren i at handle uden for instruksen, herunder overfører til USA, hvis der ikke er instruks hertil.

Godkendelse af underdatabehandlere

Den dataansvarlige kan derudover sikre, at der ikke sker overførsel til USA ved, at der kun gives specifik eller generel skriftlig godkendelse til underdatabehandlere, der er placeret i EU/EØS, jf. databeskyttelsesforordningens art. 28, stk. 3, litra d, jf. art 28, stk. 2. På den måde giver den dataansvarlige kun instruks til overførsel inden for EU/EØS, og dermed vil det være en utilsigtet overførsel til USA, hvis cloudleverandøren overfører til USA. Konsekvensen heraf vil igen være, at cloudleverandøren bliver selvstændig dataansvarlig for den del af behandlingen.[310]

Den dataansvarlige kan sikre, at der ikke sker overførsel til USA, ved at underretning af ny underdatabehandler reguleres i databehandleraftalen, således at den dataansvarlige kan gøre indsigelse mod cloudleverandørens nye underdatabehandlere, jf. databeskyttelses-forordningens art. 28, stk. 2.

Slutteligt kan det bemærkes, at i tilfælde af, at cloudleverandøren handler uden for instruks, vil den dataansvarlige fortsat være ansvarlig, jf. databeskyttelsesforordningens art. 82-84.

Tilsyn

Den dataansvarlige kan sikre, at cloudleverandørerne overholder bestemmelserne i databehandleraftalen og databeskyttelsesforordningen ved at føre løbende tilsyn og revisioner.

[307] (Datatilsynet Journalnummer: 2023-431-0001, 2024)
[308] (Databeskyttelsesforordningen, 2016), artikel 28, stk. 3, litra a og artikel 29
[309] (Databeskyttelsesforordningen, 2016), artikel 28, stk. 10
[310] Ibid.

Efter databeskyttelsesforordningens art. 28, stk. 3, litra h skal databehandleraftalen fastlægge, at cloudleverandøren er forpligtet til at stille alle nødvendige oplysninger til rådighed for den dataansvarlige således, at den dataansvarlige kan påse, at cloudleverandøren overholder kravene. Ved at føre tilsyn med cloudleverandøren opfylder den dataansvarlige forpligtelsen til at føre løbende tilsyn, jf. databeskyttelsesforordningens art. 5, stk. 2. Som tidligere nævnt har Datatilsynet i 2022 udtalt kritik til Styrelsen for International Rekruttering, idet de ikke havde ført tilsyn med to databehandlere. I den forbindelse anførte Datatilsynet, at de ikke kunne dokumentere, at principperne i databeskyttelsesforordningens art. 5, stk. 1 overholdes, jf. databeskyttelsesforordningens art. 5, stk. 2.[311]

9.4.5.2 Overførselsgrundlag til certificerede cloudleverandører

I skrivende stund er Data Privacy Framework et gyldigt overførselsgrundlag, da EU-Kommissionen i medfør af databeskyttelsesforordningens art. 45 har truffet en tilstrækkelighedsafgørelse. Dermed kan europæiske dataansvarlige overføre person-oplysninger til de certificerede virksomheder i USA, herunder Google og AWS.[312] Med vedtagelse af E.O 14086 er efterretningsaktiviteterne i USA underlagt passende sikkerhedsforanstaltninger således, at de registrerede er sikret deres grundlæggende rettigheder og frihedsrettigheder. Efterforskningsaktiviteter kan i henhold til certificeringsordningen nu kun foretages, hvis det vurderes, at det er nødvendigt, legitimt og proportionelt for efterforskningen. Derudover er der med etableringen af E.O. 14086 indført den manglende klageadgang, som medfører, at enhver person, hvis personoplysninger er overført fra EU/EØS til virksomheder i USA, kan klage. Disse klager behandles af en upartisk domstol, navnlig CLPO og DPRC. Virksomheder som er certificeret i Data Privacy Framework har dermed et tilstrækkeligt beskyttelsesniveau, som kræves i henhold til EU-retten. Dog har Maximillian Schrems udtalt kritik af denne tilstrækkelighedsafgørelse, og der er muligvis en Schrems III på vej, nærmere herom i perspektiveringen.[313]

[311] (Datatilsynet Journalnummer: 2021-421-0102, 2021)
[312] (Data Privacy Framework, 2024)
[313] (Executive Order 14086, 2022)

9.5 Delkonklusion

Det kan på baggrund af analysen udledes, at en europæisk dataansvarlig kun må anvende en cloudleverandør, der kan efterleve databeskyttelsesforordningens krav.[314] Der skal udarbejdes en databehandleraftale med cloudleverandøren, hvilket ofte er en standard-databehandleraftale udarbejdet af cloudleverandøren. Den europæiske dataansvarlig kan ikke undgå at blive ansvarlig for manglende overholdelse af databeskyttelsesforordningen med den begrundelse, at der benyttes en standard-databehandleraftale og at cloudleverandøren har en høj forhandlingsstyrke grundet dens markedsposition.[315]

Cloudleverandøren skal handle efter den dataansvarliges instruks, herunder instruks til brugen af underdatabehandlere.[316] Den europæiske dataansvarlige skal godkende cloudleverandørens underdatabehandlere, og såfremt der godkendes underdatabehandlere i et tredjeland, skal forordningens kapitel V iagttages, og i den forbindelse skal der sikres et gyldigt overførselsgrundlag.[317] Denne forpligtelse gælder formentlig både for den dataansvarlige og cloudleverandøren.[318]

Endvidere kan databeskyttelsesforordningens art. 46 anvendes som et gyldigt overførselsgrundlag, såfremt der ikke er en tilstrækkelighedsafgørelse. Dog er databeskyttelsesforordningens art. 46 betinget af, at der er sikret et tilstrækkeligt beskyttelses-niveau, som i det væsentligste svarer til niveauet i EU/EØS. Den amerikanske lovgivning FISA 702 og E.O. 12333 giver de amerikanske myndigheder adgang til personoplysningerne uden at være i overensstemmelse med chartrets art. 52. Desuden er der ikke adgang til domstolsprøvelse, hvilket er i strid med chartret art. 47. Konsekvensen af disse amerikanske lovgivninger er, at der ikke sikres et tilstrækkeligt beskyttelsesniveau ved den blotte anvendelse af standardbestemmelserne, hvorfor der skal anvendes supplerende foranstaltninger, eksempelvis kryptering. På baggrund af Chromebook-sagen kan det konstateres, at kryptering ikke er en effektiv supplerende foranstaltning, såfremt der er adgang til personoplysninger i klartekst i USA.[319]

[314] (Nielsen & Lotterup, 2020), side 610, (Udsen, 2022), side 105-106 og (Databeskyttelsesforordningen, 2016), præambelbetragtning nr. 81
[315] (Datatilsynet Journalnummer: 2023-431-0001, 2024)
[316] (Databeskyttelsesforordningen, 2016), artikel 28, stk. 2 og 4
[317] (Databeskyttelsesforordningen, 2016), artikel 44
[318] (Udsen, 2022), side 112 og (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[319] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)

Efter Chromebook-sagen har Datatilsynet imidlertid udtalt i en forespørgsel fra Region Syddanmark, at ved anvendelse af andre cloudleverandører, navnlig Microsoft 365, gælder de samme forpligtelser. Hertil nævner Datatilsynet, at databeskyttelsesforordningen ikke forbyder brugen af cloudleverandører, men at den dataansvarlige er forpligtet til at kunne dokumentere, at personoplysningerne bliver behandlet i overensstemmelse med principperne i databeskyttelsesforordningens art. 5, stk.1, jf. art. 5, stk. 2.[320]

Problemstillingen angående overførsel til enten cloudleverandører eller dennes underdatabehandlere i USA kan løses ved, at disse er certificeret under Data Privacy Framework. Såfremt denne certificeringsordning erklæres ugyldig i fremtiden eller der overføres til en ikke-certificeret virksomhed i USA, kan databeskyttelsesforordningens art. 46, stk. 2, litra c anvendes som overførselsgrundlag med eksempelvis kryptering som supplerende foranstaltning. Denne kryptering skal være effektiv og det vil være tilfældet, såfremt krypteringen forhindrer myndighederne i tredjelandet i at få adgang til personoplysningerne.[321] På den måde vil overførslen være i overensstemmelse med databeskyttelsesforordningen og chartret.

Der kan dog opstå en anden problemstilling ved benyttelse af amerikanske cloudleverandører placeret i EU/EØS, da disse kan blive mødt med myndighedsanmodninger, såfremt moderselskabet er beliggende i USA, jf. nærmere herom i kapitel 10.

10. CLOUD Act-anmodninger

Dette kapitel har til formål at analysere, hvordan den dataansvarlige kan sikre, at en amerikansk cloudleverandør ikke udleverer personoplysninger som følge af CLOUD Act-anmodninger. I den forbindelse vil kapitlet belyse den problematiske amerikanske lovgivning, CLOUD Act. Dernæst vil kapitlet analysere Datatilsynets besvarelse af en forespørgsel fra KOMBIT for at klarlægge, hvorvidt Datatilsynets vurdering af tilsigtet overførsel, overførselsgrundlag og behandlingssikkerhed er i overensstemmelse med databeskyttelsesforordningen. I den henseende analyseres Datatilsynet opmærksomhedspunkter, som de anfører i besvarelsen til KOMBIT. Herefter vil specialet inddrage en aktindsigt i dialogen mellem Datatilsynet og KOMBIT for at belyse, hvordan formuleringer i databehandleraftalen kan afhjælpe

[320] (Datatilsynet, Journalnummer: 2023-431-0012, 2024)
[321] (EDPB Henstilling nr. 01/2020, 2021), side 31

problemstillingen angående CLOUD Act-anmodninger. På baggrund af analysen vil specialet fastlægge den gældende retstilstand og besvare problemformuleringens tredje underspørgsmål.

10.1 CLOUD Act

Nærværende afsnit vil beskrive CLOUD Act, herunder den historiske baggrund og anvendelsesområdet.

