En undersøgelse af retsstillingen omkring tredjelandsoverførsler ved anvendelse af amerikanske cloudtjenester set i lyet af Schrems II-dommen.

Kandidatspeciale

Jakob Bjørn Sørensen
Studie nr.: 20165369

Titelblad

Titel	En undersøgelse af retsstillingen omkring overførsler til tredjelande ved anvendelse af amerikanske cloudtjenester set i lyet af Schrems II-dommen.
Engelsk titel	An investigation on the legal status of transfers to third countries when using American cloud services in the light of the Schrems II-ruling
Forfatter	Jakob Bjørn Sørensen
Studieretning	Jura
Fagområde	Persondataret
Semester	10. semester
Universitet	Aalborg Universitet (AAU)
Vejleder	Tanja Kammersgaard Christensen
Afleveret	12. maj 2022
Anslag inkl. mellemrum (eksl. forside, fodnoter, titelblad, abstract, indholdsfortegnelse og litteraturliste)	141.092

Abstract

This paper will describe the investigation of cross border transfers from the EU/EEA to the U.S. by virtue of the usage of American cloud service providers, such as Microsoft, Google and Amazon. It will revolve around how data exporters, subject to the General Data Protection Regulation ("GDPR"), can continue to use American cloud services even though these are subject to U.S. surveillance laws, including FISA 702, EO 12.333 and CLOUD Act, seen in the light of the infamous CJEU judgment in the Schrems II case.

The investigation is carried out by the author by applying the legal dogmatic method as the purpose of the investigation is to describe the current legal status within this field. To achieve this purpose, the investigation entails an analysis and explanation of the Schrems II-ruling. This will be used to gain a full understanding of the interpretation and application of the GDPR, where personal data is being processed by a data processor in the U.S on behalf of a data controller in the EU/EEA.
Based on the ruling, EDPB released their recommendations on supplementary measures, which constitutes a valuable and decisive interpretative contribution for this investigation. The recommendations are used during the investigation to apply in a fictional scenario, created by the author, to put the recommendations in to the context of a somewhat "normal" data exporter within the EU/EEA, which are using American cloud service providers for various purposes.
Furthermore, decisions taken by various supervisory authorities within the EU will be subject to a discussion aiming to clarify whether - and how - the continued usage of American cloud providers is possible within the law.

The investigation does conclude that some lawful use cases of American cloud services exist, however not without the functionality of these services being significantly limited to storage purposes only. Furthermore, it concludes that there's still a fair amount of uncertainty within this field due to the lack of a uniform application of the GDPR across the EU/EEA.

Indholdsfortegnelse

1. Indledning

1.1Præsentation af emne

I en hastigt udviklende digitalisering af det globale samfund har vi siden årtusindskiftet været vidne til en eksplosion i mængden af personoplysninger som behandles, ikke blot af myndigheder og offentlige institutioner, men især også af private aktører. Dette er bestemt ingen undtagelse i EU, og i Danmark især, hvor digitaliseringen af den offentlige- og private sektor har grebet om sig. Vores personoplysninger indsamles, behandles, opbevares og sågar sælges af så mange forskellige aktører, at man i EU har set sig nødsaget til at regulere dette felt yderligere. Reguleringen er Persondataforordningen, eller *the General Data Protection Regulation* (herefter benævnt "GDPR"), der trådte i kraft den 25. maj 2018, som har givet indehavere af egne personoplysninger, ejerskab og (med)bestemmelse over sine egne personoplysninger. Blandt aktørerne der behandler og opbevare vores personoplysninger er nogle af verdens største udbydere af cloudtjenester så som Microsoft, Google og Amazon[1]. Disse firmaer er hyppigt brugt indenfor både det private og det offentlige i Danmark og resten af EU. Mange europæiske aktører er afhængige af disse tjenester til opbevaring, hosting og andre kritiske funktioner for deres IT-infrastruktur.

GDPR har været et ambitiøst skridt imod større retssikkerhed og tryghed for borgere når deres personoplysninger behandles og opbevares af denne slags aktører. Virksomheder og myndigheder bruger mange ressourcer på at efterleve kravene[2], da der ved brud på reglerne kan være tale om bøder på op mod 4% af virksomhedernes globale omsætning, jf. GDPR, art. 83, stk. 5. Efterlevelsen af reglerne i GDPR er derfor blevet en vital del af en seriøs forretning, som ikke kan ignoreres af ledelser og bestyrelser. Ikke desto mindre er det ikke altid en nem opgave, at sikre efterlevelsen af kravene da der er tale om en lov der kræver en kontinuerlig aktiv indsats for at sikre efterlevelse. Til hjælp herfor kan offentlige- og private aktører blandt andet læse i vejledninger fra de nationale tilsynsmyndigheder og retspraksis fra Den Europæiske Unions Domstol (herefter benævnt "EU-Domstolen"), selvom retspraksis indenfor netop GDPR, fortsat forekomme lidt tyndt sammenlignet med andre retsområder, hvilket blandt andet skyldes, at GDPR i sin nuværende form er relativt ny[3].

En af de helt store udfordringer, som virksomhederne er stødt på efter GDPR's introduktion i maj 2018 har været overførslen af personoplysninger til USA. Dette emne blev især højaktuelt i kølvandet på den såkaldte Schrems II-afgørelse fra EUD afsagt den 16. juli 2020. Emnet er desuden fortsat mere aktuelt end nogensinde i denne periode, hvor denne afhandling er udarbejdet, da problematikken som var omdrejningspunktet i Schrems II-sagen fortsat er eksisterende. Ganske vist omhandlede sagen Facebook Irelands overførsel af personoplysninger til moderselskabet, Facebook Inc. I USA, men problematikken er også aktuel for de førnævnte udbydere af cloudtjenester, som alle har base i USA.
De juridiske-, faktuelle- og tekniske detaljer bliver belyst i kapitel 2, men for at give en indledende forståelse af problematikken, bør det kort bemærkes at dommen gjorde den hidtidige Privacy

[1] https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/
[2] https://legaljobs.io/blog/gdpr-statistics/
[3] Se metodeafsnit/retskildeværdi-afsnit for uddybende bemærkninger om omkring retskilder indenfor persondataretten.

Shield-afgørelse ugyldig. Dette var ellers et overførselsgrundlag, som mange amerikanske og europæiske aktører havde baseret sine tredjelandsoverførsler til USA på.
EU-Domstolen fastslog dog i forbindelse med Schrems II-dommen, at overførsel baseret på standardkontraktbestemmelser, jf. GDPR, art. 46, stk. 2, litra c), fortsat er muligt, såfremt man sikrer sig at modtagerlandets beskyttelsesniveau kan garantere en databeskyttelse der i det væsentlige er tilsvarende den beskyttelse, som efter GDPR. EU-Kommissionen (herefter benævnt "Kommissionen") har således også siden domsafsigelsen offentliggjort nye standardkontraktsbestemmelser, som tager højde for problematikkerne i Schrems II-dommen. Standardkontraktsbestemmelser kan dog ikke stå alene og bør suppleres af yderligere for at sikre den fornødne beskyttelse for de registrerede og deres personoplysninger.
Problematikken drejede sig især om at lovgivning omkring amerikansk national sikkerhed, er problematisk ud fra et privatlivssynspunkt og således uforeneligt med rettigheder som følger af EU-Chartret (herefter benævnt "Chartret") og GDPR.
For at sådanne overførsler kan ske lovligt skal private- og offentlige aktører i EU implementere supplerende foranstaltninger der i realiteten fjerner den risiko der er for, at personoplysningerne bliver genstand for den problematiske lovgivning i USA. Disse foranstaltninger og den juridiske vurdering der leder frem til dem, er ikke nogen simpel øvelse og netop derfor er denne problemstilling interessant ud fra både et juridisk men også et - for mange virksomheder - praktisk synspunkt.

1.2 Problemformulering

Specialets problemformulering kommer derfor til at lyde som følger:

Hvordan kan overførsel af personoplysninger til usikre tredje lande ved brug af amerikanske cloudtjenester, ske i overensstemmelse med GDPR med særligt henblik på Schrems II-dommen?

1.3 Uddybende bemærkninger til problemformulering

Problemformuleringen søger først og fremmest at analysere Schrems II-dommen med to formål for øje. Det første er, at sagens fakta på plads og få en forståelse for omstændighederne og handlingsforløbet. Det andet er at analysere, hvordan EUD anvender og fortolker GDPR samt Chartret henset til sagens faktum. Det er især, de ting som EUD lægger særlig vægt på, som er interessant for specialets videre behandling, da dette kan udgøre et fortolkningsbidrag i aktørernes vurderinger af tredjelandets lovgivning.

Desuden søger problemformuleringen at finde ud af hvilke juridiske overvejelser og vurderinger man som dataeksportør skal foretage sig, såfremt man anvender en amerikansk leverandør af cloudtjenester og dermed i teorien foretager overførsler af personoplysninger til et tredjeland. Dette vil på trods af et klart juridisk islæt også indebærer overvejelser om de praktiske omstændigheder og teknologiske værktøjer der er tilgængelig på denne tid.
Endeligt lægger problemstillingen op til en vurdering af retstilstanden, som den er på tidspunktet for specialets udarbejdelse henset til praksis, vejledninger fra tilsynsmyndigheder mv.

1.4 Afgrænsning

Det lægges til grund i specialet, at læseren har indgående kendskab til GDPR og de overordnede principper heri. Enkelte bestemmelser, vil være redegjort for, da det er vurderet, at disse er særligt vigtige for forståelsen af resten af specialet. Det forventes desuden at læseren har en grundlæggende indsigt i informationsteknologiske begreber, koncepter og konstellationer så som cloudtjenester, hosting, kryptering og deslige.
Specialets fokusområde er afgrænset til en specifik del af persondataretten, som konkret kun tager stilling til enkelte bestemmelser i kapitel V af GDPR og beskæftiger sig således ikke med andet udover enkelte bestemmelser, som er relevant for diskussionen omkring retstilstanden, herunder eksempelvis art. 83. Det bør desuden også bemærkes, at specialet alene tager sigte på overførsel af personoplysninger til USA i forbindelse med brug af amerikanske cloudtjenester så som Microsoft produkter, Google produkter og Amazon produkter. Ingen af vurderingerne tager således sigte på andre usikre tredjelande end USA, selvom termen "usikkert tredjeland" eller blot "tredjeland" kan optræde flere steder i nærværende fremstilling. Årsagen til dette findes i at USA er det klart vigtigste land når det kommer til cloudtjenester som anvendes af private- og offentlige aktører i EU. Desuden bunder problematikken i Schrems-dommene udelukkende i amerikanske overvågningslove, da disse vedrører Facebook, som har base i USA.

Specialet rækker ind i det amerikanske retssystem, da enkelte amerikanske love har særlig relevans både for analysen af Schrems II-dommen, men især også den efterfølgende vurderingsfremgangsmåde, som er udarbejdet af EDPB. Specialet tager dog ikke stilling til retskildeværdi, rangfølge af lovgivning og lignende i USA, da dette forudsætter indgående kendskab til det amerikanske juridiske system. I øvrigt bør det bemærkes, at det i afsnit 3.2.2.3 alene vil være *electronic communication service providers* (herefter "ECSP"), jf. 50 U.S.C. § 1881(b)(4)(b) der vil blive behandlet. Henset til afsnittets fokusområde er diskussionen om *remote computing services,* jf. 50 U.S.C. § 1881(b)(4)(c) også relevant, men er undladt på baggrund af nærværende fremstillings tilladte omfang. Behandlingen af ECSP-begrebet alene, er dog også tilstrækkeligt til at demonstrere den relevante fremgangsmåde, der er afsnittets fokusområde og vurderingen ville ligeledes komme til samme konklusion.

Henset til GDPR kapitel V's overførselsgrundlag, er der alene anvendt standardkontraktsbestemmelser, jf. GDPR, art. 46, stk. 2, litra c). Årsagen er, at de øvrige overførselsgrundlag kun er mulige og relevante i et mere begrænset omfang, i modsætning til standardkontraktsbestemmelserne, som der i udgangspunktet kan bruges af alle aktører. Desuden er standardkontraktsbestemmelserne formentlig også det mest brugte overførselsgrundlag[4]. Ydermere er det også dette overførselsgrundlag, som der er særlig relevant i Schrems II-dommen. På trods af dette valg, vil specialet dog ikke gå i dybden med, hvad de nye standardkontraktsbestemmelser konkret indeholder, da det henset til problemformuleringen, er

[4] Vejledning: Overførsel af personoplysninger til tredjelande, Juli 2021, 3. udgave, Datatilsynet

mere relevant at kigge på supplerende foranstaltninger, som skal støtte disse, med henblik på at udgøre et effektivt overførselsgrundlag.

Endeligt bør det også bemærkes, at nærværende fremstilling ikke tager stilling til de undtagelser der findes i GDPR, art. 49, til at kunne foretage en tredjelandsoverførsel i særlige situationer. Problemformuleringen tager ikke sigte på særlige situationer, men snarere generel anvendelse af amerikanske cloudtjenester.