10.1.1 Vedtagelsen af CLOUD Act

CLOUD Act blev vedtaget i forbindelse med, at den amerikanske efterretningstjeneste havde forsøgt at indhente personoplysninger hos en amerikansk virksomhed placeret i Europa. Sagen United States v. Microsoft Corporation (herefter "Microsoft-sagen") vedrører de amerikanske myndigheders forsøg på at indhente beviser i forbindelse med en narkotikaefterforskning, hvor den mistænkte var kunde hos Microsoft. I december 2013 forsøgte de amerikanske myndigheder at få udleveret personoplysninger om den mistænkte person fra Microsofts servere. Microsoft udleverede herefter e-mails, der var opbevaret på deres servere inden for USA's jurisdiktion, men afviste at udlevere e-mails placeret på deres server i Irland.[322] Retssagen mellem den amerikanske regering og Microsoft verserede i flere år. Microsoft mente ikke, at der var hjemmel til udlevering af personoplysninger fra det irske datterselskab til USA.[323] Den amerikanske appeldomstol var enig med Microsoft i, at de amerikanske myndigheder ikke havde tilladelse til at kræve udlevering af personoplysninger placeret i EU/EØS fra virksomheder underlagt amerikansk jurisdiktion. Dette skyldes, at hverken Microsoft eller appeldomstolen mente, at den amerikanske lovgivning Stored Communication Act (herefter "SCA") fandt eksterritorial anvendelse.[324] Efter afgørelsen nægtede flere amerikanske virksomheder at udlevere personoplysninger, som var opbevaret på servere uden for USA, selvom der var udstedt retskendelser i overensstemmelse med SCA.[325] Det var forventet, at den amerikanske højesteret skulle tage stilling til, om SCA fandt anvendelse eksterritorialt på personoplysninger uden for USA. Sagen blev imidlertid irrelevant, idet CLOUD Act blev vedtaget inden domsafsigelsen, og dermed præciserede en klar hjemmel til at pålægge Microsoft at udlevere de pågældende oplysninger.[326]

[322] (Hemmings, Srinivasann, & Swire, 2020), side 646
[323] (Udsen, 2022), side 376
[324] (Hemmings, Srinivasann, & Swire, 2020), side 636-638
[325] (U.S Department of Justice White Paper, 2019), side 7
[326] (Udsen, 2022), side 376

CLOUD Act er en amerikansk lovgivning, som blev vedtaget af Den Amerikanske Kongres i marts 2018. CLOUD Act blev vedtaget for at fremskynde adgangen til information, der opbevares af amerikanske globale virksomheder. Den amerikanske regering har problematiseret, at cloudleverandørerne har kunder og virksomheder over hele verden, og som følge heraf kan de være underlagt flere landes lovgivninger, herunder databeskyttelses-forordningen som begrænser udleveringen af personoplysninger. Når en cloudleverandør modtager en ordre fra USA, kan der således opstå modstridende juridiske forpligtelser. I disse situationer er cloudleverandøren tvunget til at vælge, hvorvidt de vil efterleve den amerikanske lovgivning eller den europæiske lovgivning. Ved beslutning heraf er cloudleverandørerne velvidende om, at de kan stå overfor konsekvenser ved at overtræde det andets lands lov.[327]

10.1.2 Konventionen om cyberkriminalitet og MLAT

Konventionen om cyberkriminalitet pålægger hvert enkelt land, der er tiltrådt konventionen at pålægge cloudleverandører inden for deres jurisdiktion at udlevere personoplysninger, som er under cloudleverandørens kontrol, uanset hvor personoplysningerne er placeret. Som nævnt ovenfor kan cloudleverandørerne stå i en konflikt mellem flere landes lovgivninger og vil formentlig overtræde det ene lands lovgivning. Denne lovkonflikt håndteres sommetider ved hjælp af Mutual Legal Assistance Treaties (herefter "MLAT").[328]

MLAT muliggør, at et lands retshåndhævende myndighed kan anmode et andet land om at skaffe personoplysningerne. Den udenlandske part gennemgår MLAT-anmodningen i overensstemmelse med eget lands regler og kan anmode om en retskendelse i henhold til egen lov for at skaffe personoplysningerne. Såfremt retskendelsen gives, skaffer den udenlandske regering personoplysningerne og udleverer disse til den anmodede regering. Processen har mange trin og på grund af anmodningens kompleksitet, kan det tage mange måneder at fuldføre. Derudover er antallet af MLAT-anmodninger de seneste år steget drastisk, grundet den enorme mængde af elektronisk data, som virksomheder over hele verden besidder. Den amerikanske regering mener derfor, at samfundet står overfor et kritisk spørgsmål om, hvordan der kan gives en effektiv adgang til beviser for at beskytte den offentlige sikkerhed samtidig med, at respekten for privatlivet bevares. Som et svar på dette spørgsmål vedtog USA, CLOUD Act.[329]

[327] (U.S Department of Justice White Paper, 2019), side 2 og 3
[328] Ibid., side 2
[329] Ibid., side 3

10.1.3 Anvendelsesområdet for CLOUD Act

CLOUD Act indeholder to muligheder for at indhente personoplysninger fra lande uden for USA. For det første bemyndiger CLOUD Act, USA til at indgå *executive agreements* med andre lande for at løse lovkonflikten. Til efterforskning af alvorlig kriminalitet kan *executive agreements* bruges til at fjerne begrænsninger i hvert lands lov, således cloudleverandørerne kan overholde ordrer fra de forskellige lande. *Executive agreement* fremgår af CLOUD Act § 104, men vil ikke blive beskrevet nærmere i dette kapitel, da kun UK og Australien har indgået denne aftale med USA og derfor ikke har relevans for Europa på nuværende tidspunkt.[330]

Den anden del af CLOUD Act præciserer, at en virksomhed, som er underlagt ét lands jurisdiktion kan pålægges at udlevere personoplysninger, som virksomheden kontrollerer, uanset hvor det er gemt og uanset hvornår.[331] Særligt relevant for cloudleverandører er CLOUD Act § 103. Det er denne sektion, der skabte grundlaget for, at USA havde beføjelse til at pålægge Microsoft at udlevere personoplysningerne, som var placeret på de irske servere i Microsoft-sagen.[332]

Det fremgår af CLOUD Act § 103 (a), som er implementeret i SCA § 2713, at de amerikanske myndigheder har bemyndigelse til at kræve personoplysninger fra de amerikanske cloudleverandører *"uanset om sådanne [beviser] befinder sig inden for eller uden for USA."*[333] I stedet for lokation fastslår CLOUD Act, at cloudleverandørens *besiddelse, varetægt eller kontrol* er afgørende for, hvorvidt cloudleverandøren skal udlevere de beviser, som der anmodes om. Dog er det uklart, hvad der menes med *besiddelse, varetægt eller kontrol*, idet CLOUD Act ikke definerer disse begreber.[334]

De amerikanske myndigheder kan kræve udlevering af personoplysninger ved, at der udstedes en retskendelse i henhold til U.S.C § 2703.[335] For at opnå en retskendelse skal der sendes en anmodning til en uafhængig dommer i USA, som skal godkende retskendelsen. Dommeren kan

---

[330] (U.S Department of Justice White Paper, 2019), side 4 og (Swire & Paul , 2020), *"NEW DEVELOPMENTS FOR THE U.K. AND AUSTRALIAN EXECUTIVE AGREEMENTS WITH THE U.S. UNDER THE CLOUD ACT"*
[331] (U.S Department of Justice White Paper, 2019), side 3
[332] (Hemmings, Srinivasann, & Swire, 2020), side 631
[333] Ibid., side 631
[334] Ibid., side 631 og 632
[335] (U.S.C § 2703)

kun godkende retskendelsen, såfremt dommeren finder, at der er *rimelig grund til at tro*, at en bestemt forbrydelse har fundet sted eller der er formodning om, at en bestemt forbrydelse skal begås. Desuden skal retskendelsen beskrive specifikt de personoplysninger, som skal udleveres.[336] I henhold til U.S.C § 2703(2) (A-B) har cloudleverandøren mulighed for at anmode om ophævelse eller ændring af en retskendelse, men dette er meget begrænset.

Som beskrevet ovenfor har CLOUD Act fastslået, at SCA nu har eksterritorial anvendelse og kan kræve, at cloudleverandører udleverer personoplysninger, hvis der foreligger en retskendelse fra en uafhængig dommer i USA.[337]

10.1.4 Artikel 48 i relation til CLOUD Act

Cloudleverandører placeret i EU/EØS kan være underlagt amerikansk lovgivning, da de er amerikanske datterselskaber. Nærværende afsnit vil belyse, hvorvidt en udlevering af personoplysningerne i medfør af en CLOUD Act-anmodning vil kunne anerkendes i henhold til databeskyttelsesforordningens art. 48.

EU-Kommissionen har i forbindelse med den førnævnte Microsoft-sag pointeret, at databeskyttelsesforordningens art. 48 gør det klart, at en udenlandsk dommerkendelse ikke i sig selv gør en overførsel lovlig i henhold til databeskyttelsesforordningens art. 48. Endvidere har EDPB udtalt, at såfremt der ikke eksisterer en international aftale (MLAT), kan cloudleverandører underlagt EU-lovgivning ikke lovligt overføre personoplysninger til USA på baggrund af en CLOUD Act-anmodning. EDPB har desuden i deres retningslinjer fremhævet, at hvis der foreligger en MLAT mellem parterne, bør de europæiske virksomheder afvise CLOUD Act-anmodningerne og henvise det anmodede land til den eksisterende MLAT. På denne måde mener EDPB, at MLAT-processen sikrer, at personoplysninger overføres i overensstemmelse med EU-lovgivningen. Såfremt den amerikanske cloudleverandør vælger at overføre til USA grundet en CLOUD Act-anmodning fra en myndighed, finder bestemmelserne i databeskyttelsesforordningen kapitel V anvendelse samt resten af for-ordningen.[338] Endvidere fastslår EDPB, at enhver ordrer om overførsel af personoplysninger

[336] (U.S Department of Justice White Paper, 2019), side 8
[337] Ibid.
[338] (Databeskyttelsesforordningen, 2016), artikel 44

fra EU/EØS i henhold til CLOUD Act kun kan være lovlig, hvis der er et retligt grundlag i henhold til databeskyttelsesforordningens art. 6 og art. 49.[339]

Opsummerende kan det udledes, at en dommerkendelse ikke i sig selv udgør et gyldigt overførselsgrundlag, da databeskyttelsesforordningens art. 48 tillige kræver, at der foreligger en international aftale, MLAT, mellem parterne. Det betyder derfor, at hvis en dataansvarlig benytter en amerikansk cloudleverandør, der bliver mødt af CLOUD Act-anmodninger, kan det udledes, at der lovligt kan ske overførsel, hvis dette sker gennem den internationale aftale, MLAT og der er en dommerkendelse.

10.1.5 Artikel 49 i relation til CLOUD Act

Databeskyttelsesforordningens art. 49 kan i undtagelsessituationer benyttes som overførselsgrundlag, men bestemmelsen fortolkes strengt. EDPB har foretaget en undersøgelse af, hvorvidt databeskyttelsesforordningens art. 49, stk. 1, litra d-f og art. 49, stk. 1, 2. pkt. giver mulighed for udlevering af personoplysninger i medfør af en CLOUD Act-anmodning.

Databeskyttelsesforordningens art. 49, stk. 1, litra d vedrører overførsler, som er nødvendige af hensyn til vigtige samfundsinteresser. Det er fastslået i databeskyttelsesforordningens art. 49, stk. 4, at det udelukkende er samfundsinteresser anerkendt i EU-lovgivningen eller medlemsstaternes lovgivning, som den dataansvarlige er underlagt. Hertil pointerer EDPB, at et tredjelands samfundsmæssige interesser som sådan er uden betydning.[340] Det må på baggrund af EDPB's udtalelse og bestemmelsens ordlyd formodes, at der ikke kan ske overførsel på baggrund af en CLOUD Act-anmodning med hjemmel i databeskyttelsesforordningens art. 49, stk. 1, litra d.[341]

Databeskyttelsesforordningens art. 49, stk. 1, litra e vedrører overførsler, som er nødvendige for at retskrav kan fastlægges, gøres gældende eller forsvares. Endvidere fremgår det af præambelbetragtning 111, at overførslen skal være nødvendig og lejlighedsvis uanset om det er en retssag, en administrativ- eller udenretlig procedure. EDPB har i sine retningslinjer anført, at en overførsel kan finde sted i en række tilfælde. Dette kan eksempelvis være i forbindelse med

[339] (EDPB's ANNEX, 2019), side 2-4 og (Datatilsynets Vejledning, 2024), afsnit 5.5
[340] (EDPB's ANNEX, 2019), side 6 og 7
[341] (EDPB's ANNEX, 2019), side 6 og 7

en undersøgelse af kriminalitet i et tredjeland, hvor formålet med overførslen af personoplysninger er, at disse personoplysninger kan benyttes til at forsvare sig selv i en retssag. Endvidere anfører EDPB, at denne undtagelse ikke kan benyttes, hvis overførslen af personoplysninger kun giver mulighed for indledning af sager i fremtiden.[342] Det må på baggrund af EDPB's udtalelse og bestemmelsens ordlyd formodes, at der i visse snævre situationer kan ske overførsel på baggrund af en CLOUD Act-anmodning med hjemmel i databeskyttelsesforordningens art. 49, stk. 1, litra e.

Databeskyttelsesforordningens art. 49, stk. 1, litra f vedrører overførsler, som er nødvendige for beskyttelsen af den registrerede eller andre personers vitale interesser, hvor den registrerede, ikke er i stand til at give samtykke. EDPB anfører, at under visse ekstraordinære, specifikke og nødvendige omstændigheder, kan den registreredes vitale interesser bruges som et gyldigt overførselsgrundlag til at overføre personoplysninger på baggrund af en CLOUD Act-anmodning. Dog påpeger EDBP, at undtagelsen i databeskyttelsesforordningens art 49, stk. 1, litra f ikke bør benyttes ved en CLOUD Act-anmodning, når der er tale om andre personers vitale interesse, idet dette bør imødekommes med en MLAT.[343] Det må på baggrund af EDPB's udtalelse og bestemmelsens ordlyd formodes, at der ikke kan ske overførsel på baggrund af en CLOUD Act-anmodning med hjemmel i databeskyttelsesforordningens art. 49, stk. 1, litra d, hvis der er tale om andre personers vitale interesser, men det må formodes, at der er en snæver mulighed for overførsel, hvis det omhandler den registreredes vitale interesser.

Derudover findes der i databeskyttelsesforordningens art. 49, stk. 1, 2. pkt. en interesse-afvejningsregel, som kan give mulighed for overførsel, hvis det er nødvendigt af hensyn til vægtige legitime interesser. EDPB anfører i den forbindelse, at denne interesseafvejningsregel er strengere end interesseafvejningsreglen i databeskyttelses-forordningens art. 6, stk. 1, litra f, grundet de strengere betingelser. Én betingelse er blandt andet, at den dataansvarlige skal underrette tilsynsmyndigheden samt den registrerede. Dette kan give problemer i henhold til den fortrolighed, som er påkrævet i henhold til CLOUD Act-anmodninger, idet de amerikanske myndigheder sigter mod at holde anmodningen hemmelig af hensyn til efterretningsaktiviteten. Endvidere finder EDPB, at det er vanskeligt for den dataansvarlige i praksis at overholde kravet om at give den registrerede de passende garantier. EDPB er af den opfattelse, at data-

[342] (EDPB's ANNEX, 2019), side 7
[343] (EDPB's ANNEX, 2019), side 7

beskyttelsesforordningens art. 49, stk. 1, 2. pkt. ikke kan udgøre et overførselsgrundlag, når der modtages CLOUD Act-anmodninger.[344]

Slutteligt påpeger EDPB, at de resterende bestemmelser i databeskyttelsesforordningen er relevante, navnlig databeskyttelsesforordningen art. 28, stk. 3, litra a angående instruks. EDPB går dog ikke nærmere ind i denne bestemmelse, men fastslår vigtigheden af denne bestemmelse.[345]

Opsummerende kan det udledes, at databeskyttelsesforordningens art. 49 kræver en grundig vurdering og er vanskelig at benytte som overførselsgrundlag, idet disse undtagelser har et snævert anvendelsesområde og skal fortolkes strengt. I særlige situationer må det på baggrund af ovenstående formodes, at databeskyttelsesforordningen art. 49, stk. 1, litra e og f kan anvendes som overførselsgrundlag for at imødekomme en CLOUD Act-anmodning. Endvidere kan det på baggrund af ovenstående udledes, at databeskyttelsesforordningens art. 49, stk. 1, litra d ikke kan benyttes som et gyldigt overførselsgrundlag for at imødekomme en CLOUD Act-anmodning. Derudover må det formodes, at interesseafvejningsreglen i databeskyttelsesforordningens art. 49, stk. 1, 2. pkt. heller ikke kan benyttes som overførsels-grundlag for at imødekomme en CLOUD Act-anmodning. Det betyder derfor, at hvis en dataansvarlig benytter en amerikansk cloudleverandør, der bliver mødt af CLOUD Act-anmodninger, må det formodes, at der lovligt kan ske overførsel på baggrund af databeskyttelsesforordningen art. 49, stk. 1, litra e og f i særlige situationer.[346]

10.2 KOMBIT-sagen

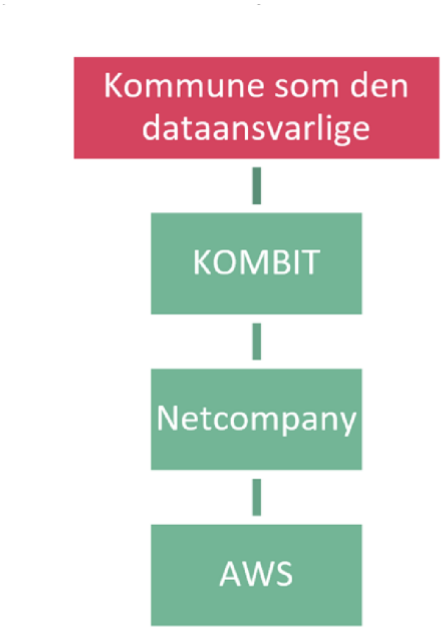
Nærværende afsnit vil analysere en konkret forespørgsel fra KOMBIT angående tilsigtede og utilsigtede overførsler til USA. Herudover vil analysen belyse vigtigheden af overførselsgrundlag, databehandleraftale og behandlingssikkerhed. I den henseende vil specialet sammenholde Datatilsynets udtalelser i KOMBIT-sagen med databeskyttelses-forordningen, chartret, tidligere retspraksis og juridisk litteratur.

[344] (EDPB's ANNEX, 2019), side 7
[345] (EDPB's ANNEX, 2019), side 8
[346] (EDPB's ANNEX, 2019), side 7 og 8

10.2.1 Sagens faktum

Datatilsynet har den 29. marts 2022 besvaret en konkret forespørgsel fra KOMBIT angående tilsigtede og utilsigtede overførsler til USA. Mere specifikt har KOMBIT forespurgt, hvorvidt det kan være en utilsigtet overførsel til et tredjeland, når AWS i databehandleraftalen forbeholder sig ret til at udlevere personoplysninger, såfremt de bliver mødt med en dommerkendelse fra en myndighed i et tredjeland.[347]

KOMBIT leverer et IT-system til kommunerne, kaldet Aula. KOMBIT benytter Netcompany som underdatabehandler og Netcompany benytter sig af AWS som underdatabehandler. I figuren nedenfor illustreres databehandlerkonstruktionen:[348]



10.2.2 Vedrørende tilsigtede og utilsigtede overførsler til tredjelande

I konkrete sag bliver personoplysningerne som udgangspunkt behandlet inden for EU/EØS, hvilket også fremgår af databehandleraftalen med AWS.[349] Endvidere fremgår det af databehandleraftalen, at KOMBIT selv vælger, hvor personoplysninger geografisk samles i et

[347] (Datatilsynet, Journalnummer: 2022-212-3529, 2022)
[348] (Datatilsynet, Journalnummer: 2022-212-3529, 2022)
[349] (Datatilsynet, Journalnummer: 2022-212-3529, 2022)

datacenter. Der er anført nedenstående formulering i standarddatabehandleraftale punkt 12.1:[350]

> *"12.1 Regions. Customer may specify the location(s) where Customer Data will be processed within the AWS Network, including the EU (Dublin) Region, the EU (Frankfurt) Region, the EU (London) Region and the EU (Paris) Region (each a "Region"). Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body. If the Standard Contractual Clauses apply, nothing in this Section varies or modifies the Standard Contractual Clauses."* (Datatilsynets fremhævning)

I dette tilfælde er Aula placeret i datacenteret Irland og AWS' behandling sker således herfra som udgangspunkt.[351] Problemstillingen, der bliver behandlet i sagen, vedrører det tilfælde, hvor AWS er forpligtet til at overføre personoplysninger til tredjelande, såfremt det er nødvendigt for at overholde lovgivning eller bindende myndighedsanmodning, jf. Datatilsynet fremhævning i ovenstående punkt 12.1.

I KOMBIT-sagen anfører Datatilsynet, at AWS kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, jf. databeskyttelses-forordningens art. 28, stk. 3, litra a. Herefter anfører Datatilsynet, at der i ovenstående punkt 12.1 i databehandleraftalen fremgår, at AWS må overføre personoplysninger til tredjelande, hvis det er *nødvendigt* for at overholde lovgivning eller en bindende ordre fra en offentlig myndighed. Hertil bemærker Datatilsynet, at denne formulering medfører, at den dataansvarlige har givet instruks til, at AWS kan overføre personoplysninger som følge af en myndighedsanmodning. I den forbindelse fastslår Datatilsynet, at det vil være en tilsigtet overførsel til et tredjeland, såfremt AWS imødekommer en myndighedsanmodning fra et tredjeland. Datatilsynets opfattelse i KOMBIT-sagen stemmer overens med Datatilsynets opfattelse i den nyere Chromebook-sag, hvor de ligeledes udtalte, at det vil være en tilsigtet overførsel, hvis cloudleverandøren overfører til USA, når cloudleverandøren har fået instruks via databehandleraftalen.[352] Datatilsynet har således ikke ændret sin opfattelse vedrørende tilsigtede og utilsigtede overførsler. Herudover kan det på baggrund af ovenstående udledes, at

[350] (Datatilsynet, Journalnummer: 2022-212-3529, 2022)
[351] (Datatilsynet, Journalnummer: 2022-212-3529, 2022)
[352] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)

AWS dermed ikke vil handle i strid med databehandleraftalen, hvis AWS imødekommer en myndighedsanmodning fra et tredjeland, og derved overfører personoplysninger til et tredjeland.[353]

Opsummerende kan det udledes, at det vil anses som en instruks og dermed en tilsigtet overførsel til tredjelande, såfremt databehandleraftalen indeholder en bestemmelse, som giver cloudleverandøren mulighed for at overføre til et tredjeland, når det er *nødvendigt* for at overholde lovgivning eller en bindende ordre fra en offentlig myndighed. Det betyder, at databeskyttelsesforordningens kapitel V skal iagttages, jf. nærmere herom i nedenstående afsnit.