Tidsmæssigt er indholdet af nærværende fremstilling begrænset til at inkludere praksis, nyheder og lignende, som er blevet offentliggjort senest 12. maj 2022, hvor nærværende fremstilling er endeligt færdiggjort og afleveret.

1.5 Metode

Formålet med specialet og dettes problemformulering er, at forsøge at konkludere noget om hvad retstilstanden er lige nu (*de lege lata)*, indenfor persondataretten omkring tredjelandsoverførsler til USA med særligt henblik på anvendelsen af cloudtjenester udbudt af amerikanskbaserede leverandører.
For at kunne beskrive retstilstanden på et givent område indenfor juraen, kan man anvende den retsdogmatiske metode. Den retsdogmatiske metode anvendes her, da der inddrages en bred vifte af retskilder (og andre kilder) til at konkludere noget om retstilstanden. Det er således ikke alene GDPR og anden lovgivning, men i høj grad retspraksis fra EUD samt en række vejledninger og anbefalinger fra EDPB og nationale tilsynsmyndigheder. Sådanne kilder ville ikke altid have relevans ved andre retsområder, hvor man eksempelvis ofte vil anvende den juridiske metode. Indenfor mange andre retsområder vil man anse denne slags kilder for irrelevante eller med en meget svag retskildeværdi. Persondataretten er dog lidt speciel i denne henseende, da man forlader sig på en række retskilder og kilder, som man ikke traditionelt tillægger meget vægt. Eksempelvis ville man i en straffesag næsten udelukkende interesserer sig for straffeloven og nærliggende lovgivning og således sjældent eller aldrig inddrage branchesædvane, vejledninger eller lignende af gode grunde. Indenfor persondataretten anvender man dog en række andre kilder som fortolkningsbidrag. Disse kilder kan netop også anvendes til at sige noget om retstilstanden her og nu. Den retsdogmatiske metode søger at beskrive, fortolke og systematisere gældende ret[5] og alt imens en sådan formulering kan virke højtflyvende og abstrakt, så er det netop det, som nærværende fremstilling søger at gøre. Retsområdet er i en hastig udvikling pga. den teknologiske udvikling og opdaterede vejledninger, anbefalinger mv. er derfor særdeles vigtige for forståelsen, fortolkningen og anvendelsen af den primære retskilde, GDPR. Derfor vil nærværende fremstilling anvende den retsdogmatiske metode for at kunne belyse problemstillingen tilstrækkeligt til at kunne konkludere noget[6].

For at anvende den retsdogmatiske metode efter de videnskabeligt korrekte principper vil specialet inddrage dokumentation og kilder der, så objektivt som muligt, belyser forskellige vinkler og holdninger på den problemstilling som undersøges. Forskelligartetheden af kilderne anvendt i

[5] https://denstoredanske.lex.dk/retsdogmatik
[6] Hamer og Schaumburg-Müller (2020), 1. udgave, Juraens Verden, side 265ff.

nærværende fremstilling giver anledning til en vurdering af de forskellige kilders retskildeværdi. Dog bør det også bemærkes at enkelte kilder kan forekomme forudindtaget og sådanne kilder anvendes da også udelukkende til at argumentere for- og imod enkelte synspunkter relateret til diskussioner i nærværende fremstilling.

1.5.1 Retskilder og retskildeværdi

1.5.1.1 Lovgivning

Det overordnede lovgrundlag indenfor i persondataretten er GDPR, som er en sekundær EU-retskilde. Det vil sige den slags lovgivning der er afledt af de primære EU-retskilder. Primær ret er traktatgrundlaget i EU. I nærværende fremstilling anvendes Chartret, som kategoriseres om primær ret, da den har samme juridiske værdi, som traktatgrundlaget, jf. art. TEU, art. 6, stk. 1[7]. Det bør bemærkes at Databeskyttelsesloven også, nationalt, regulerer persondataretten, men har ringe relevans i forbindelse med nærværende fremstillings fokusområde da det, som førnævnt, primært er GDPR's kapitel V der har relevans her og da der ikke er noget særligt nationalt islæt henset til problemformuleringen. Forordninger er bindende direkte i medlemsstaterne uden implementering og har således en tungtvejende retskilde.

1.5.1.2 EU-Retspraksis

Retspraksis fra EU er en væsentlig retskilde i nærværende fremstilling. Problemformuleringen og motivationen for at behandle netop dette emne udspringer fra EUD's dom i Schrems II-sagen. Det er netop denne dom der skal hjælpe til at forklare de faktuelle såvel som de juridiske aspekter ved brugen af amerikanske cloudtjenester og den tredjelandsoverførsel der sker i forbindelse med denne brug.
Da GDPR kun har været gældende i knap 4 år er mængden af relevant retspraksis selvsagt begrænset. Der er dog intet i vejen for at inddrage retspraksis fra GDPR's forgænger, Direktiv 95/46, men henset til problemformuleringens fokusområde, har det kun været relevant at inddrage en kort gennemgang af Schrems I-dommen for at give en fuld forståelse for kompleksiteten og problematikken i Schrems II-dommen.

1.5.1.3 Afgørelser fra nationale tilsynsmyndigheder

Afgørelser fra medlemslandenes nationale tilsynsmyndigheder indgår, som bidrag til diskussioner omkring nuværende retstilstand, endog i begrænset omfang. Der optræder enkelte afgørelser fra blandt andet den franske tilsynsmyndighed, *CNIL*, og den østrigske tilsynsmyndighed, Datenschutzbehörde, mens der også er sammenholdt med afgørelser fra Datatilsynet, endog også i begrænset omfang. Netop den franske tilsynsmyndighed er også en af de mere fremtrædende og toneangivende tilsynsmyndigheder i EU. Henset til, at GDPR er en forordning, bør anvendelsen og fortolkningen af GDPR gerne være nogenlunde identisk i de forskellige medlemslande, hvorfor retskildeværdien af denne slags afgørelser også kan tillægges en vis vægt. Afgørelserne bidrager ikke til nogle afgørende konklusioner i nærværende fremstilling men anvendes alene til at belyse nogle problematikker med relevans til problemformuleringen[8].

[7] Hamer og Schaumburg-Müller (2020), 1. udgave, Juraens Verden, side 139ff.
[8] Hamer og Schaumburg-Müller (2020), 1. udgave, Juraens Verden, side 271.

1.5.2 Øvrige kilder

Forfatteren af nærværende fremstilling er bestemt ikke den første til at forsøge at analysere og fortolke på EUD's domsafsigelse i Schrems II-sagen. Blandt andet har EDPB udgivet to sæt anbefalinger baseret på netop denne dom. Dertil har Datatilsynet også udgivet vejledninger, som i det væsentligste relaterer sig til praksis på baggrund af denne dom. Disse bruges i varierende grad, men vil blive beskrevet nærmere i det følgende. Omkring disse kilder bør det bemærkes, at disse ikke er retskilder, som dem der er beskrevet ovenfor. Disse kaldes *bløde retskilder* eller *soft law* og indebærer "*retskilder, der principielt ikke er bindende, men som i realiteten har betydning*"[9]. Selvom der er tale om soft law og dermed i udgangspunktet ringe retskilde værdi, bør det konstateres, at soft law er en vigtig retskilde i persondataretten. Årsagen hertil er, at det er EDPB og tilsynsmyndighederne, som udgiver vejledninger mv., som er udarbejdet på baggrund af GDPR og retspraksis fra EUD. Nationale retsinstanser og andre der praktiserer loven, anvender denne type retskilder i deres arbejde til at forstå, anvende og fortolke GDPR[10].

1.5.2.1 Vejledninger

Der anvendes to vejledninger vedtaget af EDPB i nærværende fremstilling. Den der anvendes klart mest, er *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, som man som dataeksportør bør gennemgå for at sikre lovligheden af sin overførsel[11]. Den vil i det følgende blive omtalt som *roadmappet*.
Den anden vejledning – *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures* - vedrører konkret det tredje skridt i roadmappet og kan anvendes til at afgøre om et tredjelands lovgivning svarer til det som er påkrævet efter EU-retten henset de registreredes rettigheder[12]. Om retskildeværdien af disse, anføres det blandt andet i anbefaling nr. 43 i roadmappet, at disse anbefalinger er en "*referential standard*" og at de stammer fra "*…EU law and the jurisprudence of the CJEU and the ECtHR, which is binding on EU Member States*"[13]. Denne vejledning vil ikke blive dybdegående gennemgået i nærværende fremstilling, henset til undersøgelsens tilladte omfang, men de 4 principper indgår i vurderingen flere steder[14].

Den førstnævnte af de to vejledninger anvendes i stort omfang og danner således rammen om hele vurderingen og diskussionen i hele afsnit 3.2. Den anden vejledning anvendes i et relativt begrænset omfang.
Vejledningerne – eller anbefalingerne som de også kaldes – tillægges i nærværende fremstilling stor vægt. EDPB består af lederne af alle medlemslandenes tilsynsmyndigheder, Den Europæiske Datatilsynsførende og en præsentant for Kommissionen, som træffer deres anbefalinger i forening. Desuden har EDPB en vigtig rolle i arbejdet med at føre tilsyn med anvendelsen af GDPR i

[9] Hamer og Schaumburg-Müller (2020), 1. udgave, Juraens Verden, side 269.
[10] Hamer og Schaumburg-Müller (2020), 1. udgave, Juraens Verden, side 269f.
[11] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
[12] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures
[13] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures
[14] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

EU samt at rådgive Kommissionen i anliggender indenfor persondataretten. Disse anbefalinger og udtalelser udgør den opfattelse og holdning, som EDPB har til et givent emne og dette tillægges vægt hos aktører der praktiserer loven i EU[15]. Derfor er EDPB's roadmap en bærende retskilde for nærværende fremstillings forsøg på at beskrive retstilstanden.

På nationalt niveau offentliggør tilsynsmyndighederne også vejledninger – typisk på baggrund af EDPB's anbefalinger og vejledninger. På denne måde får man også oversat det til det nationale sprog og således lettere forståeligt og anvendeligt stof for medlemslandenes virksomheder, borgere og offentlige aktører. Datatilsynet har udgivet vejledninger på baggrund af EDPB's roadmap efter Schrems II-dommen. Den der har haft særlig relevans for nærværende fremstilling er dets *Vejledning om cloud* (herefter "cloudvejledningen")[16], som har været anvendelig i undersøgelsens vurdering af konkrete foranstaltninger, som kunne træffes, som supplement til overførselsgrundlaget. Tilsynsmyndighedernes udgivelser kan ofte være af mere specifik karakter end EDPB's og kan derfor tjene som godt grundlag til at inddrage konkrete eksempler, løsningsmuligheder og lignende fra det virkelige liv. Desuden er Datatilsynets cloudvejledning også udkommet i marts 2022 og kan således også sige noget om hvor udviklingen har båret sig hen siden EDPB's anbefalinger blev udgivet[17]

1.5.2.2 Udtalelser

Enkelte steder i nærværende fremstilling er der også anvendt udtalelser af forskellig karakter. Den første er en ekspertudtalelse med (såkaldt *Expert Opinion*) indhentet af Datenschutzkonferenz (herefter "DSK"), som er en sammenslutning af samtlige tyske databeskyttelsesmyndigheder. Ekspertudtalelsen blev indhentet for at belyse en række problemstillinger og uklare forhold omkring amerikansk sikkerhedslovgivning[18]. I denne fremstilling anses denne for at have samme retskildeværdi, som hvis et lignende dokument var offentliggjort af Datatilsynet bortset fra sproget, som er engelsk.

Den anden udtalelse som er anvendt i denne fremstilling, er en udtalelse fra jurist og IT-sikkerhed specialist, Allan Frank. Han optræder i Datatilsynets eget podcast, i artikler, interviews og er generelt en fremtrædende figur hos Datatilsynet. I nærværende fremstilling anvendes hans udtalelser, som er givet i interviews til Version2. Årsagen til at dette er anvendt i denne fremstilling er, at Allan Frank, i kraft sin stilling og erfaring, må forventes at udtale sig i sin kapacitet, som ekspert hos Datatilsynet, når han giver interviews til et af landet største compliance- og techmedier. Hvis disse udtalelser alene afspejlede hans egen private holdning og dermed ikke i kraft af sin kapacitet, som ekspert hos Datatilsynet, ville de ikke være interessante for et medie som Version2 og desuden ville det være anført i artiklerne, at der var tale om en privat holdning. Nærværende fremstilling er ikke alene båret på en sådan udtalelse, men anvender den til en relevant diskussion på baggrund af det i, i de foregående afsnit, diskuterede.

[15] Hamer og Schaumburg-Müller (2020), 1. udgave, Juraens Verden, side 270.
[16] Vejledning om cloud, Marts 2022, Datatilsynet
[17] Hamer og Schaumburg-Müller (2020), 1. udgave, Juraens Verden, side 271.
[18] Se nærmere i afsnit 3.2.2.3

1.5.3 Metodiske udfordringer

En overordnet metodisk udfordring i nærværende fremstilling er, at der er en relativt begrænset mængde retspraksis, som man kan anvende til at beskrive retstilstanden. Der er én skelsættende dom, som bidrager til stort set hele fortolkningen. Derudover må man forlade sig på soft law kilder så som vejledninger fra tilsynsmyndigheder mv.
Derudover er emnet også relativt nyt i den forstand, at GDPR kun har været i kraft i knap 4 år imens at Schrems II-dommen er knap 2 år gammel. Af samme årsag har det har været vanskeligt at finde bøger og anden juridisk litteratur, som var særligt brugbart i forbindelse med denne undersøgelse. Dette har resulteret i, at de fleste kilder, som har været anvendt til at belyse problemstillingen, udover ovenstående, stammer fra internettet. Det bør dog bemærkes at flere af kilderne er fra de officielle hjemmesider (EU mv.), mens andre er kilder af mere uofficiel karakter. Selv relativt nye kilder kan hurtigt være forældet i sammenhæng med nærværende problemformulering, da det er et område der er i udvikling blandt andet på grund af teknologien.

Især har teknologiske (kommercielle) nyhedsmedier været en kilde og udfordringen med disse kan være, at der undlades "kedelige" juridiske detaljer, da dette ikke har nogen særlig værdi for den almene læser. Dog bør det bemærkes, at eksempelvis Version2, som ofte er refereret til, er et medie for fagfolk, hvor der derfor også detaljeret beskrives de mere tekniske aspekter af både juraen og teknologien.

Under arbejdet med nærværende fremstilling er det blevet forsøgt at afsøge tilgængelige platforme, databaser, søgemaskiner mv. for relevant juridisk litteratur, men det har ikke været muligt, at finde noget særligt brugbart pånær dem der er nævnt i dette metodeafsnit.

Ikke alle anbefalinger, vejledninger og afgørelser er oversat til dansk og det er således den engelske version der er anvendt. Der foreligger naturligvis altid en mindre risiko for misforståelser og fejlfortolkninger når det det skrevne sprog ikke er det samme som forfatterens modersmål. Dette opfatter forfatteren ikke som en udfordring, men bør være nævnt i forbindelse med de metodiske overvejelser. Som udgangspunkt anvendes de danske tekster, hvor muligt. Derudover anvendes de engelske. Det har været muligt at fremsøge relevant litteratur på tysk, og også maskinoversatte udgivelser, hvilket ikke er blevet inddraget pga. risikoen for fejloversættelser. I forbindelse med de engelsksprogede kilder er centrale begreber blevet krydstjekket for at sikre, at et ord er oversat på samme måde som det var tiltænkt af forfatteren eller udgiveren af pågældende kilde.

2. Reguleringen af overførsel af personoplysninger til tredjelande

2.1 Personoplysninger og aktørerne omkring disse

I det følgende vil de mest væsentlige begreber være defineret samt de mest relevante bestemmelser fra lovgivningen være redegjort for. Med henvisning til afsnit 1.4, er det forudsat at

læseren har kendskab til persondataretten generelt, og det følgende vil derfor være begrænset til det, som har særligt relevans henset til problemformuleringen.

3.2.1 Personoplysninger

GDPR omfatter kun data, såfremt der er tale om *personoplysninger*, jf. GDPR, art. 2, stk. 1. Det fremgår af GPDR artikel 4, stk. 1, at personoplysninger er enhver form for information, som direkte eller indirekte kan henføres til en fysisk person (herefter benævnt som "de(n) registrerede"). Det kan således være oplysninger som navn, identifikationsnummer, lokaliseringsdata, e-mail, telefonnummer mv. Desuden gælder det også oplysninger, som alene kan henføres til en registreret i kombination med en anden oplysning[19]. Da der ikke er findes en positivliste over hvilke oplysninger, der er personoplysninger, må man tage udgangspunkt førnævnte definitionen, fra art. 4, hvor første sætning fastslår "at enhver information, som helt eller delvist kan bidrage til at identificere" den registrerede er personoplysninger. Ud fra dette kan man udlede, at definitionen favner bredt.

Der sondres imellem forskellige kategorier af personoplysninger, hvorefter bestemte kategorier nyder skærpet beskyttelse i forhold til andre. Personoplysninger, så som etnicitet, religiøse tilhørsforhold samt seksuelle orientering betragtes i persondataretten som værende mere følsomme og kræver derfor strengere sikkerhed end de almindelige personoplysninger. Kategorierne har dog ikke særlig relevans i forbindelse med nærværende fremstilling og vil derfor ikke blive redegjort yderligere for.

Indsamling, opbevaring og behandling af personoplysninger indebærer to aktører, som bliver behandlet i det følgende.

3.2.2 Dataansvarlig og databehandler

Den dataansvarlige er den aktør, som er ansvarlig for at den registreredes personoplysninger og rettighederne knyttet hertil, bliver iagttaget. I GDPR art. 4, defineres en dataansvarlig til at være: 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[..]"*. Det er således eksempelvis en virksomhed, som indsamler, opbevare og behandler personoplysninger fra sine medarbejdere til at kunne udbetale løn, oprette dem i diverse IT-systemer mv. Den dataansvarlige kan eksempelvis anvende et lønsystem udbudt af en tredjepart eller en cloudtjeneste til intern kommunikation, e-mail mv. udbudt af en tredjepart. En sådan tredjepart er en i dette scenarie databehandler. Det er altså en "*fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne*", jf. GDPR, art. 4. Databehandleren behandler kun personoplysningerne efter en instruks gives af den dataansvarlige. Desuden skal der også være en databehandleraftale i stand imellem disse to parter, jf. GDPR, art. 28, stk. 3.

3.2.3 Dataeksportør og dataimportør

En vigtig term i nærværende fremstilling er dataeksportøer og dataimportør. De er i princippet synonyme med ovenstående i afsnit 3.2.2, men har alligevel en særskilt betydning og vil da også

[19] https://www.datatilsynet.dk/hvad-siger-reglerne/grundlaeggende-begreber-/hvad-er-personoplysninger

være den betegnelse, som bliver anvendt primært i nærværende fremstilling henset til fokusområdet. Termen optræder ikke i selve GDPR, men anvendes blandt andet af EUD i Schrems II-dommen og af Datatilsynet i deres vejledning om tredjelandsoverførsler.
Datatilsynet har i fornævnte vejledning defineret termen til det følgende:
"*Den dataansvarlige eller databehandleren, som overfører personoplysninger ud af EU/EØS bliver typisk betegnet "dataeksportøren", og den dataansvarlige eller databehandleren i tredjelandet, som personoplysningerne bliver overført til, bliver typisk betegnet "dataimportøren""*. Det bemærkes også i vejledningen, at det er den dataansvarlige, som anses for værende dataeksportør, når databehandleren overfører personoplysninger til et tredjeland på den dataansvarliges vegne. Databehandleren handler jo netop indenfor den dataansvarliges instruks. Foretager databehandleren tredjelandsoverførslen på vegne af en "dataansvarlig", som er placeret udenfor EU/EØS og derfor ikke omfattet af GDPR, anses databehandleren i dette scenarie for at være dataeksportør. Dataimportøren vil ifølge ovennævnte eksempel være udbyderen af lønsystem, cloudtjeneste mv., som er placeret i et tredjeland, herunder USA[20].

3.3Tredjelandsoverførsel

3.3.1 Overførslen

GDPR definerer heller ikke hvad en overførsel helt konkret er. Det er dog i særdeleshed vigtigt at gøre klart, hvad en overførsel, herunder til tredjeland, indebærer. Ifølge Datatilsynets vejledning er der tale om en tredjelandsoverførsel når de personoplysninger man behandler *"forlader EU/EØS eller gøres tilgængelige uden for EU/EØS. Det gælder, uanset om overførslen af personoplysninger sker til en virksomhed eller en myndighed.*". Det er således nok, at personoplysningerne blot er tilgængelige for en virksomhed eller myndighed udenfor EU/EØS. Netop dette omkring personoplysningernes tilgængelighed i tredjelandet bliver kommenteret i Schrems II-dommen, som vil blive behandlet nærmere i kapitel 2.
Ifølge GDPR, art. 44, gælder der et princip om, at enhver overførsel af personoplysninger til et tredjeland, må kun finde sted, hvis betingelserne i GDPR's kapitel V er opfyldt. Det er af denne årsag, at det er relevant at finde ud af om en overførsel sker til et tredjeland eller ej.

3.3.2 Usikre tredjelande

Lande udenfor EU/EØS-samarbejdet, hvor Kommissionen ikke har udstedt en tilstrækkelighedsafgørelse efter GDPR, art. 45, stk. 3 og nedenfor. Det vil typisk være fordi, at tredjelandet ikke overholder krav til at de registrerede har mulighed fore domstolsprøvelse, tilstedeværelsen af en uafhængig tilsynsmyndighed og øvrige forhold, som er listet i GDPR, art. 45, stk. 2.

3.3.3 Sikre tredjelande - overførsel på baggrund af tilstrækkelighedsafgørelse

Sikre tredjelande er de lande udenfor EU/EØS-samarbejdet, hvor Kommissionen har vurderet, at tredjelandet eller en international organisation sikrer en tilstrækkelig beskyttelse af personoplysningerne og den registreredes rettigheder. Efter GDPR, artikel 45, stk. 1, kan overførsler til tredjelande ske med hjemmel i en såkaldt tilstrækkelighedsafgørelse, som udstedt

[20] Vejledning: Overførsel af personoplysninger til tredjelande, Juli 2021, 3. udgave, Datatilsynet

efter art. 45, stk. 3. Dette er eksempelvis tilfældet for Storbritannien, som har implementeret en lov der minder om GDPR og dermed sikrer en tilstrækkelig beskyttelse i overensstemmelse med princippet i artikel 44 (og art. 45, stk. 2).

3.3.4 Overførsler omfattet af fornødne garantier - artikel 46

I overførselstilfælde, hvor Kommissionen ikke har udstedt en tilstrækkelighedsafgørelse, fremgår det af artikel 46, stk. 1, at en dataeksportør gerne må overføre personoplysninger til et usikkert tredjeland under visse omstændigheder. Overordnet set gør det sig gældende at dataeksportøren har givet de fornødne garantier, garanterer at den registreredes rettigheder kan håndhæves og garanterer at den registrerede har effektive retsmidler tilgængelige. Dette kan ske på flere måder igennem de overførselsgrundlag, som er listet i artikel 46, stk. 2, litra a-f.

3.3.5 GDPR, art. 46, stk. 2, litra c): Standardbestemmelser vedtaget af Kommissionen

Kommissionen vedtog nye standardkontraktsbestemmelser ved afgørelse 2021/914, som afløste den tidligere afgørelse 2010/87, som oprindeligt var tilpasset Direktiv 95/46.
Standardkontraktsbestemmelserne kan anvendes som overførselsgrundlag, da de "*fastsætter fornødne garantier, herunder rettigheder for registrerede, som kan håndhæves, samt effektive retsmidler, jf. artikel 46, stk. 1, og artikel 46, stk. 2, litra c)*"[21]. Dataimportøren i tredjelandet stiller således, i medfør af kontrakten, en række garantier som skal sikre et tilstrækkeligt beskyttelsesniveau for de registrerede og disses personoplysninger. Desuden kan der i bilag II til kontrakten aftales hvilke tekniske- og organisatoriske foranstaltninger man har truffet som supplement til de kontraktuelle forpligtelser.

3.3.6 Beskyttelseshensyn og rettigheder, som skal sikres ved tredjelandsoverførsel

Grundlæggende er beskyttelseshensynet i GDPR, jf. præambel 1 og 4 til GDPR, retten til privatliv, som det er givet i EMRK art. 8, Chartrets art. 7 og retten til beskyttelse af personoplysninger i Chartrets art. 8. Dette har man i GDPR's kapitel III forsøgt at sikre de registrerede ved en række rettigheder som vedrører opbevaring og behandling af disses personoplysninger, herunder retten til at blive glemt, retten til oplysning, retten til indsigt mv.
Desuden er en vigtig rettighed i Chartret, henset til nærværende problemformulering, retten til adgang til effektive retsmidler og til en upartisk domstol, jf. Chartrets art. 47. I forbindelse med en tredjelandsoverførsel skal man ifølge EUD i Schrems II-dommen nemlig fortolke GDPR i lyset af Chartret, og herunder tage hensyn til denne rettighed.

3.4 Amerikansk lovgivning

I Schrems II-dommen og i nærværende fremstilling indgår der amerikansk lovgivning og overvågningsprogrammer baseret på disse. Disse vil der kort blive redegjort for her, så der er en bedre forståelse herfor, når disse inddrages i domsanalysen samt senere i nærnærende fremstilling. Det bør dog bemærkes at det følgende sigter på, at skabe en grundforståelse for lovgivningen her, mens der i selve domsanalysen af Schrems II-dommen mv. bliver gået mere i dybden med de relevante dele af lovgivningen.