10.2.3 Vedrørende overførselsgrundlag

I KOMBIT-sagen anfører Datatilsynet, at databeskyttelsesforordningens art. 48 ikke udgør et gyldigt overførselsgrundlag, såfremt der alene foreligger en afgørelse fra en domstol eller administrativ myndighed i et tredjeland. Det betyder således, at en anmodning fra en myndighed i et tredjeland aldrig vil være et gyldigt overførselsgrundlag i sig selv.[354]

Datatilsynets udtalelse i KOMBIT-sagen er i overensstemmelse med databeskyttelses-forordningens art. 48, hvor det fremgår, at der kan ske overførsel på baggrund af domme og afgørelser fra tredjelandets domstole og myndigheder, hvis der samtidig er en international aftale, eksempelvis en traktat om gensidig retshjælp. Dermed kan en myndighedsanmodning ikke i sig selv udgøre et gyldigt overførselsgrundlag i henhold til art. 48, hvilket EU-Kommissionen tillige har pointeret i forbindelse med Microsoft-sagen. Derudover har EU-Kommissionen i den henseende udtalt, at MLAT er den foretrukne løsning for disse overførsler.[355]

EDPB har tillige udtalt, at ved mangel af en international aftale, såsom MLAT, kan der ikke lovligt overføres personoplysningerne alene på baggrund af en myndighedsanmodning, navnlig en CLOUD Act-anmodning. Endvidere anfører EDPB, at i tilfælde af, at der er en MLAT mellem landene, bør europæiske dataansvarlige henvise til den eksisterende MLAT, således at

[353] (Datatilsynet, Journalnummer: 2022-212-3529, 2022)
[354] (Datatilsynet, Journalnummer: 2022-212-3529, 2022)
[355] (EDPB's ANNEX, 2019), side 3

overførslen sker i overensstemmelse med databeskyttelsesforordningen.[356] Flere europæiske lande har indgået en MLAT med USA via Konventionen om cyberkriminalitet, men de amerikanske myndigheder forsøger at omgå MLAT-processen ved at sende CLOUD Act-anmodningerne direkte til cloudleverandørerne.[357] Den amerikanske regering hævder, at MLAT er en langsommelig og kompleks proces, som tager længere tid at gennemføre og mener derfor, at problemet bliver løst ved vedtagelsen af CLOUD Act, som fremskynder processen for udlevering af personoplysninger.[358]

Opsummerende kan det udledes, at databeskyttelsesforordningens art. 48 ikke kan benyttes som et gyldigt overførselsgrundlag, når der alene overføres i medfør af en CLOUD Act-anmodning. Derimod skal de amerikanske myndigheder anmode om udlevering af personoplysningerne gennem MLAT-processen.

10.2.4 Databehandleraftalen og behandlingssikkerhed

Dernæst nævner Datatilsynet i KOMBIT-sagen, at i den situation, hvor cloudleverandøren udelukkende befinder sig i EU/EØS, men har moderselskab i USA, kan cloudleverandøren i EU/EØS blive mødt af myndighedsanmodninger fra USA. Det betyder derfor, at der vil ske en overførsel til USA, hvis anmodningen imødekommes. Hertil understreger Datatilsynet, at det er en grundlæggende forudsætning, at der ikke gives instruks til overførsel af personoplysninger til tredjelande i databehandleraftalen. Såfremt der ikke er givet instruks til overførsel i medfør af databehandleraftalen, vil det være i strid med databehandleraftalen, hvis cloudleverandøren imødekommer en CLOUD Act-anmodning og derfor være et spørgsmål om behandlingssikkerhed, jf. databeskyttelsesforordningens art. 32. Det fremgår af databeskyttelsesforordningens art. 32, at det både er den dataansvarlige og databehandleren, der skal sikre passende behandlingssikkerhed, således et tilstrækkeligt sikkerhedsniveau opretholdes.[359]

[356] (EDPB's ANNEX, 2019), side 3
[357] (Hemmings, Srinivasann, & Swire, 2020), side 674 og (U.S Department of Justice White Paper, 2019), side 2
[358] (U.S Department of Justice White Paper, 2019), side 3
[359] (Datatilsynet, Journalnummer: 2022-212-3529, 2022)

10.2.5 De tre opmærksomhedspunkter fra Datatilsynet

Herefter oplister Datatilsynet i KOMBIT-sagen en række opmærksomhedspunkter, som den dataansvarlige skal iagttage ved brugen af en databehandler, som kan blive mødt af myndighedsanmodninger. Først og fremmest skal den dataansvarlige sikre at cloudleverandøren kan og agter at overholde databeskyttelsesforordningen.[360] Opmærksomhedspunktet i KOMBIT-sagen er i overensstemmelse med Datatilsynets nyere udtalelse i Chromebook-sagen, hvor det fremgår, at en dataansvarlig udelukkende må anvende en cloudleverandør, der kan overholde databeskyttelsesforordningen.[361] Datatilsynet har således ikke ændret synspunkt i forhold til, at den dataansvarlige kun skal benytte en cloudleverandør, som kan overholde databeskyttelsesforordningen.

Dernæst anfører Datatilsynet i KOMBIT-sagen et andet opmærksomhedspunkt, som vedrører, at den dataansvarlige skal sørge for, at der er den nødvendige behandlingssikkerhed, jf. databeskyttelsesforordningens art. 32. I den henseende skal den dataansvarlige foretage en vurdering af, hvorvidt der er en risiko for, at cloudleverandøren vil imødekomme en myndighedsanmodning i strid med databehandleraftalen. Datatilsynets opmærksomhedspunkt er i overensstemmelse med databeskyttelsesforordningens art. 32, hvor det fremgår, at sikkerhedsforanstaltningerne skal fastlægges ud fra en risikobaseret tilgang. Det vil sige, at den dataansvarlige skal vurdere de potentielle konsekvenser ved at anvende en cloudleverandør, som kan blive mødt af myndighedsanmodning fra et tredjeland, og dermed foretage en utilsigtet ulovlig behandling i strid med databehandleraftalen.[362]

Slutteligt anfører Datatilsynet i KOMBIT-sagen et tredje opmærksomhedspunkt, som vedrører, at den dataansvarlige skal føre tilsyn med databehandleren og sikre, at cloudleverandøren overholder databehandleraftalen og dermed databeskyttelsesforordningen. I den forbindelse påpeger Datatilsynet, at i det tilfælde, hvor den dataansvarlige bliver bekendt med, at cloudleverandøren overfører til et tredjeland i strid med databehandleraftalen, skal den dataansvarlige reagerer straks.[363] I henhold til databeskyttelsesforordningens art. 28, stk. 3, litra h, skal databehandleren stille alle nødvendige oplysninger tilgængelige for den dataansvarlige,

[360] (Datatilsynet, Journalnummer: 2022-212-3529, 2022) og (Databeskyttelsesforordningen, 2016), artikel 28, stk. 1
[361] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[362] (Udsen, 2022), side 291
[363] (Datatilsynet, Journalnummer: 2022-212-3529, 2022) og (Datatilsynets Vejledning, 2024), side 12

hvilket skal fremgå af databehandleraftalen. På den måde kan den dataansvarlige sikre sig, at databehandleren overholder databeskyttelsesforordningen. Derudover sikrer udveksling af oplysninger, at den dataansvarlige er fuldt informeret om behandlingsaktiviteterne og kan således påvise, at behandlingen er i overensstemmelse med databeskyttelsesforordningen. Forpligtelsen til at føre tilsyn følger af databeskyttelsesforordningens art. 5, stk. 2, hvilket Datatilsynet ligeledes har lagt til grund i flere afgørelser, herunder afgørelsen som nævnt i afsnit 7.1.4 angående Styrelsen for International Rekruttering.[364]

Opsummerende kan det udledes, at Datatilsynet opstiller tre opmærksomhedspunkter, som en dataansvarlig skal iagttage, såfremt den dataansvarlige benytter sig af en cloudleverandør, som har moderselskab i USA og dermed kan være genstand for CLOUD Act-anmodninger. Her nævner Datatilsynet, at den dataansvarlig skal vælge en cloudleverandør, som kan efterleve forordningens krav. Derudover skal den dataansvarlige sørge for nødvendig behandlings-sikkerhed ud fra en risikobaseret tilgang samt føre tilsyn med, at cloudleverandøren overholder databehandleraftalen. Såfremt dette ikke er tilfældet, skal den dataansvarlige reagere straks. En efterlevelse af disse opmærksomhedspunkter medfører, at den dataansvarlige overholder databeskyttelsesforordningens krav og at de registreredes grundlæggende rettigheder sikres.[365]

10.3 Aktindsigten

Datatilsynet har efterfølgende den 30. maj 2022 været i dialog med KOMBIT angående Datatilsynets besvarelse, og denne dialog er der søgt aktindsigt i.[366] Som nævnt i afsnit 7.1 har Henrik Udsen anført, at ved brugen af amerikanske cloudleverandører, kan der opstå en tvivl i forhold til udlevering af oplysninger som følge af en CLOUD Act-anmodning. I den henseende mener Henrik Udsen, at den dataansvarlige *nok* skal få afklaret denne tvivl. I nærværende analyse vil det blive klarlagt, hvorvidt denne tvivl skal afklares af den dataansvarlige.

10.3.1 Ændringsforslag til databehandleraftalen

Efter dialogen med Datatilsynet har AWS, KOMBIT og Netcompany udarbejdet nogle ændringsforslag til den oprindelige standard-databehandleraftale for at få bestemmelserne i databehandleraftalen i overensstemmelse med databeskyttelsesforordningen.[367]

[364] (Datatilsynet Journalnummer: 2021-421-0102, 2021)
[365] (Datatilsynet, Journalnummer: 2022-212-3529, 2022)
[366] Aktindsigten (Bilag 1)
[367] Aktindsigten afsnit 1 (Bilag 1)

I ændringsforslaget er nedenstående formulering foreslået til punkt 2 i databehandleraftalen:[368]

> *"**2. Customer Instructions.** The parties agree that this Addendum and the Agreement (including Customer providing instructions via configuration tools such as the AWS management console and APIs made available by AWS for the Services) constitute Customer's documented instructions regarding AWS's processing of Customer Data ("Documented Instructions"). AWS will process Customer Data only in accordance with Documented Instructions (which if Customer is acting as a processor, could be based on the instructions of its controllers), including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by European Union or Member State law to which AWS is subject. [...]"* (Ændringsforslaget understreget af Datatilsynet)

Ovenstående ændringsforslag blev sendt til revidering hos Datatilsynet, som har udtalt sig i den forbindelse. Datatilsynets anfører, at det understregede ændringsforslag er identisk med databeskyttelsesforordningens art. 28, stk. 3, litra a, hvorefter databehandleren ikke kan fravige instruksen, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret. Dermed er denne formulering i overensstemmelse med databeskyttelsesforordningens art. 28, stk. 3, litra a.[369]

Datatilsynet har påpeget, hvilke bestemmelser i databehandleraftalen, der mangler yderligere afklaring og som stadig fremstår tvetydige og uklare. Dette er navnlig punkt 3 og 12.1 i databehandleraftalen, som ligeledes omhandler muligheden for overførsel til USA. Punkt 3 og 12.1 har følgende ordlyd:[370]

> *"**3. Confidentiality of Customer Data.** AWS will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to (i) maintain or provide the Services, or (ii) as ~~necessary to comply~~ with the law or a valid and binding order of a governmental body (such as a subpoena or court order), but only to the extent permitted by European Union or Member State law."* (Ændringsforslaget understreget af Datatilsynet)

[368] Ibid., afsnit 2
[369] Ibid., afsnit 2.2
[370] Ibid., afsnit 2.2

> *"**12.1 Regions.** Customer can specify the location(s) where Customer Data will be processed. within the AWS Network (each a "Region"), including Regions in the EEA. Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to (i) provide the Services initiated by Customer, or (ii) ~~as necessary to comply~~ with the law or binding order of a governmental body, but only to the extent permitted by European Union or Member State law."* (Ændringsforslaget understreget af Datatilsynet)

I KOMBIT-sagen anførte Datatilsynet, at det vil være en tilsigtet overførsel til USA, hvis AWS imødekommer en CLOUD Act-anmodning, hvis der er instruks hertil i databehandleraftalen. Såfremt det fremgår af databehandleraftalen, at der kan ske overførsel, når det er *nødvendigt* for at overholde lovgivning eller bindende ordre fra en offentlig myndighed, vil det være en tilsigtet overførsel. Hertil anførte Datatilsynet, at såfremt den dataansvarlige ikke ønsker, at der skal ske overførsel til USA, skal det fremgå af databehandleraftalen, at der ikke er givet instruks hertil.[371] Efterfølgende har KOMBIT, AWS og Netcompany udarbejdet et ændringsforslag, som forsøger at fjerne instruksen til overførsel til USA. Ovenfor kan det ses, at formuleringen i punkt 3 og 12.1, "*as necessary to comply"* er fjernet, og i stedet har de foreslået, at der skal stå *"but only to the extent permitted by European Union or Member State law.*"[372] På den måde mener parterne, at databehandleraftalen ikke indeholder en instruks til overførsel til USA.