[21] Afgørelse 2021/914, EU-Kommissionen, Bestemmelse 2

1.1.1 FISA section 702

Foreign Intelligence Surveillance Act (herefter benævnt "FISA") er en amerikansk lov er regulerer overvågning af blandt andet elektronisk kommunikation og er særligt henvendt mod overvågning af ikke-amerikanske statsborgere. Foreign Intelligence Surveillance Court ("FISC" eller "FISA-domstolen") kontrollerer lovligheden af overvågningsprogrammerne baseret på FISA. FISA section 702 ("FISA 702") tillader indsamling og brug af data om udenlandske statsborgere, herunder borgere i EU. Indsamlingen af data under FISA 702 sker ved at NSA og andre efterretningstjenester grundlæggende kan bede om få data udleveret af aktører indenfor telekommunikation og udbydere af cloudtjenester. De nærmere lavpraktiske detaljer herom er udeladt.
Blandt overvågningsprogrammer baseret på FISA 702, kan nævnes *PRISM* (senere DOWNSTREAM) og *UPSTREAM*, som blev gjort verdenskendt af whistlebloweren Edward Snowden. UPSTREAM overvågning gør det muligt for amerikanske efterretningstjenester at "tappe" ind på selve infrastrukturen af internettet, altså undersøiske kabler mv. for at indsamle information. DOWNSTREAM overvågning indebærer at man indsamler data fra telekommunikationsudbydere samt udbydere af cloudtjenester[22].

1.1.2 Executive Order 1322 (EO 12333)

EO 12.333 er et præsidentielt dekret, som giver mulighed for indsamling og overvågning af udenlandsk "signals intelligence", som er defineret nærmere i afsnit 3.2.2.3. EO 12.33 er ikke begrænset af nogle restriktioner eller tilsyn, blandt andet fordi den anvendes til at indsamle data i større portioner og skal således ikke være rettet imod en eller flere bestemte fysiske personer udenfor USA, som FISA 702[23].

1.1.3 Presidential Policy Directive 28 ("PPD-28")

PPD-28 blev indført af Barack Obama i et forsøg på, at etablere nogle overordnede spilleregler og principper for indsamlingen af udenlandsk *signal intelligence*. Hensigten med disse regler var at begrænse anvendelsesområdet for EO 12.333 og desuden begrænse anvendelsesmulighederne for hvad den indsamlede data kunne bruges til[24].

1.1.4 CLOUD Act

Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") er en lov I USA, som giver myndigheder mulighed for at få udleveret data, herunder personoplysninger, som er opbevaret på datacentre uden for USA, eksempelvis i Europa, såfremt det er relevant i forbindelse med en igangværende straffesag. Således vil de storeudbydere at cloudtjenester så som Microsoft og Google kunne blive pålagt at udlevere data, som er opbevaret på deres datacentre lokaliseret i EU. Det bør bemærkes at de nærmere tekniske detaljer omkring indsamling af efterretninger under EO 12.333 er hemmelighedsstemplet og det er derfor ikke muligt at gå helt ned i specifikke detaljer i nærværende fremstilling da det ganske enkelt ikke er muligt at finde tilstrækkelig information.

---

[22] https://www.complycloud.com/wp-content/uploads/2021/09/FISA-whitepaper-download.pdf; https://www.eff.org/pages/upstream-prism; https://www.fieldfisher.com/en/insights/us-surveillance-s702-fisa-eo-12333-prism-and-ups

[23] https://www.complycloud.com/wp-content/uploads/2021/09/FISA-whitepaper-download.pdf og C-311/18, præmis 183.

[24] https://www.complycloud.com/wp-content/uploads/2021/09/FISA-whitepaper-download.pdf

CLOUD Act blev først vedtaget i USA, i 2018 og var derfor ikke oprindeligt en del af Schrems sagerne, men falder nu ind under det som i nærværende fremstilling senere bliver omtalt som *problematisk lovgivning*[25].

2. Schrems II-dommen (Sag C-311/18)

2.1 Resumé af dommen

Dommen er en præjudiciel afgørelse afsagt af EU-Domstolen den 16. juli 2020 på baggrund af en anmodning indgivet fra *High Court*, som er retten i første instans i Irland. Den præjudicielle afgørelse skulle søge at afklare gyldigheden og anvendelsen af afgørelse 2010/87 om standardkontraktsbestemmelser (herefter benævnt "afgørelse 2010/87") og afgørelse 2016/1250 (herefter benævnt "Privacy Shield").

Omkring 5 år forud for denne afgørelse blev der afsagt dom i forgængeren til denne sag, nemlig Schrems I-sagen (Sag C-362/14). Her havde den østrigske advokat og privacyaktivist, Maximillian Schrems, indgivet en klage til det irske datatilsyn der anfægtede lovligheden af Facebook Irelands overførsel af hans personoplysninger til deres amerikanske moderselskab, Facebook Inc. Schrems støttede denne klage på, at hans personoplysninger ikke var tilstrækkeligt beskyttet, som følge af amerikanske overvågningslove der giver amerikanske myndigheder mulighed for adgang til data som opbevares og behandles af virksomheder, der har base i USA – uanset om behandlingen sker ved et datterselskab i EU. På dette tidspunkt var forgængeren til GDPR gældende (Databeskyttelsesdirektivet 95/46/EF, herefter benævnt "Direktiv 95/46") og der var samtidigt også lovligt grundlag for overførsel af personoplysninger på baggrund af Safe Harbour-beslutningen (beslutning 2000/520, herefter benævnt "Safe Harbour"), som grundlæggende var en beslutning der havde fastslået at USA sikrede et tilstrækkeligt beskyttelsesniveau. Klagen, som var indgivet af Schrems, blev i imidlertid afvist med henvisning til at sådanne overførsler havde hjemmel i Safe Harbour. Dog indgav den irske High Court en anmodning til EU-domstolen omkring en præjudiciel afgørelse til afklaring af Safe Harbours gyldighed. Safe Harbour blev herefter, af EU-Domstolen, kendt ugyldig i det der i dag omtales som Schrems I-dommen.

Schrems I-sagen lagde således kimen til hvad der skulle blive Schrems II-sagen, der netop kredser om de samme juridiske udfordringer.
Da Safe Harbour nu var kendt ugyldig, måtte Schrems ændre klagen til nu at anfægte lovligheden af overførslen til USA, som skete på det overførselsgrundlag, som Facebook Ireland nu anvendte, nemlig standardkontraktsbestemmelser. Schrems' argument var, at man på trods af dette ellers lovlige overførselsgrundlag, ikke herved kunne undtage sig at være omfattet de amerikanske overvågningslove. Klagen gik derfor nu på, at overførslen og behandlingen skulle stoppe, da Facebook Ireland stadig ikke kunne sikre en tilstrækkelig beskyttelse af hans personoplysninger ved overførslen. Kort efter indledningen af proceduren af den irske *High Court* vedtog Kommissionen afgørelse 2016/1250 der erklærede Privacy Shield for at give et tilstrækkeligt beskyttelsesniveau. Denne tilstrækkelighedsafgørelse blev da også genstand for den præjudicielle afgørelse i Schrems II-sagen.

[25] https://www.linklaters.com/en/insights/blogs/digilinks/2019/september/us-cloud-act-and-gdpr-is-the-cloud-still-safe

Overordnet set skulle EUD nu tage stilling til om GDPR fandt anvendelse på tredjelandsoverførsler baseret på afgørelse 2010/87, hvilket beskyttelsesniveau sådanne overførsler krævede samt gyldigheden af afgørelse 2010/87 og afgørelse 2016/1250. Desuden skulle EUD også tage stilling til hvilke forpligtelser tilsynsmyndighederne har i forbindelse med den slags tredjelandsoverførsler, som var omdrejningspunkt i sagen.

I alt blev EUD forelagt 11 forskellige præjudicielle spørgsmål, som denne skulle tage stilling til[26]. EUD valgte at besvare flere af spørgsmålene under samme besvarelse, da spørgsmålene på grund af deres karakter var egnet til at blive behandlet sammen.

3.2 EUD's stillingtagen til de præjudicielle spørgsmål

I det følgende, vil det undersøges nærmere, hvad det er EUD lægger vægt på i sin afgørelse. Med andre ord – hvad er det for nogle retlige regler der anvendes og analyseres på, og hvordan fortolker EUD disses anvendelse ift. de foreliggende omstændigheder. Med overblik og læsevenlighed for øje, vil dette afsnit være inddelt efter hver besvarelse, som EUD har besvaret dem. Dette betyder at enkelte afsnit adresserer mere end ét spørgsmål ad gangen og analysen vil derfor ikke behandle hvert enkelt spørgsmål særskilt. Det bør dog bemærkes, at de 11 spørgsmål ikke vil være listet i sin fulde længde i nærværende fremstilling. Læseren bør derfor henvises til præmis 68 i Schrems II-domen (C-311/18), hvis denne har ønske om at læse spørgsmålene i sin fulde længde.

Indledningsvist bør det desuden bemærkes, at de præjudicielle spørgsmål i sagen afgøres med GDPR som lovgrundlag, og altså ikke Direktiv 95/46. Den oprindelige klage, som var indgivet af Maximillian Schrems, henviste til Direktiv 95/46, da denne var gældende på daværende tidspunkt. Dog havde Kommissionen ikke truffet endelig afgørelse endnu, da Direktiv 95/46 blev ophævet og erstattet af GDPR og af denne grund anvendes reglerne i GDPR til EUD's afgørelse. Af denne årsag vil der i følgende analyse henvises til bestemmelser i GDPR, på samme måde, som EUD har gjort i sin besvarelse, men der bør gøres opmærksom på at spørgsmålene i præmis 68 er formuleret med Direktiv 96/46 for øje og henviser derfor til bestemmeler, som var ophævet på dommens tidspunkt. Desuden bør det også bemærkes, at afgørelsen om standardkontraktsbestemmelser som udgør en væsentlig kilde og fortolkningsbidrag for EUD i denne afgørelse, nu er blevet erstattet af en ny afgørelse om standardkontraktsbestemmelser[27]. I det følgende vil enhver reference til standardkontraktsbestemmelser – eller afgørelsen om standardkontraktsbestemmelser – være henvendt til afgørelse 2010/87.

3.2.1 Anvendelsesområdet for overførslen

Det første spørgsmål som High Court forelagde EUD, drejede sig om hvor vidt overførslen var omfattet af GDPR. Faktum var, at overførslen var af forretningsmæssig karakter og skete fra et privat selskab i EU til et privat selskab i USA i medfør af standardkontraktsbestemmelser. Derudover var faktum også, at personoplysningerne kunne blive behandlet af myndighederne i

[26] C-311/18, præmis 68

[27] Kommissionens afgørelse af 5. februar 2010 om standardkontraktbestemmelser for videregivelse af personoplysninger til registerførere etableret i tredjelande i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF

USA af hensyn til deres nationale sikkerhed. Spørgsmålet blev således om EU-retten (GDPR og således også Chartret) finder anvendelse på denne slags overførsler på trods af bestemmelserne i TEU, art. 4, stk. 2, der blandt andet indebærer at national sikkerhed er medlemsstaternes eneansvar.

EUD lagde for det første til grund, at TEU, art. 4, stk. 2 ikke har nogen relevans i forbindelse med dette præjudicielle spørgsmål. TEU omfatter kun medlemsstaterne og gælder derfor ikke når der er tale om et tredjeland, som per definition ikke er en medlemsstat.

I spørgsmålet om, hvor vidt overførslen er omfattet af EU-retten, fremhæver EUD GDPR, art. 2, stk. 1, der positivt angiver anvendelsesområdet og GDPR, art. 2, stk. 2, som fastsætter undtagelser til GDPR's anvendelsesområde. EUD slår først fast, at overførslen opfylder indholdet i GDPR, art. 2, stk. 1, da der i bestemmelse ikke sondres mellem om aktiviteter foretages indenfor EU eller har forbindelse til et tredjeland[28]. Det må derfor være underforstået, at overførslen i det hele taget opfylder kravene til en overførsel i GDPR's forstand, da EUD slet ikke kommenterer på selve karakteren af databehandlingen. Dertil nævnes det også, at den blotte eksistens af GDPR's kapitel V må være årsag nok til, at fastslå at sådanne overførsler er omfattet af GDPR. Desuden oplyses det, at undtagelserne til GDPR's anvendelsesområde, som er angivet i GDPR art. 2, stk. 2, skal fortolkes "strengt"[29]. Bestemmelsen giver 4 muligheder (a til d), for undtagelse, hvor kun én af dem (litra c) ikke vedrører behandlingsaktiviteter, som foretages af staten eller statslige myndigheder. Da overførslen sker imellem to private selskaber, og således to juridiske personer, er der ikke tale om behandling af en fysisk person, hvorfor overførslen også falder udenfor anvendelsesområdet af art. 2, skt. 2, litra c.

Det vel nok mest relevante forhold der retfærdiggør netop dette præjudicielle spørgsmål, ligger i, om den behandling der kan ske under eller efter overførslen, af en myndighed i tredjelandet, kan undtage overførslen fra GDPR's anvendelsesområde. Her lægger EUD vægt på ordlyden i GDPR, art. 45, stk. 2, litra a). EUD citerer direkte fra GDPR og konkluderer dermed at der ikke kan være usikkerhed om hvor vidt GDPR finder anvendelse på den omtalte overførsel[30]. Det må udledes af EUD's præmis 87, at lovgiver tydeligvis haft tredjelandes lovgivning, herunder lovgivning omkring national sikkerhed, med i overvejelserne da man vedtog GPDR og der derfor ikke kan herske tvivl om hvor vidt, at en sådan behandling af en myndighed i tredjeland kan undtage overførslen fra GDPR's anvendelsesområde.

3.2.2 Det påkrævede beskyttelsesniveau

Indledningsvist bør det bemærkes, at, man ifølge EUD, skal fastlægge det beskyttelsesniveau der er sikret indenfor EU på grundlag af EU-retten i modsætning til medlemsstaternes nationale lovgivning. De lægger således vægt på, at man bør have de rettigheder som er tilsikret i Chartret for øje, herunder retten til privatliv, som er tilsikret i kapitel 2 af Chartret.
De forhold, der ifølge EUD, skal tages i betragtning ved vurderingen om, hvor vidt et tilstrækkeligt sikkerhedsniveau er sikret, er de kontraktvilkår der er vedtaget imellem dataeksportør og

[28] C-311/18, præmis 82
[29] C-311/18, præmis 84
[30] C-311/18, præmis 87

dataimportør samt de forhold der gør sig gældende i tredjelandets retssystem, hvis en offentlig myndighed har adgang til personoplysningerne. EUD uddyber med forklaring om, at de forhold der skal tages i betragtning, er dem "som på ikke udtømmende vis er opregnet i dens artikel 45, stk. 2. Netop artikel 45, stk. 2, er de forhold, som Kommissionen skal inddrage i deres betragtning når de skal foretage en vurdering af beskyttelsesniveauet i et tredjeland[31].

Domstolen blev også bedt om at tage stilling til hvilke forhold man bør iagttage ved bedømmelsen af om et tredjeland sikrer det, i EU-retten, krævede beskyttelsesniveau. Her har EUD ikke udtrykkeligt gjort klart om de vurderede at man skulle bruge hverken mulighed "a)" eller mulighed "b)" ved vurderingen af tredjelandets beskyttelsesniveau[32]. Det lægges dog til grund, at det er den dataansvarlige eller databehandleres pligt at "kompensere for den manglende databeskyttelse i tredjeland. I stedet for at pege på enten mulighed a) eller mulighed b), lægger EUD vægt på at bedømmelsen skal ske ud fra de forpligtelser, som følger af landets nationale lovgivning og dets internationale forpligtelser[33]. Desuden forklarer man at de fornødne garantier *"skal være af sådan en art, at de sikrer, at der for de personer, hvis personoplysninger overføres til et tredjeland på grundlag af standardbestemmelserne om databeskyttelse, gælder et beskyttelsesniveau, der i det væsentlige svarer til det niveau, der er sikret indenfor Unionen, således som det er tilfældet for en overførsel baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet"*. Man lægger dermed især vægt på, at vurderingen skal ske på samme måde, som en artikel 45, stk.1-vurdering[34]. Det kan altså dermed udledes, at der ifølge EUD ikke er nogen forskel på den vurdering som Kommissionen foretager ved en tilstrækkelighedsafgørelse af et tredjeland eller en sektor i tredjeland, og så den vurdering som dataeksportøren bør foretage ved den type overførsel, som er genstand i sagen.

Den forelæggende ret ønsker med sit spørgsmål 6 to forhold belyst. For det første ønsker man oplysning om hvilket beskyttelsesniveau der er krævet ved brug af standardkontraktsbestemmelser efter GDPR's kapitel V og i lyset af Chartret. For det andet ønskes man at få belyst, hvilke forhold der skal inddrages i vurderingen af om en overførsel på baggrund af standardkontraktsbestemmelser er sket i overensstemmelse med de krav der anføres i GDPR kapitel V og de krav der eksisterer på baggrund af Chartret.

Det væsentlige her er, at den dataansvarlige eller databehandleren, skal give de "fornødne garantier" om, at den registreredes rettigheder kan sikres ved overførslen til tredjelandet. Netop den registreredes rettigheder bliver et springende punkt i denne vurdering og spiller en central rolle i vurderingen af GDPR's kapitel V's bestemmelser.
For at lægge et fundament for fortolkningen og forståelsen af bestemmelserne i GDPR's kapitel V, henviser EUD til det generelle princip i art. 44, som pejlemærke for, at alle bestemmelse i kapitel V skal forstås og fortolkes i sammenhæng med art. 44. Dermed er ingen af bestemmelserne undtaget fra det generelle princip i art. 44[35]. EUD begrunder det desuden med, at bestemmelserne

[31] C-311/18, præmis 104.
[32] C-311/18, præmis 68, spørgsmål 2.
[33] 311/18, præmis 94
[34] C-311/18, præmis 96
[35] C-311/18, præmis 92

i kapitel V søger at opretholde det høje beskyttelsesniveau, som der udtrykkes ønske om i 6. betragtning til GPDR.
EUD henviser også, som nævnt i afsnit **Error! Reference source not found.**, til at en art. 45, stk.1-vurdering blot søger at tilsikre et "tilstrækkeligt beskyttelsesniveau" og dermed ikke en identisk beskyttelse. Det må dermed kunne udledes, at beskyttelsesniveauet derfor ikke er en fast størrelse. Netop formuleringen om et tilstrækkeligt beskyttelsesniveau bør derfor afklares, for at kunne svare klart på, hvilket beskyttelsesniveau der er krævet efter GDPR kapitel V og set i lyset af Chartret.
Ifølge EUD, bør man derfor i stedet skal søge oplysning i betragtning 104 om retsstatsprincippet, ret til domstolsprøvelse mv. I vurdering af om beskyttelsesniveau er "tilstrækkeligt" bør man vurdere den registreredes rettigheder, blandt andet i form af klageadgangen, domstolsprøvelse, rettigheden til privatliv mv. Endeligt nævnes den registreredes ret i forhold til offentlig sikkerhed, forsvar og statens sikkerhed, som jo netop er hovedtemaet i denne dom. En vurdering kan således ikke ignorere hvilke rettigheder den registrerede har i forbindelse med indgreb i sin grundlæggende menneskeret til privatliv, uanset hensynet til tredjelandets nationale sikkerhed og forsvar. Det kræves således, ifølge EUD med henvisning til betragtning 104, at man "sikrer et passende beskyttelsesniveau, som i det væsentlige svarer til det, der sikres i Unionen, især når personoplysninger behandles i en eller flere specifikke sektorer"[36].

Det kan derfor opsummerende konkluderes, at beskyttelsesniveauet skal, i det væsentligste, svare til det, der sikres i EU, herunder med henblik på den registreredes rettighed til privatliv, domstolsprøvelse og klageadgang. I vurderingen af beskyttelsesniveauet ved den overførsel, som der er genstand i sagen, skal kontraktvilkårene imellem dataeksportør og dataimportør inddrages. Herunder er det især vigtigt at inddrage tredjelandets offentlige myndigheders adgang til personoplysningerne, under eller efter overførslen er foretaget.

3.2.3 Tilsynsmyndighedernes pligt til indgriben

Den forelæggende ret ønskede, at få belyst, hvor vidt de nationale tilsynsmyndigheder har en pligt til at anvende sine håndhævelsesbeføjelser til at suspendere en dataeksportørs overførsel, hvis dataimportøren i et tredjeland er underlagt overvågningslovgivning, som efter tilsynets opfattelse gør, at overførslen ikke kan ske i overensstemmelse med GDPR's artikel 45 og 46 samt Chartret[37]. Spørgsmålet angår således både de nationale tilsynsmyndigheders kompetence, og deres forpligtelser og om de ud fra en skønsmæssig vurdering, kan undlade at gribe ind, hvis altså en sådan pligt består.

Om tilsynsmyndighedernes generelle kompetence og rækkevidden af denne, henleder EUD opmærksomheden på Chartrets artikel 8, stk. 3, der fastslår at overholdelsen af reglerne for beskyttelse af personoplysninger i Chartrets art. 8 er underlagt en uafhængig myndigheds kontrol. Ydermere refererer de også til GDPR, art. 51, stk. 1, om at medlemsstaternes tilsynsmyndigheders pligt til at føre tilsyn med anvendelsen af GDPR[38]. Endeligt henvises der til GDPR, art. 57, stk. 1, litra a), definerer, at de nationale tilsynsmyndigheders opgave, blandt andet indebærer, at "føre tilsyn med og håndhæve anvendelsen af denne forordning". EUD siger, at da tilsynsmyndigheden

[36] C-311/18, præmis 97.
[37] C-311/18, præmis 68, spørgsmål 8.
[38] GDPR, art. 51, stk. 1.

på baggrund af disse bestemmelser beføjelser til at undersøge om EU-retten, herunder GDPR, er overholdt indebærer dette også overførsler, som der behandles i GDPR's kapitel V[39]. Faktisk tillægges tilsynsopgaven en særlig vigtig rolle, da der i forbindelse med overførsler af personoplysninger til tredjelande opstår yderligere risici for de registrerede med henvisning til 116. betragtning til GDPR[40]. Desuden er tilsynsmyndighedens opgave også at behandle klager, jf. GPDR, art. 57, stk. 1, litra f), med den fornødne omhu.

EUD forklarer, om tilsynsmyndighedens egen kompetence til at vælge det middel den finder hensigtsmæssigt efter artikel 58, stk. 2, at tilsynsmyndigheden har "pligt til at gøre dette med den fornødne omhu, som kræves af dens opgave bestående i at sikre den fulde overholdelse af databeskyttelsesforordningen"[41]. Dette efterlader så spørgsmålet om hvad det "som kræves" konkret indebærer i denne sammenhæng. Her lægger EUD vægt på det som generaladvokaten har anført i punkt 148 i forslaget til afgørelsen[42]. Generaladvokaten anerkender, at der er tale om en skønsmæssig vurdering, men at myndigheden har "pligt til fuldt ud at udføre den tilsynsopgave, som den er blevet tillagt.[43]". Det følger således her af i generaladvokatens næste bemærkning, at myndigheden skal suspendere en sådan overførsel, hvis standardkontraktsbestemmelserne ikke er overholdt og det ikke er muligt at sikre den fornødne beskyttelse. EUD behandlede da også spørgsmålet om netop denne beføjelse kunne tænkes at være begrænset som følge af brugen af standardkontraktsbestemmelser. Med henvisning til 5. betragtning, 2. pkt. til afgørelse 2016/2297 fastslår EUD dog, at der uanset afgørelsen omkring standardkontraktsbestemmelser, ikke sker en begrænsning af tilsynsmyndighedernes beføjelser, som denne har efter GDPR art. 58, stk. 2[44].

I tilfælde, hvor der allerede foreligger en tilstrækkelighedsafgørelse, fastslår EUD, at tilsynsmyndighederne ikke kan kræve en overførsel suspenderet. Dog påvirker dette ikke de registreredes klager til tilsynsmyndigheden[45].

3.2.4 Gyldigheden af afgørelsen om standardkontraktsbestemmelser

I den forelæggende rets syvende spørgsmål, ønsker man, at EUD tager stilling til, om standardkontraktsbestemmelser kan sikre et tilstrækkeligt beskyttelsesniveau ved overførsler til tredjelande, da disse ikke er bindende for tredjelandets myndigheder, men kun de to aftaleparter[46]. I det ellevte spørgsmål ønsker man EUD's stillingtagen til om afgørelsen om standardkontraktsbestemmelser er i strid med Chartrets art. 7, 8 og 47.