Dog anfører Datatilsynet, at punkt 3 og 12.1 sammenholdt med punkt 2 i databehandleraftalen, skaber en uklarhed, idet ordlyden ikke er identisk. I den forbindelse pointerer Datatilsynet, at der er en fortolkningstvivl. AWS har dog udtalt, at disse formuleringer ikke er indholdsmæssigt forskellige.[373]

Datatilsynet bemærker at *"uklare eller tvetydige bestemmelser i aftalegrundlaget mellem den dataansvarlige og dennes databehandlere, der kan give anledning til fortolkningstvivl, som en altovervejende hovedregel skal undgås."*[374] Hertil fastlægger Datatilsynet, at ordlyden i punkt 2, 3 og 12.1 i databehandleraftalen skal være identisk, således at der ikke opstår en fortolkningstvivl. Endvidere præciserer Datatilsynet, at fortolkningstvivlen konkret består i

[371] (Datatilsynet, Journalnummer: 2022-212-3529, 2022)
[372] Aktindsigten afsnit 2.2 (Bilag 1)
[373] Ibid.
[374] Aktindsigten afsnit 2 (Bilag 1)

ordvalget *påkrævet* som nævnt i punkt 2[375] og *tilladt* som nævnt i punkt 3 og 12.1.[376] Ordvalget skal være identisk, hvilket betyder, at punkt 3 og 12.1 skal ændre ordlyden til *påkrævet*.[377]

Datatilsynet udtalelse i aktindsigten om, at det skal være ordet *påkrævet*, som skal anvendes i databehandleraftalen fremfor ordet *tilladt*, er i overensstemmelse med databeskyttelses-forordningens art. 28, stk. 3, litra a, som har samme ordlyd. Datatilsynet har i Chromebook-sagen udtalt, at den dataansvarlige ikke kan begrunde den manglende overholdelse af databeskyttelsesforordningen med, at det er en standard-databehandleraftale udarbejdet af cloudleverandøren.[378] Datatilsynet har endvidere anført i den nyeste Chromebook-afgørelse fra 2024, at databehandleraftalen skal gøres mere gennemskuelig.[379] Dette hænger også sammen med principperne i databeskyttelsesforordningens art. 5, stk. 1. Datatilsynet fastholder dermed deres opfattelse af, at databehandleraftaler skal indeholde klare og gennemskuelige bestemmelser, som ikke kan medføre en fortolkningstvivl. Dette vil være med til at sikre, at databeskyttelsesforordningen overholdes.

10.3.2 Sammenfatning

Som nævnt i starten af dette kapitel, har der tidligere i litteraturen været en usikkerhed i forhold til, hvorvidt den dataansvarlige skal få afklaret fortolkningstvivl i databehandleraftalen, navnlig når tvivlen angår cloudleverandørens udlevering af personoplysningerne til de amerikanske myndigheder i medfør af amerikansk lovgivning.[380]

Som det fremgår af databeskyttelsesforordningens art. 28, stk. 1, skal den dataansvarlige udelukkende benytte sig af en databehandler, som kan overholde forordningen. Den dataansvarlige skal dermed sikre, at cloudleverandøren ikke handler i strid med data-behandleraftalen.[381] Såfremt der er uklare bestemmelser i databehandleraftalen, kan det være en svær vurdering af, hvorvidt cloudleverandøren har handlet i strid med databehandleraftalen eller ej. På baggrund af analysen af aktindsigten kan det konstateres, at uklare og tvetydige bestemmelser i databehandleraftalen som altovervejende hovedregel skal undgås.[382] For at

[375] på engelsk *required*
[376] på engelsk *permitted*
[377] på engelsk *required*
[378] (Datatilsynet Journalnummer: 2023-431-0001, 2024)
[379] (Datatilsynet Journalnummer: 2023-431-0001, 2024)
[380] (Udsen, 2022), side 105 og 106
[381] (Datatilsynet, Journalnummer: 2022-212-3529, 2022)
[382] Aktindsigten afsnit 2 (Bilag 1)

undgå fortolkningstvivl i databehandleraftalen skal ordlyden i bestemmelserne være identiske.[383] Endvidere skal ordlyden ændres til *påkrævet at overføre i henhold til EU-ret eller medlemsstaternes nationale ret*, hvis den dataansvarlige ikke ønsker, at der skal ske overførsel til USA i medfør af en CLOUD Act-anmodning. Det vil være en tilsigtet overførsel, såfremt ordlyden i bestemmelserne vedrørende muligheden for overførsel til USA er enten ordet *tilladt at overføre* eller *nødvendigt at overføre* som følge af lovgivning eller en ordre fra en offentlig myndighed.[384]

Konsekvensen ved at udarbejde en databehandleraftale med uklare og tvetydige bestemmelser er, at cloudleverandøren kan fraskrive sig en del af ansvaret i og med det fremstår uklart, om cloudleverandøren har fået instruks til overførslen. Den dataansvarlige er ansvarlig for overtrædelse af databeskyttelsesforordningen, og cloudleverandørens ansvar er begrænset til den behandling af personoplysninger, som foretages i strid med instruksen, jf. databeskyttelsesforordningens art. 82, stk. 2. Det vil formentlig sige, at såfremt der fremgår en fortolkningstvivl i databehandleraftalen, der fortolkes som en instruks til at overføre på baggrund af en myndighedsanmodning, vil cloudleverandøren ikke handle i strid med instruksen, hvis anmodning imødekommes. Dermed vil cloudleverandøren være fri fra ansvar.[385] Dog må cloudleverandøren kun efterleve lovlige instrukser, og idet databeskyttelsesforordningens art. 48 tilsiger, at en CLOUD Act-anmodning ikke i sig selv udgør et gyldigt overførselsgrundlag, vil dette ikke i sig selv være et lovlig overførselsgrundlag. Det påhviler *formentlig* både den dataansvarlige og databehandleren at sikre, at der tilvejebringes et lovligt overførselsgrundlag, jf. databeskyttelsesforordningens art. 44. Dog kan der i særlige situationer være mulighed for at overføre på baggrund af en CLOUD Act-anmodning i henhold til databeskyttelsesforordningens art. 49, stk. 1, litra e og f.

10.4 Delkonklusion

På baggrund af kapitel 10 kan det konstateres, at den amerikanske lovgivning CLOUD Act kan pålægge cloudleverandører at udlevere personoplysninger til de amerikanske myndigheder. Personoplysningerne skal i henhold til CLOUD Act udleveres uanset, hvor de befinder sig, hvis personoplysningerne blot er inden for cloudleverandørens *besiddelse, varetægt eller kontrol.* Når cloudleverandøren modtager en dommerkendelse fra en uafhængig domstol i

[383] Ibid., afsnit 2.2
[384] Ibid., afsnit 2.2
[385] (Databeskyttelsesforordningen, 2016), artikel 82, stk. 2

USA, kan der opstå modstridende juridiske forpligtelser, da databeskyttelsesforordningen begrænser udleveringen af personoplysningerne.[386]

I henhold til databeskyttelsesforordningens art. 48 kan en sådan dommerkendelse ikke anerkendes i sig selv, og udgør derfor ikke et lovligt overførselsgrundlag. Det betyder, at såfremt cloudleverandøren overfører til USA, som følge af en CLOUD Act-anmodning, vil det ikke være i overensstemmelse med databeskyttelsesforordningen. Det vil dog være tilladt at overføre til USA, hvis der er en international aftale (MLAT) samt en dom eller afgørelse afsagt af en domstol.[387] Dette kan tillige udledes af Datatilsynets udtalelse i KOMBIT-sagen.[388]

Databeskyttelsesforordningens art. 49 har et snævert anvendelsesområde og skal fortolkes strengt. I særlige situationer må det formodes, at såfremt den dataansvarlige benytter en amerikansk cloudleverandør, der bliver mødt af CLOUD Act-anmodninger, kan der i snævre tilfælde lovligt kan ske overførsel på baggrund af databeskyttelsesforordningen art. 49, stk. 1, litra e og f. Derudover kan det udledes, at databeskyttelsesforordningens art. 49, stk. 1, litra d ikke kan benyttes som et gyldigt overførselsgrundlag for at imødekomme en CLOUD Act-anmodning. Interesseafvejningsreglen i databeskyttelsesforordningens art. 49, stk. 1, 2. pkt. kan heller ikke benyttes som overførselsgrundlag for at imødekomme en CLOUD Act-anmodning.[389]

Som følge af Datatilsynets konstateringer i aktindsigten kan det udledes, at den tidligere usikkerhed i litteraturen formentlig, er afklaret. Datatilsynet har klart udtrykt, at uklare og tvetydige bestemmelser i databehandleraftalen som altovervejende hovedregel skal undgås.[390] Endvidere har Datatilsynet i den seneste Chromebook-sag fra 2024 fastholdt synspunktet om, at databehandleraftaler med cloudleverandører skal gøres mere gennemskuelige.[391]

[386] Nærmere herom i afsnit 10.1.1
[387] (Databeskyttelsesforordningen, 2016), artikel 48
[388] Nærmere herom i afsnit 10.1.4
[389] Nærmere herom i afsnit 10.1.5
[390] Aktindsigt afsnit 2 og 2.2 (Bilag 1)
[391] (Datatilsynet Journalnummer: 2023-431-0001, 2024)

11. Perspektivering

FISA 702 skulle fornyes inden den 19. april 2024, hvorfor den amerikanske regering skulle tage stilling til, om denne lovgivning skulle forlænges eller udgå. I sidste øjeblik, den 20. april 2024, underskrev Joe Biden en forlængelse af FISA 702, hvilket betyder, at denne lovgivning fortsætter i 2 år yderligere.[392] Det er ikke blot en forlængelse af den oprindelige problematiske overvågningslovgivning, men en udvidelse af FISA 702. Udvidelsen indebærer, at begrebet *electronic communication service provider* er udvidet fra at omfatte udbydere af elektroniske kommunikationsudbydere til nu at omfatte *enhver* virksomhed, som blot har en adgang til kommunikationsudstyr og data, heriblandt virksomheder der har adgang til wi-fi, routere og servere. Det vil sige, at det allerede brede begreb, som omfattede enhver *electronic communication service provider*, er udvidet, hvorefter flere amerikanske virksomheder kan blive pålagt at overvåge for de amerikanske myndigheder. Udvidelsen medfører, at eksempelvis frisører, fitnesscentre, byggemarkeder, kan blive tvunget til at overvåge på vegne af de amerikanske myndigheder.[393]