Det syvende spørgsmåls præmis om, at afgørelsen om standardkontraktsbestemmelser og dennes bilag tilsikrer en tilstrækkelig beskyttelse, samt det faktum, at en sådan vedtaget aftale på grundlag af standardkontraktsbestemmelser, ikke er bindende overfor tredjelandets myndigheder,

[39] C-311/18 præmis 107.
[40] C-311/18, præmis 108.
[41] C-311/18, præmis 112.
[42] C-311/18, præmis 113.
[43] C-311/18, - Forslag til afgørelse, punkt 148.
[44] C-311/18, præmis 115.
[45] C-311/18, præmis 118-119.
[46] C-311/18, præmis 123.

men alene kontraktsparterne, anerkendes indledningsvist af EUD[47]. Uden at komme nærmere ind på konkrete tilfælde, anerkender EUD desuden også, at der kan forekomme situationer, hvor en dataimportør i tredjelandet, "under hensyn til retstilstanden og gældende praksis i pågældende tredjeland"[48] kan garantere en tilstrækkelig beskyttelse på baggrund af standardkontraktsbestemmelser. Dog anerkender de også, at der i andre situationer ikke kan garanteres en tilstrækkelig beskyttelse[49]. Netop vurderingen af om overførslen er genstand for en tilstrækkelig beskyttelse, fastslår EUD, er kontraktparternes ansvar. Dette begrunder de med flere argumenter. Først og fremmest adskiller en afgørelse om standardkontraktsbestemmelser efter art. 46, stk. 2, litra c) sig væsentligt fra en tilstrækkelighedsafgørelse efter art. 45, stk. 3. I denne sammenhæng er den væsentlige forskel, at Kommissionen i en art. 46, stk. 2, litra c)-afgørelse ikke har "pligt til at foretage en vurdering af tilstrækkeligheden af beskyttelsesniveauet i de tredjelande, hvortil personoplysninger kan blive overført på grundlag af sådanne bestemmelser"[50], på samme måde som de har ved en tilstrækkelighedsafgørelse, som tager sigte på et tredjeland, et område eller enkelte sektorer i tredjelandet. Når ikke Kommissionen har truffet en tilstrækkelighedsafgørelse, lægger EUD vægt på blandt andet 108. og 114. betragtning. Opsummerende kan disse forklares med, at der i sådanne tilfælde, af den dataansvarlige eller databehandleren, skal benyttes løsninger, som sikrer den registreredes rettigheder og håndhævelsen af disse i form af supplerende garantier[51]. Det er altså med andre ord kontraktparternes ansvar, at sikre, at de fornødne garantier er stillet og kan overholdes i medfør af standardkontraktsbestemmelser[52]. Det er ikke blot supplerende garantier, som EUD nævner, men også supplerende foranstaltninger. Standardkontraktsbestemmelsernes formål er, at der imellem dataimportøren og dataeksportøren kan etableres nogle kontraktuelle garantier, der kan anvendes ens i alle tredjelande og dermed uafhængigt af det pågældende lands databeskyttelsesniveau. Da der i forskellige tredjelande vil eksistere forskellige overvågningslove regler omkring domstolsprøvelse, klageadgang mv. bør man derfor ifølge EUD implementere supplerende foranstaltninger henset til situationen i det pågældende land[53]. EUD kommer ikke nærmere ind på hvad "supplerende foranstaltninger" konkret indebærer. I begrundelsen fortolker EUD GDPR's art. 44, art. 46, stk.1, og art. 46, stk. 2, litra c) i lyset af Chartrets art. 7, art. 8 og art. 47[54]. De kommenterer ikke på, hvordan denne fortolkning konkret foretages, men disse bestemmelser er ikke absolutte, da de kan fraviges under proportionalitetsprincippet[55].
Med baggrund i de ovenstående argumenter, samt det faktum, at overførslen skal suspenderes såfremt der ikke kan implementeres tilstrækkelige supplerende foranstaltninger, konkluderer EUD om gyldigheden, at det faktum, at standardkontraktsbestemmelser ikke kan binde offentlige myndigheder og alene parterne, ikke er til hinder for at standardkontraktsbestemmelserne yder tilstrækkelige garantier.

[47] C-311/18, præmis 124 og 125.
[48] C-311/18, præmis 126.
[49] C-311/18, præmis 126.
[50] C-311/18, præmis 129.
[51] C-311/18, præmis 131.
[52] C-311/18, præmis 131.
[53] C-311/18, præmis 133.
[54] C-311/18, præmis 132.
[55] Se nærmere i afsnit 3.2.5

For at sikre effektive mekanismer, skal det blot være *muligt* sikre sikkerhedsniveauet ved at gøre brug af standardkontraktsbestemmelser [56]. En af de mekanismer som bestemmelserne sikrer, er blandt andet, at dataimportøren har pligt til at underrette dataeksportøren såfremt denne ikke kan, eller ikke forventer at kunne, overholde sine forpligtelser omkring det tilstrækkelige sikkerhedsniveau[57]. I et sådant tilfælde har dataeksportøren pligt at til at suspendere overførslen straks[58], og alternativt, da dataeksportøren er forpligtet til at underrette tilsynsmyndigheden hvis tredjelandets lovgivning ændres til fare for persondatasikkerheden, kan tilsynsmyndigheden anvende sine beføjelser til at bringe overførslen til ophør, jf. afsnit 3.2.3 og præmis 145[59].
Som en naturlig del af førnævnte pligt, har begge parter også efter bestemmelserne pligt til forudgående at undersøge, hvor vidt et tilstrækkeligt beskyttelsesniveau kan garanteres på baggrund af tredjelandets love, regler og myndighedsbeføjelser[60]. Har parterne ikke overholdt de netop nævnte forpligtelser og overførslen af personoplysninger således er sket på ulovlig vis, så er parterne også kontraktuelt forpligtet til at destruere eller tilbagelevere de pågældende personoplysninger[61].

Det faktum, at tredjelandets myndigheder kan behandle og få adgang til personoplysninger, er dermed ikke en hindring for standardkontraktsbestemmelser kan yde de tilstrækkelige garantier efter EU-retten.

3.2.5 Amerikanske tilsynsmyndigheder og Privacy Shield

Det fremgår af Privacy Shield-afgørelsens art. 1, stk. 1, at USA sikrer et tilstrækkeligt beskyttelsesniveau under Privacy Shield. En overførsel anses for sket under denne ordning, når overførslen sker til ” foretagender i USA, der er opført på »listen over deltagere i værnet om privatlivets fred«”, jf. Privacy Shield-afgørelsens, art. 1, stk. 3[62]. Da der er tale om en tilstrækkelighedsafgørelse, truffet af Kommissionen, som ikke er blevet kendt ugyldig, kan de nationale tilsynsmyndigheder ikke anvende sine beføjelser til at suspendere eller forbyde overførslen med henvisning til at tredjelandet ikke kan sikre et tilstrækkeligt beskyttelsesniveau. Derfor fastslår EUD, at Kommissionens konstatering i Privacy Shield-afgørelsen har bindende virkning overfor de nationale tilsynsmyndigheder og således giver Facebook Ireland ret i sin påstand, som beskrevet indledningsvist i dette afsnit[63]. Dog er de nationale tilsynsmyndigheder pålagt at behandle en klage, som denne har modtaget fra en fysisk person, der gør gældende at tredjelandets lovgivning og praksis ikke sikrer et tilstrækkeligt beskyttelsesniveau, uanset en tilstrækkelighedsafgørelse[64]. Den skal undersøge om kravene i GDPR er efterlevet, og i tilfælde af den klagende har anfægtet gyldigheden af en tilstrækkelighedsafgørelse, skal tilsynsmyndigheden anlægge sag ved den nationale domstol, som skal forelægge spørgsmålet for EUD[65]. Det er netop

[56] C-311/18, præmis 137.
[57] C-311/18, præmis 139 og præmis 148.
[58] C-311/18, præmis 140.
[59] C-311/18, præmis 145.
[60] C-311/18, præmis 142.
[61] C-311/17, præmis 143.
[62] C-311/18, præmis 155.
[63] C-311/18, præmis 156.
[64] C-311/18, præmis 157 og præmis 158.
[65] C-311/18, præmis 157.

dette, som der er faktum i nærværende sag[66]. Med henvisning til generaladvokatens punkt 175[67], fastslår EUD derfor at de forlagte spørgsmål skal forstås på en sådan måde, at der rejses tvivl om Privacy Shield-afgørelsens gyldighed og undersøgelsen, samt besvarelsen, derfor især angår denne tvivl[68]. For at lægge kimen til en sådan undersøgelse, fastslår EUD, at for at Kommissionens tilstrækkelighedsafgørelser, efter GDPR art. 45, stk. 3, kan være gyldige, skal Kommissionen kunne "behørigt konstatere", at tredjelandet faktisk sikrer et tilstrækkeligt beskyttelsesniveau[69]. Undersøgelsen belyser først og fremmest indholdet af Privacy Shield-afgørelsen. Herefter sammenholder EUD så indholdet med Kommissionens konstatering om, at beskyttelsesniveau er tilstrækkeligt, for at vurdere om konstateringen lever op til de krav til beskyttelsesniveauet, som fremgår af GDPR art. 45, stk. 3 og Chartrets art. 7, 8 og 47.

Overholdelsen af principperne i bilagene til Privacy Shield-afgørelsen er vigtige i spørgsmålet om hvor vidt et tilstrækkeligt beskyttelsesniveau er garanteret efter amerikansk ret. I den forbindelse bemærker EUD da også, at der i punkt I.5 i bilag 2 er indført en begrænsning til principperne, hvorefter at tilslutningen til principperne kan være begrænset på baggrund af krav med hensyn til blandt andet den nationale sikkerhed. Dette betyder, at amerikanske dataimportører under Privacy Shield er forpligtet til at tilsidesætte de principper, som netop sikrer et tilstrækkeligt beskyttelsesniveau, når disse principper strider imod de førnævnte krav som USA har til den nationale sikkerhed. På denne måde får USA's hensyn til den nationale sikkerhed forrang overfor de rettigheder som de registrerede bør have i medfør af principperne under Privacy Shield[70]. En sådan afvejningsregel, hvor hensyn til national sikkerhed, offentlig interesse og retshåndhævelse vægtes tungere end individets rettigheder, er da ikke heller ikke unormal i demokratiske samfund, men spørgsmålet er om en sådan begrænsning er proportionel[71]. EUD lægger vægt på at undtagelsen til principperne i punkt I.5 i bilag II er af en så general karakter, at der reelt set åbnes op for, at amerikanske myndigheder med henvisning til den nationale sikkerhed, kan få adgang til – og gøre brug af – personoplysninger som er beskyttet efter EU-retten. Dette betyder at indgreb kan ske som følge af PRISM[72] og UPSTREAM. Desuden kan der også ske indgreb på baggrund af EO 12.333[73].
Kommissionen vurderede om disse begrænsninger til at overholde principperne ville begrænse beskyttelsen i en sådan grad, at der ikke kunne være tale om et tilstrækkeligt beskyttelsesniveau, men nåede frem til at eventuelle indgreb fra de amerikanske myndigheder i medfør af begrænsningerne, "vil blive begrænset til det strengt nødvendige med henblik på at nå det tilsigtede legitime mål..."[74].

Om de amerikanske myndigheders behandling af - eller adgang til - personoplysninger slår EUD fast, at der både er tale om indgreb i de registreredes rettigheder efter Chartrets art. 7 og 8[75].

[66] C-311/18, præmis 159.
[67] C-311/18, Forslag til afgørelse: punkt 175.
[68] C-311/18, præmis 160 og 161.
[69] C-311/18, præmis 162.
[70] C-311/18, præmis 164.
[71] C-311/18, præmis 174.
[72] Også "DOWNSTREAM"
[73] C-311/18, præmis 165.
[74] C-311/18, præmis 167.
[75] C-311/18, præmis. 170-171.

Det fremgår dog også, at rettighederne som følger af Chartrets art. 7 og 8 ikke er absolutte i deres natur og kan derfor godt begrænses under iagttagelse af proportionalitetsprincippet, jf. Chartrets art. 52, stk. 1. En sådan begrænsning skal fastlægges nærmere ved lov[76] og skal både præcisere rækkeviden og anvendelsen for begrænsningen samt indeholde mindstekrav således, at de registrerede har tilstrækkelige garantier til at beskytte sine personoplysninger[77]. EUD lægger især vægt på, at Kommissionen i sin vurdering skal tage hensyn til, hvor vidt de registrerede fortsat har effektive rettigheder, som kan håndhæves, som det fremgår af GDPR art. 45, skt. 2, litra a)[78]. Spørgsmålet bliver således om et tilstrækkeligt beskyttelsesniveau så er til stede, når der foretages indgreb i de registreredes grundrettigheder i medfør af overvågningsprogrammer, som ikke er underlagt krav, om at overholde proportionalitetsprincippet[79], herunder i henhold til rettigheder forbundet med databehandlingen.

FISA-domstolens kontrol af overvågningsprogrammerne tager udelukkende sigte på om overvågningen er sket i overensstemmelse med formålet og tager således ikke sigte på, om det faktum at fysiske personer, og dermed disse personoplysninger, er velegnede mål henset til formålet[80]. Der er derfor ingen kontrol eller begrænsninger i beføjelserne, som amerikanske myndigheder har i forbindelse med overvågningsprogrammerne og ej heller garantier for ikke-amerikanske statsborgere[81]. På trods af at PPD-28 fastsætter garantier der tilsigter at respektere privatlivets fred, som er bindende for amerikanske myndigheder[82], kan de registrerede alligevel ikke påberåbe sig disse garantier ved nogen domstol[83]. Ligeledes forholder det sig med EO 12.333, hvorefter de registrerede ej heller er indrømmet nogle rettigheder, som kan håndhæves overfor de amerikanske myndigheder ved en domstol[84]. På baggrund af dette konkluderer EUD, at de overvågningsprogrammer, som er baseret på FISA 702 og EO 12.333, ikke overholder proportionalitetsprincippet jf. Chartres art. 52, stk. 1, 2. pkt., da indgrebene i de registreredes rettigheder ikke er begrænset til det strengt nødvendige[85]. EUD nævner ikke noget om, hvor vidt PPD-28 lever op til kravet om, at begrænsninger til rettighederne skal være fastsat ved lov, jf. Chartrets art. 52, stk. 1, 1. pkt., men generaladvokaten har i sine bemærkninger til Forslag til afgørelse, anført, at PPD-28 og EO 12.333 begge snarere har karakter af en administrativ instruks end det har karakter af lovgivning[86]. Med henvisning til de ovenstående afsnit, hvori EUD har fastslået, at der ingen – eller kun ringe – retsmidler eksisterer indenfor sfæren af PPD-28, FISA 702 og EO 12.333 og at manglen på effektiv domstolsbeskyttelse gjorde, at Chartrets art. 47 ikke var overholdt[87].