Årsagen til at den amerikanske regering vil forlænge og udvide FISA 702 skyldes, at de vil sikre USA ved at opdage alvorlige nationale sikkerhedstrusler. Forlængelsen og udvidelsen af FISA 702 vil give større adgang til overvågning og bedre beskyttelse af USA.[394] Udvidelsen og forlængelsen af FISA 702 er dog problematisk i forhold til EU-borgeres databeskyttelse.[395]

Som det blev fastslået i Schrems I og II er FISA 702 en problematisk lovgivning, som giver de amerikanske myndigheder adgang til personoplysninger uden en dommerkendelse. De to problematikker, som blev fremstillet i Schrems I og II, var 1) at der ikke var en effektiv klageadgang og 2) at efterforskningsaktiviteterne ikke var begrænset til, hvad der var nødvendigt og proportionalt for efterretningsaktiviteterne.[396] Disse problematikker er imødekommet i den nye certificeringsordning Data Privacy Framework. Dette imødekommes ved E.O. 14086, som indeholder sikkerhedsforanstaltninger, der sikrer EU-borgernes grundlæggende rettigheder. E.O. 14086 sikrer først og fremmest, at en klage bliver undersøgt

[392] (Fazliu, 2024) ” *USA siger ja til stor spionlov: Danske organisationer bør genoverveje partnerskaber med amerikanske tjenester”* og (Olifent, USA forlænger kontroversiel og »utrolig farlig« spionlov i sidste time, 2024)
[393] (Have, 2024), ”*Truslen fra amerikansk overvågning stiger*” og (H.R 7888, 2024), Section 25
[394] (House, 2024)
[395] (Have, 2024), ”*Truslen fra amerikansk overvågning stiger*”
[396] Nærmere herom i afsnit 9.1.2 og 9.1.4

af CLPO, og hvis CLPO's undersøgelse er utilfredsstillende, kan der klages til den uafhængige klagemekanisme DPRC, hvilket er i overensstemmelse chartret art. 47. Desuden sikrer E.O. 14086, at efteretningsaktiviteter kun kan forekomme, såfremt det er nødvendigt, legitimt og proportionelt for efterforskningen, hvilket er i overensstemmelse chartret art. 52. På den baggrund blev Data Privacy Framework vedtaget af EU-Kommissionen i juli 2023, jf. databeskyttelsesforordningens art. 45, stk. 1.[397]

Der kan imidlertid stilles spørgsmålstegn ved, hvorvidt udvidelsen og forlængelsen af FISA 702 vil have en indvirkning på gyldigheden af Data Privacy Framework. Maximilian Schrems er påbegyndt planlægningen af en Schrems III afgørelse, hvor han har anført kritikpunkter til Data Privacy Framework.

For det første mener Maximillian Schrems ikke, at E.O. 14086 med ordet *proportionelt* sikrer, at overvågningen er *proportionel* ud fra EU-rettens forståelse af ordet *proportionelt*, jf. chartrets art. 52. Men overvågningen er derimod *proportionel* ud fra den amerikanske fortolkning af ordet. Endvidere bemærker Maximillian Schrems, at den amerikanske fortolkning af ordet *proportionelt* ikke er offentliggjort.[398]

For det andet mener Maximillian Schrems, at den klageadgang, som er opdelt i to henholdsvis CLPO og DPRC, kun er en mindre forbedring, men stadig ikke er i overensstemmelse med chartrets art. 47. Maximillian Schrems begrunder dette med, at DPRC ikke er en domstol, men en delvis uafhængig udøvende myndighed. Hertil bemærker Maximillian Schrems, at EU-borgere ikke vil have nogen interaktion med de nye organer, idet de skal sende klagen til den nationale tilsynsmyndighed og bliver ikke hørt i USA. Endvidere har USA nægtet at give EU-borgere grundlæggende rettigheder, som svarer til chartrets art. 7, 8 og 47.[399]

Som nævnt er FISA 702 for nylig blevet forlænget, og i den forbindelse mener Maximillian Schrems, at dette vil være det perfekte tidspunkt at forbedre den amerikanske lovgivning, således at den er i overensstemmelse med EU-retten. Slutteligt pointerer Maximillian Schrems, at EU/EØS og USA gennem tiden har haft aftaler såsom Safe Harbor, Privacy Shield og Data

[397] (Databeskyttelsesforordningen, 2016), artikel 45, stk. 1
[398] (noyb, European Commission gives EU-US data transfers third round at CJEU, 2023), "*European Commission gives EU-US data transfers third round at CJEU"*
[399] Ibid.

Privacy Framework, men der er ikke sket en væsentlig ændring af den amerikanske overvågningslovgivning. Maximillian Schrems mener, at det er nødvendigt for, at EU-borgeres grundlæggende rettigheder kan sikres, således de er i overensstemmelse med chartret. Maximillian Schrems er derfor i gang med forberedelserne til en Schrems III-afgørelse.[400]

Data Privacy Framework skal evalueres inden længe for at vurdere, hvorvidt de nye tiltag i den amerikanske lovgivning er effektiv i praksis.[401] Det bliver interessant at følge med i om der opstår en Schrems III afgørelse, som erklærer Data Privacy Framework ugyldig. Det bliver ligeledes spændende at følge evalueringen af Data Privacy Framework og få konstateret, hvorvidt den amerikanske lovgivning er effektiv i praksis.

12. Konklusion

Databehandleraftalen skal opfylde minimumskravene, som er fastsat i databeskyttelses-forordningens art. 28, stk. 3, litra a-h for at overholde databeskyttelsesforordningen. Specialet har haft særligt fokus på de minimumskrav, der har størst indflydelse på, hvorvidt de amerikanske myndigheder kan få adgang personoplysningerne, jf. databeskyttelses-forordningens art. 28, stk. 3, litra a, c, d og h.

Databeskyttelsesforordningens art. 28, stk. 3, litra a indeholder et krav om, at databehandler-aftalen skal fastlægge, at cloudleverandøren kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige. Dette kan kun fraviges, hvis det kræves i henhold til EU-ret eller medlemsstaternes nationale ret. I det tilfælde, hvor cloudleverandøren handler uden for den fastsatte instruks, vil cloudleverandøren blive selvstændig dataansvarlig for den del af behandling, jf. databeskyttelsesforordningens art. 28, stk. 10. Dette medfører, at cloudleverandøren skal overholde krav som en dataansvarlig. Dog er den oprindelige dataansvarlige stadig ansvarlig i medfør af databeskyttelsesforordningens art. 82, 83 og 84. Dette skyldes, at den dataansvarlige skal vælge en cloudleverandør, som efterlever databeskyttelsesforordningens krav.[402]

[400] Ibid. og (Olifent, Mens Biden og von der Leyen smiler, er Schrems III allerede i støbeskeen, 2022)
[401] (Datatilsynet, EDPB udpeger repræsentanter til evaluering af aftale mellem EU og USA, 2024)
[402] (Udsen, 2022), side 119 og (Datatilsynet, Journalnummer: 2022-212-3529, 2022)

Derudover fremgår det af databeskyttelsesforordningens art. 28, stk. 3, litra c, at databehandleraftalen skal fastsætte sikkerhedsforanstaltninger som nævnt i databeskyttelsesforordningens art. 32. Det påhviler både den dataansvarlige og cloudleverandøren at gennemføre foranstaltninger ud fra en risikobaseret tilgang. Et eksempel på en sikkerhedsforanstaltning er kryptering, som fremgår af databeskyttelsesforordningens art. 32, stk. 1, litra a.

Herudover fremgår det af databeskyttelsesforordningens art. 28, stk. 3, litra d, at databehandleraftalen skal fastsætte, at cloudleverandøren kun må gøre brug af underdatabehandlere ved forudgående, specifik eller generel godkendelse fra den dataansvarlige, jf. databeskyttelsesforordningens art. 28, stk. 2. Endvidere skal det fremgå af databehandleraftalen, at cloudleverandøren skal udarbejde en databehandleraftale med sine underdatabehandlere, hvor de samme vilkår skal gøres gældende overfor underdatabehandlerne.[403]

Slutteligt er databeskyttelsesforordningens art. 28, stk. 3, litra h relevant, idet der stilles krav om, at databehandleraftalen skal indeholde oplysninger om, hvor hyppigt og på hvilken måde udvekslingen af oplysninger mellem cloudleverandøren og den dataansvarlige skal foregå. Derudover pålægges cloudleverandøren at give den dataansvarlige mulighed for at foretage revisioner, således den dataansvarlige kan føre kontrol med, at cloudleverandøren overholder databeskyttelsesforordningen og databehandleraftalen. Dette følger af kravet om ansvarlighed i databeskyttelsesforordningens art. 5, stk. 2.

Den dataansvarlige sikrer, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen, når der anvendes en cloudleveandør med underdatabehandlere i USA ved at udarbejde en databehandleraftale, som er i overensstemmelse med databeskyttelsesforordningens art. 28, stk. 3. Den dataansvarlige kan ikke undgå at blive ansvarlig for manglende overholdelse af forordningen med den begrundelse, at der benyttes en standard-databehandleraftale udarbejdet af cloudleverandøren.[404] Såfremt cloudleverandøren har underdatabehandler i USA, skal forordningens kapitel V iagttages og i den forbindelse skal der sikres et gyldigt overførselsgrundlag, jf. databeskyttelsesforordningens art. 44. Denne forpligtelse gælder formentlig både den dataansvarlige og cloudleverandøren.[405] På baggrund

[403] (Databeskyttelsesforordningen, 2016), artikel 28, stk. 4
[404] (Datatilsynet Journalnummer: 2023-431-0001, 2024)
[405] (Udsen, 2022), side 112 og (Datatilsynet, Journalnummer: 2020-431-0061, 2022)

af analyserne i specialet kan det udledes, at databeskyttelsesforordningens art. 46, stk. 2, litra c kan benyttes som et gyldigt overførselsgrundlag, såfremt der ikke foreligger en tilstrækkelighedsafgørelse. Databeskyttelsesforordningens art. 46, stk. 2, litra c er dog betinget af, at der er et tilstrækkeligt beskyttelsesniveau. Det betyder, at det er et beskyttelsesniveau, der i det *væsentligste* svarer til niveauet i EU/EØS. Dette blev fastslået i Schrems I og II, hvor det blev påpeget, at et manglende tilstrækkeligt beskyttelsesniveau var i strid med chartrets art. 7, 8, 47 og 52. Schrems II fastslog, at Privacy Shield ikke sikrede et tilstrækkeligt beskyttelsesniveau grundet den amerikanske lovgivning, FISA 702 og EO 12 333. Disse lovgivninger var i henhold til EU-Domstolen i strid med chartrets art. 47 og 52, idet der ikke var adgang til domstolsprøvelse for EU-borgerne, og overvågningen var ikke begrænset til det strengt nødvendige.[406] I Chromebook-sagen konstaterede Datatilsynet, at disse amerikanske lovgivninger medfører, at standardbestemmelserne i henhold til databeskyttelsesforordningens art. 46, stk. 2, litra c ikke kan anvendes uden supplerende foranstaltning. Hertil konstaterede Datatilsynet, at ved anvendelse af kryptering, er det en nødvendighed, at kryptering er effektiv, således at der ikke overføres personoplysninger i klartekst til USA.[407]

Datatilsynet har til Region Syddanmarks forespørgsel udtalt, at samme regler gælder ved benyttelse af Microsoft. Desuden udtaler Datatilsynet, at databeskyttelsesforordningen ikke forbyder brugen af cloudleverandører, men at den dataansvarlige er forpligtet til at kunne dokumentere, at personoplysningerne bliver behandlet i overensstemmelse med forordningen, jf. databeskyttelsesforordningens art. 5, stk. 2.[408]

Den dataansvarlige kan ligeledes sikre, at databeskyttelsesforordningen overholdes ved anvendelse af en cloudleverandør med underdatabehandlere i USA ved at benytte databehandlere, der er certificeret under Data Privacy Framework.[409] Såfremt denne tilstrækkelighedsafgørelse bliver erklæret ugyldig, kan databeskyttelsesforordningens art. 46, stk. 2, litra c anvendes som overførselsgrundlag, hvis der anvendes supplerende foranstaltninger. På den måde vil den dataansvarlige sikre, at anvendelsen af cloudleverandører med underdatabehandlere i USA er i overensstemmelse med databeskyttelsesforordningen.