[76] C-311/18, præmis 175-176.
[77] C-311/18, præmis 172-174.
[78] C-311/18, præmis 177.
[79] C-311/18, præmis 178.
[80] C-311/18, præmis 179.
[81] C-311/18, præmis 180.
[82] C-311/18, Forslag til afgørelse: punkt 63 og C-311/18, præmis 181.
[83] C-311/18, Forslag til afgørelse: punkt 267 og C-311718, præmis 181.
[84] C-311/18, præmis 182.
[85] C-311/18, præmis 184.
[86] C-311/18, Forslag til afgørelse, punkt 267.
[87] C-311/18, præmis 191.

Den forelæggende ret satte også spørgsmålstegn ved om oprettelsen af en ombudsfunktion i USA var nok til at sikre de registrerede rettighed til effektiv domstolsprøvelse ved en uafhængig og upartisk domstol, som følger af Chartrets art. 47[88]. En sådan rettighed er i særdeleshed vigtig i forbindelse med overførsel af personoplysninger til et tredjeland, da disse som regel ligger uden for medlemsstaternes tilsynsmyndigheders jurisdiktion[89]. Kommissionen nåede i sin tilstrækkelighedsafgørelse frem til, at på trods af de manglende retsmidler under PPD-28, FISA 702 og EO 12.333, som beskrevet ovenfor, var oprettelse af en ombudsmandsmekanisme, nok til at USA kunne anses for at sikre et tilstrækkeligt beskyttelsesniveau med henblik på Chartrets art. 47[90]. Det vigtige er dog om ombudsfunktionen er effektiv, henset til Chartrets art. 47.
Der skal, ifølge EUD, særligt tages hensyn til om de registrerede har muligheden for at anvende retsmidler ved en domstol som skal være uafhængig og upartisk[91]. Netop ombudsmandens uafhængigheden og upartiskheden betvivles af EUD, som fremhæver, at det på trods af påstand om uafhængighed, forholder sig således, at ombudsmanden udpeges af den amerikanske udenrigsminister og at ombudsmanden indberetter direkte til udenrigsministeren. Kommissionen og generaladvokaten anser derfor også ombudsmanden som værende en del af det amerikanske udenrigsministerium, hvilket kan pege i retning af at ombudsmanden er underlagt et ministerium, som har modsatrettede interesser end den selv har og derfor så tvivl om upartiskheden og uafhængigheden i dens virke. Endeligt indeholder Privacy Shield-afgørelsen heller ingen garantier i tilfælde af at ombudsfunktionen nedlægges eller tilbagekaldes[92]. Det et dog tvivlsomt, at sådanne garantier i det hele taget ville hjælpe noget, da ombudsmanden ej heller er blevet tildelt nogle lovbestemte kompetencer og beføjelser[93]. Af disse årsager kan EUD endeligt bekræfte den forelæggende ret i sin tvivl om, hvor vidt ombudsfunktionen har nogen reel indflydelse på efterlevelse af Chartrets art. 47 og dermed konkludere, at de registrerede ikke har de garantier omkring effektiv domstolsprøvelse i forbindelse med overførsler til USA[94]. Dermed konkluderer EUD også endeligt at Kommissionen i sin konstatering i Privacy Shield-afgørelsen art. 1, stk. 1, har tilsidesat de krav der følger omkring tilstrækkelighedsvurderingen i GDPR, art. 45, stk. 1 sammenholdt med Chartrets art. 7, 8 og 47 og denne er derfor uforenelig med EU-retten[95]. Da Privacy Shield-afgørelsen, artikel 1, ifølge EUD, ikke kan adskilles fra dennes art. 2-6 påvirker det gyldigheden af hele afgørelsen og må derfor konkludere at Privacy Shield-afgørelsen er ugyldig.

EUD forklarer desuden, at der ikke opstår et retligt tomrum på baggrund af ugyldiggørelsen af Privacy Shield-afgørelsen, da det af dommens præmisser er afgjort, hvad der fortsat er gyldigt og hvilke rettigheder der skal være iagttaget[96].

3.2.6 Opsamling

Overordnet set kan EUD's vigtigste konklusioner opsummeres, som følger:

[88] C-311/18, præmis 190.
[89] C-311/18, præmis 189.
[90] C-311/18, præmis 193.
[91] C-311/18, præmis 194.
[92] C-311/18, præmis 195 og Forslag til afgørelse: punkt 337.
[93] C-311/18,præmis 196.
[94] C-311/18, præmis 197.
[95] C-311/18, præmis 198-199.
[96] C-311/18, præmis 202.

- Den type overførsler, som der var sagens omdrejningspunkt, er omfattet af GDPR og således også Chartret.

- Personer, hvis personoplysninger overføres til et tredjeland med hjemmel i standardkontraktbestemmelser, skal være omfattet af et beskyttelsesniveau der i det væsentlige svarer til det, som personerne ville have efter GDPR.

- De nationale tilsynsmyndigheder er forpligtet til at skride ind, hvis en overførsel ikke vurderes at kunne ske i overensstemmelse med EU-retten. Hvis databeskyttelsen ikke er overholdt, eller hvis den vurderes ikke at kunne overholdes pga. lovgivning i tredjelandet, skal tilsynsmyndighederne suspendere eller forbyde overførslen i det tilfælde, hvor dataeksportøren ikke af egen drift har indstillet den omtalte overførsel.

- Afgørelse 2010/87 om standardkontraktsbestemmelser var fortsat gyldig. Det faktum, at standardkontraktsbestemmelser der vedtages imellem to parter ikke er bindende overfor et lands myndigheder, påvirkede således ikke på gyldigheden af afgørelse 2010/87.

- På trods af Privacy Shield-afgørelsen, har national sikkerhedslovgivning i tredjelandet fortsat forrang og åbner således for muligheden for at der gøres indgreb i de registreredes rettigheder i et omfang der ikke er foreneligt med det proportionalitetsprincip der foreskrives i EU-retten.

I sin sidste præmis i dommen fastslår EUD, at ugyldiggørelsen af Privacy Shield-afgørelsen ikke skaber et tomrum[97]. Dette er vigtigt, da alle de overførsler, som tidligere var sket på baggrund af Privacy Shield-afgørelsen, altså dermed ikke nu var ulovlige, men blot skulle ske på et andet grundlag. Dataeksportører, som anvendte Privacy Shield-afgørelsen, skulle handle for at kunne iagttage de registreredes rettigheder og for at kunne anvende deres eksisterende amerikansk-baserede leverandører. Denne nye virkelighed har givet anledning til nye overvejelser omkring den digitale samhandel med USA og som har krævet, at dataeksportører forventes at spille en mere aktiv og forebyggende rolle i modsætning til tidligere, hvor det var tilstrækkeligt, at en samhandelspartner havde selvcertificeret sig under Privacy Shield. Det følgende kapitel vil derfor beskæftige sig med, den gældende retstilstand i kølvandet på Schrems II-dommen, herunder især, hvordan dataeksportøren lovligt kan fortsætte brugen af amerikanske cloudtjenester.

3. Den (u)lovlige tredjelandsoverførsel i lyset af Schrems II-dommen

3.1Tidslinje over vigtige begivenheder siden dommen

I tiden efter Schrems II-dommen har der selvsagt været en del dataansvarlige og databehandlere, som har stået i en uvant situation. Dommen introducerer ikke nogen krav, som ikke fandtes før,

[97] C-311/18, præmis 202.

men slår fast, at tiltag der skal sikre et tilstrækkeligt beskyttelsesniveau, skal være effektive - også når man ridser i overfladen. Dem der tidligere havde baseret sine overførsler på Privacy Shield-afgørelsen, måtte nu sikre sig, at overførslerne kunne ske på en måde, som er i overensstemmelse med GDPR's kapitel V og således også rettighederne som følger af Chartret, herunder art. 7, 8 og 47. For det store spørgsmål var – og er stadig – hvordan dataeksportører fortsat kan foretage overførsler af personoplysninger til USA i overensstemmelse med EU-retten. For at besvare dette spørgsmål bør det undersøges hvad relevante aktører har udgivet af vejledninger og anbefalinger herom sammenholdt med EUD's præmisser i Schrems II-dommen. Først vil der i det følgende præsenteres en tidslinje, for at skabe en tidslinje der giver overblik over udviklingen siden domsafsigelsen 16. juli 2020. I perioden har Datatilsynet også udgivet vejledninger, men disse er ikke inkluderet i denne tidslinje.

3.1.1 10. november 2020: Offentliggørelse af EDPB's anbefalinger til supplerende foranstaltninger (til offentlig høring)

Den 10. november 2020 offentliggjorde EDPB deres "Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger"[98], som var en version til offentlig høring. Høringssvar kunne fremsættes indtil 21. december 2020. Dette var således det første gang at en EU-instans siden EUD's afgørelse i Schrems II-dommen offentliggjorde konkrete anbefalinger i relation til EUD's bemærkninger om, dataeksportøren pligt til at træffe supplerende foranstaltninger, hvis ikke standardkontraktsbestemmelser alene kunne sikre et tilstrækkeligt sikkerhedsniveau, som beskrevet i afsnit **Error! Reference source not found.**.

3.1.2 10. november 2020: Offentliggørelse af EDPB's anbefalinger om væsentlige garantier for overvågningsforanstaltninger

Samme dag, som Henstilling nr. 01/2020 blev offentliggjort, offentliggjorde EDPB også deres vedtagne "Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger"[99]. Disse anbefalinger skal ses i lyset af EUD's afgørelse i Schrems II-dommen, hvorefter at der som følge af overvågningsforanstaltninger i USA ikke kunne ydes en beskyttelse, som i det væsentligste svarer til den der er garanteret i EU[100]. Formålet med offentliggørelsen af disse anbefalinger er således at dataeksportører kan anvende disse i forbindelse med deres vurdering af om en myndighed i tredjelandets adgang skal betragtes som et ubegrundet indgreb i de grundlæggende rettigheder i Chartret[101].

[98] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

[99]Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

[100] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, punkt 8.

[101] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures punkt 7.

3.1.3 12. november 2020: Offentliggørelse af EU-Kommissionens reviderede standardkontraktsbestemmelser til offentlig høring.

Kort tid efter offentliggørelsen af de to ovennævnte anbefalinger fra EDPB, offentliggjorde Kommissionen sin reviderede version af standardkontraktsbestemmelserne til offentlig høring. Høringsperioden varede til 10. december 2020[102].
De nye standardkontraktsbestemmelser skulle erstatte de tre tidligere sæt af standardkontraktsbestemmelser, som var vedtaget under GDPR's forgænger, Databeskyttelsesdirektiv 95/46, med nye – mere tidssvarende – standardkontraktsbestemmelser. I Schrems II-dommen havde EUD jo netop afgjort, at standardkontraktsbestemmelser gyldighed ikke kunne anfægtes og dermed fortsat fungere, som et gyldigt overførselsgrundlag såfremt de væsentlige europæiske garantier var iagttaget, eksempelvis ved implementeringen af supplerende foranstaltninger.

3.1.4 4. juni 2021: Endelige udgaver af standardkontraktsbestemmelser offentliggjort

Knap 7 måneder efter, at de reviderede standardkontraktsbestemmelser blev sendt i offentlig høring, som beskrevet ovenfor, kunne Kommissionen endeligt offentliggøre de endelige udgaver af standardkontraktsbestemmelserne.
De nye standardkontraktsbestemmelser er opdelt i nogle moduler, som kan anvendes efter behov med henblik på hvilke roller dataimportøren og dataeksportøren har under den pågældende overførsel. Blandt bestemmelserne finder man "AFSNIT III LOKALE LOVE OG FORPLIGTELSER I TILFÆLDE AF OFFENTLIGE MYNDIGHEDERS ADGANG"[103], hvor kontraktsparterne skal tage stilling til tredjelandets love og offentlige myndigheders adgang til den personoplysninger, som overføres fra EU til et tredjeland. Dermed får dataeksportøren således et værktøj $til at dokumentere sit overførselsgrundlag.