[406] (Schrems II C-311/18, 2020), præmis 201
[407] (Datatilsynet, Journalnummer: 2020-431-0061, 2022)
[408] (Datatilsynet, Journalnummer: 2023-431-0012, 2024)
[409] (Data Privacy Framework, 2024)

En anden måde den dataansvarlige kan sikre overholdelse af databeskyttelsesforordningen ved brug af en cloudleverandør er, at den dataansvarlige helt fravælger, at cloudleverandøren må benytte underdatabehandlere i tredjelande. Dette skal klart fremgå af databehandleraftalen, jf. databeskyttelsesforordningen 28, stk. 3, litra d, jf. art. 28, stk. 2. Det vil formentlig afskrække cloudleverandøren i at benytte en underdatabehandler i et tredjeland, hvis der ikke er givet tilladelse hertil, idet cloudleverandøren vil blive selvstændig dataansvarlig for denne del af behandling, jf. databeskyttelsesforordningens art. 28, stk. 10.

En anden problematik som den europæiske dataansvarlige kan stå overfor, er den amerikanske lovgivning, CLOUD Act. Af specialet kan det udledes, at den amerikanske lovgivning CLOUD Act ligeledes kan pålægge cloudleverandørerne at udlevere personoplysninger til de amerikanske myndigheder. I henhold til CLOUD Act skal personoplysningerne udleveres uanset, hvor de befinder sig, hvis blot det er inden for cloudleverandørens *besiddelse, varetægt eller kontrol*. De amerikanske myndigheder får personoplysningerne med hjemmel i CLOUD Act ved at anmode om en dommerkendelse hos en uafhængig domstol i USA.[410] En sådan dommerkendelse anerkendes ikke i sig selv i henhold til databeskyttelsesforordningens art. 48 og udgør derfor ikke et lovligt overførselsgrundlag. Dette kan tillige udledes af Datatilsynet udtalelse i KOMBIT-sagen, hvor de henviser til bestemmelsens ordlyd.[411]

I særlige situationer må det formodes, at såfremt den dataansvarlige benytter en amerikansk cloudleverandør, der bliver mødt af CLOUD Act-anmodninger, kan der lovligt ske overførsel på baggrund af databeskyttelsesforordningens art. 49, stk. 1, litra e og f. Dog kan det udledes, at databeskyttelsesforordningens art. 49, stk. 1, litra d ikke kan benyttes som et gyldigt overførselsgrundlag for at imødekomme en CLOUD Act-anmodning. Endvidere kan interesseafvejningsreglen i databeskyttelsesforordningens art. 49, stk. 1, 2. pkt. heller ikke benyttes som overførselsgrundlag for at imødekomme en CLOUD Act-anmodning.[412]

Den dataansvarlige kan sikre, at en amerikansk cloudleverandør ikke udleverer person-oplysninger som følge af en CLOUD Act-anmodning i medfør af en instruks ved at fjerne instruksen hertil i databehandleraftalen. På baggrund af Datatilsynets konstateringer i akt-

[410] Kapitel 10
[411] (Datatilsynet, Journalnummer: 2022-212-3529, 2022)
[412] (EDPB's ANNEX, 2019), side 7 og 8

indsigten, vil instruksen blive fjernet ved, at ordlyden ændres til *påkrævet at overføre i henhold til EU-ret eller medlemsstaternes nationale ret*, hvis den dataansvarlige ikke ønsker, at der skal ske overførsel til USA i medfør af en CLOUD Act-anmodning. Det vil derimod være en tilsigtet overførsel, såfremt ordlyden i bestemmelserne vedrørende muligheden for overførsel til USA er enten ordet *tilladt at overføre* eller *nødvendigt at overføre* som følge af lovgivning eller en ordre fra en offentlig myndighed.[413]

På baggrund af Datatilsynets konstateringer i aktindsigten, kan det tillige udledes, at den tidligere uklarhed i litteraturen i forhold til, hvorvidt den dataansvarlige skal få afklaret fortolkningstvivl, er formentlig afklaret. Datatilsynet har klart udtrykt, at fortolkningstvivl i databehandleraftalen som alt overvejende hovedregel skal undgås.[414] Det kan således slutteligt konstateres, at den dataansvarlige kan undgå, at cloudleverandøren udleverer person-oplysninger til de amerikanske myndigheder ved at lave en databehandleraftale med klare og gennemskuelige bestemmelser, således der ikke forekommer fortolkningstvivl. Denne fortolkningstvivl kan undgås i databehandleraftalen ved, at ordlyden i bestemmelserne er identiske.[415]

[413] Aktindsigten afsnit 2.2 (Bilag 1)
[414] Ibid., afsnit 2
[415] Ibid., afsnit 2.2

13. Litteraturliste

Allingstrup, M. (5. Februar 2016). *Snowdens kæmpelæk: Afslørede USA's massive overvågning.* Hentet 13. maj 2024 fra DR: https://www.dr.dk/nyheder/viden/tech/snowdens-kaempelaek-afsloerede-usas-massive-overvaagning

Andersen, K. B. (Oktober 2023). Hvornår er en fysisk person ”identificeret eller identificerbar” i GDPR’s forstand? *Juristen*.

Blume, P. (2018). *Den nye persondatarets aktører* (1 udg.). København K: Jurist- og Økonomiforbundets Forlag.

Blume, P. (2020). *Retssystemet og juridisk metode* (4 udg.). København K : Djøf Forlag.

CLOUD Act. (Marts 2018). *DIVISION V—CLOUD ACT.* Hentet 13. maj 2024 fra justice.gov: https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf

Data Privacy Framework. (2024). *Data Privacy Framework*. Hentet 13. maj 2024 fra Data Privacy Framework: https://www.dataprivacyframework.gov/list

Databeskyttelsesforordningen. (27. April 2016). *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*. Hentet fra eur-lex.europa: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679

Datatilsynet. (22. Maj 2023). *Bøde på 1,2 milliarder euro til Meta Irland som følge af bindende afgørelse fra EDPB.* Hentet 13. maj 2024 fra Datatilsynet: https://www.datatilsynet.dk/internationalt/internationalt-nyt/2023/maj/boede-paa-12-millarder-euro-til-meta-irland-som-foelge-af-bindende-afgoerelse-fra-edpb

Datatilsynet. (15. Februar 2024). *EDPB udpeger repræsentanter til evaluering af aftale mellem EU og USA.* Hentet 13. maj 2024 fra Datatilsynet: https://www.datatilsynet.dk/internationalt/internationalt-nyt/2024/feb/edpb-udpeger-repraesentanter-til-evaluering-af-aftale-mellem-eu-og-usa

Datatilsynet. (7. Maj 2024). *EU-U.S. Data Privacy Framework*. Hentet 7. maj 2024 fra Datatilsynet: https://www.datatilsynet.dk/internationalt/eu-us-data-privacy-framework-

Datatilsynet. (24. April 2024). *Nye klageformularer vedrørende overførsler til USA*. Hentet 13. maj 2024 fra Datatilsynet: Nye klageformularer vedrørende overførsler til USA

Datatilsynet Journalnummer: 2019-442-3996. (19. December 2019). *Databehandlers behandling af personoplysninger uden for instruks*. Hentet 13. maj 2024 fra Datatilsynet: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2019/dec/databehandlers-behandling-af-personoplysninger-uden-for-instruks

Datatilsynet Journalnummer: 2021-421-0102. (16. December 2021). *Tilsyn med Styrelsen for International Rekrutterings tilsyn med to databehandlere*. Hentet 13. maj 2024 fra Datatilsynet: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/dec/tilsyn-med-styrelsen-for-international-rekrutterings-tilsyn-med-to-databehandlere

Datatilsynet Journalnummer: 2023-431-0001. (30. Januar 2024). *Datatilsynet giver påbud i Chromebook-sag*. Hentet 13. maj 2024 fra Datatilsynet: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/datatilsynet-giver-paabud-i-chromebook-sag

Datatilsynet, Journalnummer: 2010-52-0138. (3. Februar 2011). *Datatilsynet*. Hentet 12. maj 2024 fra Behandling af følsomme personoplysninger i cloud-løsning: https://www.datatilsynet.dk/afgoerelser/historiske-afgoerelser/2011/feb/behandling-af-foelsomme-personoplysninger-i-cloud-loesning

Datatilsynet, Journalnummer: 2020-431-0061. (14. Juli 2022). *Datatilsynet nedlægger behandlingsforbud i Chromebook-sag*. Hentet 13. maj 2024 fra Datatilsynet: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-nedlaegger-behandlingsforbud-i-chromebook-sag-

Datatilsynet, Journalnummer: 2022-212-3529. (29. Marts 2022). *Datatilsynet*. Hentet 12. maj 2024 fra Vedrørende tilsigtede eller utilsigtede overførsler til tredjelande: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/vedroerende-tilsigtede-eller-utilsigtede-overfoersler-til-tredjelande

Datatilsynet, Journalnummer: 2023-31-0007. (29. April 2024). *Kritik af Telmore A/S' behandling af personoplysninger*. Hentet 13. maj 2024 fra Datatilsynet: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/apr/kritik-af-telmore-as'-behandling-af-personoplysninger

Datatilsynet, Journalnummer: 2023-431-0012. (15. Februar 2024). *Region Syddanmarks påtænkte brug af Microsoft 365*. Hentet 13. maj 2024 fra Datatilsynet: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/feb/region-syddanmarks-paataenkte-brug-af-microsoft-365

Datatilsynets Journalnummer: 2022-431-0167. (7. Februar 2022). *Alvorlig kritik: underdatabehandler afviste at udlevere oplysninger til den dataansvarlige*. Hentet 13. maj 2024 fra Datatilsynet: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/feb/alvorlig-kritik-underdatabehandler-afviste-at-udlevere-oplysninger-til-den-dataansvarlige

Datatilsynets vejledning. (Oktober 2021). *Vejledning om tilsyn med databehandlere*. Hentet 13. maj 2024 fra Datatilsynet: https://www.datatilsynet.dk/Media/637710957381234368/Datatilsynet_Vejledning%20om%20tilsyn%20med%20databehandlere_oktober-2021.pdf

Datatilsynets Vejledning. (April 2024). *Vejledning om overførsel til tredjelande*. Hentet 13. maj 2024 fra Datatilsynet: https://www.datatilsynet.dk/Media/638478180234447566/Vejledning%20om%20overførsel%20til%20tredjelande.pdf

Datatilsynets Vejledning om cloud. (Marts 2022). *Vejledning om cloud*. Hentet 13. maj 2024 fra Datatilsynet: https://www.datatilsynet.dk/Media/637824109172292652/Vejledning%20om%20cloud.pdf

Den Europæiske Unions charter . (1. December 2009). *Den Europæiske Unions charter om grundlæggende rettigheder*. Hentet 13. maj 2024 fra eur-lex.europa: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=celex%3A12016P%2FTXT

Diamond, P. (25. September 2020). *Skylager kontra servere i det lokale miljø: Ni ting, som du bør være opmærksom på*. Hentet 13. maj 2024 fra Microsoft: https://www.microsoft.com/da-dk/microsoft-365/business-insights-ideas/resources/cloud-storage-vs-on-premises-servers

EDPB Henstilling nr. 01/2020. (18. Juni 2021). *Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger*. Hentet 13. maj 2024 fra edpb.europa: https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_da.pdf

EDPB's ANNEX. (10. Juli 2019). *ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence.*

Hentet 13. maj 2024 fra EDPB: https://www.edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf

EDPB's Retningslinjer 05/2021. (14. Februar 2023). *Retningslinjer 05/2021 om samspillet mellem anvendelsen af artikel 3 og bestemmelserne om internationale overførsler i henhold til kapitel V i GDPR*. Hentet 13. maj 2024 fra EDPB.europa: https://www.edpb.europa.eu/system/files/2023-09/edpb_guidelines_05-2021_interplay_between_the_application_da.pdf

EDPB's Retningslinjer 07/2020 . (7. juli 2021). *Retningslinjer 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse*. Hentet 13. maj 2024 fra edpb.europa: https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_da.pdf

EDPS. (11. Marts 2024). *European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies*. Hentet 13. maj 2024 fra edps.europa: https://www.edps.europa.eu/system/files/2024-03/EDPS-2024-05-European-Commission_s-use-of-M365-infringes-data-protection-rules-for-EU-institutions-and-bodies_EN.pdf

EU-Kommissionen. (10. Juli 2023). *Questions & Answers: EU-US Data Privacy Framework*. Hentet 13. maj 2023 fra ec.europa.eu: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

Europa-Parlamentet og Rådets direktiv 95/46/EF. (24. Oktober 1995). *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*. Hentet 13. maj 2024 fra eur-lex.europa: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=celex%3A31995L0046

EU-traktaten. (artikel 6). *Folketinget*. Hentet 13. maj 2024 fra Artikel 6 EU: Grundlæggende rettigheder: https://www.eu.dk/da/dokumenter/traktater/traktaten-eu/afsnit-l/artikel-6

Executive Order 14086. (7. Oktober 2022). *Executive Order 14086*. Hentet 13. maj 2024 fra Federal register: https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities

Fazliu, Q. (26. April 2024). *USA siger ja til stor spionlov: Danske organisationer bør genoverveje partnerskaber med amerikanske tjenester.* Hentet 13. maj 2024 fra Computerworld: https://www.computerworld.dk/art/287034/usa-siger-ja-til-stor-

spionlov-danske-organisationer-boer-genoverveje-partnerskaber-med-amerikanske-tjenester

Generaladvokat, Y. Bot. (23. September 2015). *FORSLAG TIL AFGØRELSE FRA GENERALADVOKAT Sag C-362/14*. Hentet 13. maj 2024 fra curia.europa: https://curia.europa.eu/juris/document/document.jsf?docid=168421&doclang=DA

Google Workspace. (19. Marts 2024). *AppScheet Subprocessors*. Hentet 13. maj 2024 fra Google Workspace: https://workspace.google.com/intl/en/terms/subprocessors/

Grundloven. (§ 20). *Folketinget.* Hentet 13. maj 2024 fra Folketinget: https://www.ft.dk/da/dokumenter/bestil-publikationer/publikationer/mingrundlov/min-grundlov/kapitel-3/paragraf-20

Hamer, C. R., & Schaumburg-Müller, S. (2020). *Juraens verden: metoder, retskilder og discipliner* (1 udg.). København K: Djøf Forlag.

Hassan, A. (30. September 2023). *Top 20 Cloud Computing Companies in USA*. Hentet 7. maj 2024 fra yahoo!finance: https://finance.yahoo.com/news/top-20-cloud-computing-companies-075236760.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJhoJHgZqzOFoFxlFwIGODcXYUK3RNSB4i3QcG7tl6zbiMpUEnmmGbk7aBa3qvtvOM-yBKD3A203h-xwK74m1RD_7e8ABNk

Hassan, A. (30. September 2023). *Top 20 Cloud Computing Companies in USA*. Hentet 7. maj 2024 fra yahoo!finance: https://finance.yahoo.com/news/top-20-cloud-computing-companies-075236760.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJhoJHgZqzOFoFxlFwIGODcXYUK3RNSB4i3QcG7tl6zbiMpUEnmmGbk7aBa3qvtvOM-yBKD3A203h-xwK74m1RD_7e8ABNk

Have, C. (26. April 2024). *Truslen fra amerikansk overvågning stiger.* Hentet 13. maj 2024 fra ITwatch: https://itwatch.dk/Klummer/article17056199.ece

H.R 7888. (20. April 2024). *To reform the Foreign Intelligence Surveillance Act of 1978.* Hentet 13. maj 2024 fra Congress.gov: https://www.congress.gov/bill/118th-congress/house-bill/7888/text

Høilund, D. (2022). *Persondataret* (4 udg.). København: Hans Reitzels Forlag.

Hemmings, J., Srinivasann, S., & Swire, P. (2020). *Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act.*

House, W. (20. April 2024). *Statement from National Security Advisor Jake Sullivan on the Senate's Vote on the Reauthorization and Reform of FISA Section 702.* Hentet 13. maj 2024 fra White House: https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/20/statement-from-national-security-advisor-jake-sullivan-on-the-senates-vote-on-the-reauthorization-and-reform-of-fisa-section-702/

Jensen, D. (24. November 2023). *Tre leverandører sidder på 65 procent af markedet: Her er verdens største cloud-leverandører lige nu*. Hentet 7. maj 2024 fra Computerworld: https://www.computerworld.dk/art/285200/tre-leverandoerer-sidder-paa-65-procent-af-markedet-her-er-verdens-stoerste-cloud-leverandoerer-lige-nu

Jones, E. (7. September 2023). *Cloud markedsandel: et kig på cloud økosystemet i 2024*. Hentet 13. maj 2024 fra kinsta: https://kinsta.com/dk/blog/cloud-markedsandel/

Kommissionens beslutning af 26. juli 2000. (26. Juli 2000). *Kommissionens beslutning af 26. juli 2000 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af safe harbor-principperne til beskyttelse af privatlivets fred og de dertil hørende*. Hentet 13. maj 2024 fra eur-lex.europa: https://eur-lex.europa.eu/legal-content/da/ALL/?uri=CELEX%3A32000D0520

KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2016. (12. Juli 2016). *KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2016/1250 af 12. juli 2016 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred*. Hentet 13. maj 2024 fra eur-lex.europa: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016D1250&from=EN

MEDDELELSE FRA KOMMISSIONEN. (27. November 2013). *MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET Genopbygning af tilliden til datastrømmene mellem EU og USA*. Hentet 13. maj 2024 fra eur-lex.curopa: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0846:FIN:DA:PDF

Mortensen, H. (2018). *Sikkerhedsforanstaltninger - i henhold til databeskyttelsesforordningen*. Hentet 13. maj 2024 fra Karnov: https://pro.karnovgroup.dk/b/documents/7000820104

Motzfeldt, H. M. (2022). *Grundlæggende databeskyttelsesret* (1 udg.). København K: Djøf Forlag.

Munk-Hansen, C. (2018). *Den juridiske løsning* (1 udg.). København K: Jurist- og Økonomiforbundets Forlag.

Nasdaq. (13. Maj 2024). *Nasdaq-100 Companies*. Hentet 13. maj 2024 fra https://www.nasdaq.com/solutions/nasdaq-100/companies

Nielsen, K. K., & Lotterup, A. (2020). *Databeskyttelsesforordningen og databeskyttelsesloven* (1 udg.). København K: Jurist- og Økonomiforbundets Forlag.

Nielsen, R., & Tvarnø, C. D. (2021). *Retskilder og retsteorier* (6 udg.). København K: Jurist- og Økonomforbundet Forlag.

noyb. (10. Juli 2023). *European Commission gives EU-US data transfers third round at CJEU*. Hentet 13. maj 2024 fra noyb: https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu

noyb. (u.d.). *Data Transfers*. Hentet 13. maj 2024 fra noyb: https://noyb.eu/en/project/eu-us-transfers

Olifent, L. (25. April 2022). *Mens Biden og von der Leyen smiler, er Schrems III allerede i støbeskeen*. Hentet 13. maj 2024 fra Version2: https://www.version2.dk/artikel/mens-biden-og-von-der-leyen-smiler-er-schrems-iii-allerede-i-stoebeskeen

Olifent, L. (23. April 2024). *USA forlænger kontroversiel og »utrolig farlig« spionlov i sidste time*. Hentet 13. maj 2024 fra Version2: https://www.version2.dk/artikel/usa-forlaenger-kontroversiel-og-utrolig-farlig-spionlov-i-sidste-time

Schrems I C-362/14. (6. Oktober 2015). *EU-Domstolen*. Hentet 13. maj 2024 fra curia.europa: https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=1854253

Schrems II C-311/18. (16. Juli 2020). *EU-Domstolen*. Hentet 13. maj 2024 fra curia.europa: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=1855891

Swire, P., & Paul , G. (19. Juli 2020). *NEW DEVELOPMENTS FOR THE U.K. AND AUSTRALIAN EXECUTIVE AGREEMENTS WITH THE U.S. UNDER THE CLOUD ACT*. Hentet 13. maj 2024 fra Cross-Border Data Forum: https://www.crossborderdataforum.org/new-developments-for-the-u-k-and-australian-executive-agreements-with-the-u-s-under-the-cloud-act-2/

TEUF. (u.d.). *Den Europæiske Unions Tidende, artikel 288.* Hentet 13.maj 2024 fra eur-lex.europa: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=celex%3A12016E288

U.S Department of Justice White Paper. (April 2019). *The Purpose and Impact of the CLOUD Act*. Hentet 13. maj 2024 fra www.justice.gov/CLOUDAct: https://www.justice.gov/d9/pages/attachments/2019/04/10/doj_cloud_act_white_paper_2019_04_10.pdf

U.S.C § 1881a . (u.d.). *U.S.C § 1881a - Procedures for targeting certain persons outside the United States other than United States persons.* Hentet 13. maj 2024 fra Legal Information Institute: https://www.law.cornell.edu/uscode/text/50/1881a

U.S.C § 2703. (u.d.). *18 U.S. Code § 2703 - Required disclosure of customer communications or records.* Hentet 13. maj 2024 fra Cornell Law School: https://www.law.cornell.edu/uscode/text/18/2703

Udsen, H. (2022). *Databeskyttelsesret* (1 udg.). www.databeskyttelsesret.dk.

Vejledning til anvendelse af cloud. (2020). *Vejledning til anvendelse af cloud*. Hentet 13. maj 2024 fra Digitaliseringsstyrelsen: https://digst.dk/data/vejledning-til-anvendelse-af-cloudservices/