3.1.5 18. juni 2021: EDPB's endelige anbefalinger til supplerende foranstaltninger

EDPB's ikke-endelige anbefalinger, som blev offentliggjort til offentlig høring tilbage i november 2020, blev nu endeligt vedtaget. Der blev foretaget en række ændringer for at imødekomme høringssvarene, men blandt de mest fremtrædende ændringer, finder man muligheden for at dataeksportøren kan lægge vægt på dataimportørens praktiske erfaringer med udleveringsanmodninger om personoplysninger fra offentlige myndigheder i tredjelandet[104].
Desuden introducere de også et alternativ til dataeksportøren, som giver mulighed for, at denne kan fortsætte/igangsætte overførslen, såfremt denne vurderer at problematisk lovgivning i tredjelandet ikke vil påvirke eller omfatte personoplysningerne[105].

---

[102] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Databeskyttelse-standardkontraktbestemmelser-om-videregivelse-af-personoplysninger-til-lande-uden-for-EU-gennemf%C3%B8relsesretsakt-_da
[103] DA Annex Standard Contractual Clauses, EU-Kommissionen, 4. Juni 2021, side 23 og https://kammeradvokaten.dk/nyheder-viden/nyheder/2021/06/nye-standardkontraktbestemmelser-for-internationale-overfoersler-vedtaget
[104] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, punkt 47 og https://www.datatilsynet.dk/internationalt/internationalt-nyt/2021/jun/edpb-har-vedtaget-endelige-anbefalinger-om-supplerende-foranstaltninger.
[105] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, punkt 43.

3.1.6 25. marts 2022: Principiel aftale i stand mellem EU-Kommissionen og USA omkring nyt overførselsgrundlag

Den 25. marts 2022 offentliggjorde EU-Kommissionen[106] og Det Hvide Hus[107] i en fælles erklæring, at EU og USA nu har indgået en principiel aftale omkring et nyt *Trans-Atlantic Data Privacy Framework*, som altså skal fungere som en erstatning til den nu ugyldige Privacy Shield-afgørelse. Dette er indtil videre blot en politisk erklæring fra begge parter og EDPB udtaler da også i den forbindelse, at denne erklæring ikke statuerer et lovligt overførselsgrundlag, som kan anvendes af dataeksportører. Situationen er således fortsat uændret indtil en konkret aftale bliver sendt til offentlig høring[108].

3.1.7 Opsamling på begivenhederne siden Schrems II-dommen

Som det ses af ovenstående afsnit, er der endnu ikke kommet en stedfortræder til Privacy Shield-afgørelsen, som der kan anvendes som overførselsgrundlag, jf. GDPR art. 45, stk. 3. Derfor bør dataeksportørerne, som tidligere anvendte Privacy Shield-afgørelsen, nu anvende standardkontraktsbestemmelser som overførselsgrundlag. Det bør i den forbindelse nævnes, at der findes, som tidligere beskrevet, flere overførselsgrundlag, men henset til nærværende fremstillings nærmere afgrænsede behandlingsområde, emnet som helhed og fokusset i Schrems II-dommen, vil der alene fokuseres på overførselsgrundlaget efter GDPR art. 46, stk. 2, litra c). Netop de nye reviderede standardkontraktsbestemmelser og anbefalingerne fra EDPB skal nemlig danne grundlag for mange dataeksportørers vurdering af overførsler til tredjelande.

3.2 Hvordan kan dataansvarlige så bringe databehandlingen i overensstemmelse med gældende ret på baggrund af Schrems II-dommen?

I det følgende vil der blive taget udgangspunkt i Virksomhed X, som er en fiktiv dansk IT-virksomhed, som anvender en *cloud service provider* (herefter "CSP") til at opbevare og behandle personoplysninger for sine brugere af dennes applikation der indeholder brugernes personoplysninger. Persondataen består af navn, telefonnummer og e-mailadresse. Virksomhed X anvendte Microsoft som CSP, som var selvcertificeret og tilmeldt under Privacy Shield. Efter Schrems II-dommen skal Virksomhed X finde ud af hvordan de fortsat lovligt kunne anvende Microsoft, som de anvender til intern kommunikation, IT-infrastruktur, intranet mv. Det lægges desuden til grund, at Virksomhed X ikke har mulighed for at anvende nogle af de andre overførselsgrundlag i GDPR art. 46, stk. 2 og må derfor ty til standardkontraktsbestemmelser. Formålet med at anvende en fiktiv virksomhed er at have nogle faste holdepunkter undervejs og konkretisere indholdet på en måde der relaterer sig til den praktiske verden.

Det netop beskrevne fiktive scenarie anvendes, da mange europæiske private - såvel som offentlige - aktører, anvender CSP'er så som Microsoft, Google, Oracle og Amazon til deres IT-

[106] https://ec.europa.eu/commission/presscorner/detail/es/ip_22_2087
[107] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/
[108] Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework (https://edpb.europa.eu/system/files/2022-04/edpb_statement_202201_new_trans-atlantic_data_privacy_framework_en.pdf)

infrastruktur og altså dermed alt fra *hosting*, drift og vedligehold af deres online platforme, applikationer mv. Det er især her, at mange aktører har haft udfordringer. Udgangspunktet ved disse CSP'er er, at man som europæisk virksomhed udelukkende får opbevaret og behandlet sin data i datacentre, som er indenfor EU/EØS, da der ellers ville være tale om en overførsel til et tredjeland. Dette udgangspunkt har med Schrems II-dommen vist sig ikke, at være effektivt med henblik på at holde overførslerne udelukkende indenfor EU, da enhver aktør, som har hjemme i USA kan blive genstand for myndighedsanmodninger. Dette medfører, jf. Schrems II-dommen, at der er tale om en overførsel til et tredjeland da offentlige myndigheder i USA kan få adgang til personoplysninger. En sådan adgang statuerer således også en overførsel, som beskrevet i afsnit 3.3.1. I det følgende vil undersøgelsen gå igennem de trin, som dataeksportører anbefales at gå igennem efter Schrems II-dommen når de ønsker at begynde, eller forsætte med, at overfører personoplysninger til USA.

3.2.1 Generelt om EDPB's anbefalinger om supplerende foranstaltninger

EDPB's anbefalinger er opbygget som et sekstrins *roadmap*, hvor dataeksportøren skal igennem alle seks trin for at kunne konkludere om den påtænkte – eller eksisterende – overførsel er i overensstemmelse med GDPR set i lyset af Chartret, jf. Schrems II-dommen. Desuden indeholder anbefalingerne også tre bilag, som skal assistere dataeksportøren blandt andet ved at opliste eksempler på supplerende foranstaltninger og ved at opliste kilder der kan give informationen der er nødvendig for at vurdere tredjelandets love.
Anbefalingerne er udfærdiget på EDPB's eget initiativ og skal efter deres eget udsagn blot anvendes støtte en ensartet anvendelse af GDPR[109]

3.2.2 EDPB's roadmap til vurdering af overførslen

Roadmappet er baseret på en tilgang om den dataansvarlige/databehandlers *accountability* (herefter omtalt som "ansvarlighed") og dennes pligt til aktivt at sikre efterlevelse af kravene i GDPR. Det er således ikke nok at forholde sig passivt og blot "tro" at kravene er opfyldt. Man skal konkret dokumentere, at man efterlever kravene efter princippet om ansvarlighed[110].

3.2.2.1 Step 1: Know your transfers

I den praktiske verden ville dette skridt ofte være forbundet med en fuld kortlægning af alle overførsler af personoplysninger i virksomheden. Dette ville dog ofte være gjort som følge af kravet om fortegnelse jf. GDPR, art. 30. I dette tænkte eksempel skal man dog kun forholde sig til den ene overførsel der sker ved brugen af virksomhedens CSP, som beskrevet indledningsvist. Her er er som nævnt tale om overførsel og opbevaring af personoplysninger i Microsofts europæiske datacentre. For at give et indblik i dybden af dette skridt bør enhver dataeksportør også tage højde for de overførsler der sker længere ude i kæden af databehandlere. I dette tilfælde ville det være det tilfælde, hvor en underleverandør til Microsoft også behandler personoplysningerne. Dette er dog ikke lagt til grund i det fiktive scenarie der anvendes henset til undersøgelsens

[109] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 8.
[110] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 9

fokusområde[111].
Det lægges desuden til grund i det fiktive scenarie, at det alene er Microsoft der har adgang til personoplysningerne og at der ikke er nogen underdatabehandlere involveret i overførslen.

3.2.2.2 Step 2: Identify the transfer tools you are relying on

Som det er lagt til grund indledningsvist her og i specialets afgræsning vil undersøgelsen her ikke kommentere nærmere på andre overførselsgrundlag end det som følger af GDPR, art. 46, stk. 2, litra c). I det fiktive scenarie var Virksomhed X vant til at gøre brug af Privacy Shield-afgørelsen og således anvendte en tilstrækkelighedsafgørelse, jf. GDPR, art. 45, stk. 3. Var situationen fortsat, at der fandtes en tilstrækkelighedsafgørelse, ville det ikke være nødvendigt at gennemgå de resterende skridt i dette roadmap[112].

3.2.2.3 Step 3: Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer

Dataeksportøren skal vurdere om det overførselsgrundlaget effektivt kan sikre, at personoplysningerne et beskyttelsesniveau, der i det væsentlige svarer til det, som er garanteret indenfor EU/EØS. Det der skal undersøges, er navnligt om tredjelandet har lovgivning eller praksis, som omfatter den pågældende overførsel – herunder også personoplysninger, som er i transit fra medlemsstaten til tredjelandet[113].

Vurderingen generelt

Vurderingen skal tage sigte på om offentlige myndigheder i tredjelandet har mulighed for at søge om adgang til dataimportørens data, både med og uden dennes vidende herom. Desuden skal vurderingen også omfatte om offentlige myndigheder kan tilgå, eller få udleveret, data direkte igennem dataimportøren eller igennem en ECSP eller andre kommunikationskanaler. Dette skal ske ved at dataeksportøren undersøger – gerne i samarbejde med dataimportøren – de informationer der findes omkring lovgivningen i tredjelandet, som er offentligt tilgængelige. Vurderingen skal ikke kun tage sigte på lovgivningen alene, men også inddrage de øvrige omstændigheder omkring myndighedernes anvendelse af beføjelser, herunder med henblik på deres tekniske-, finansielle- og menneskelige ressourcer. Myndighedernes praksis kan indeholde fortilfælde, som kan være relevant for vurderingen og derfor bør dette også indgå i vurderingen[114].
For at overskueliggøre denne opgave har EDPB i sin 32. anbefaling anført, at omfanget af undersøgelsen kun er begrænset til lovgivning og praksis, som er relevant henset til den konkrete slags data der overføres. Dette udgangspunkt står i modsætning til det omfang, som Kommissionens undersøgelser tager i forbindelse med en art. 45, stk. 3-vurdering. Dog kan denne vurdering også vise sig ganske omfangsrig da der blandt andet skal tages højde for om

[111] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 10.
[112] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 12.
[113] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 14.
[114] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 14.

dataimportøren kan være underlagt nogle love som følge af den sektor den arbejder indenfor, om dataimportøren bruger underdatabehandlere, om dataene er krypteret mv.
EDPB understreger dog, at det der skal lægges særligt fokus på i vurderingen, er om dataimportøren eller de personoplysninger der overføres, kan blive genstand for et indgreb fra en myndighed, således at personoplysningerne bliver tilgængelige for denne. Også her – ligesom EUD lagde til grund i Schrems II-dommen – kan sådanne indgreb fra et persondatabeskyttelsesperspektiv godt ske ud fra et proportionalitetsprincip. Det er især de hensyn der er listet i GDPR, art. 45, stk. 2, som er relevante at vurdere her[115]. Det kan være en svær vurdering at tage for en dataeksportør, men EDPB anbefaler, at man anvender Chartrets artikel 47 og 52 som reference i denne vurdering. Desuden anbefaler de også, at man i denne vurdering inddrager EDPB's anbefalinger om de væsentlige garantier ved overvågningsforanstaltninger.
Dataeksportørens undersøgelse kan nå frem til at tredjelandet ikke har nogen problematisk lovgivning henset til den specifikke overførsel, men hvis ikke dataeksportøren har undersøgt om det forholder sig anderledes i praksis, så har undersøgelsen ikke været dybdegående nok. Der er en risiko for at praksis forholder sig anderledes end den formelle lovgivning. Igen kan man ikke blot forholde sig til – og stole på - det juridiske, da man skal foretage en vurdering på et fuldt oplyst grundlag. På samme måde kan man i tilfælde af mangel på lovgivning eller informationer om lovgivning heller ikke udlede, at de registrerede så per automatik er garanteret et tilstrækkeligt beskyttelsesniveau. Det forholder sig på samme måde, hvis man efter sin undersøgelse fortsat er i tvivl om, hvor vidt de registreredes rettigheder kan blive krænket. I et sådant tilfælde skal man også være på den sikre side ved at arrangere sig med supplerende foranstaltninger således, at der ikke længere er en usikkerhed[116].
Man kunne som dataeksportør fristes til at afkræve sin dataimportør, at de registreredes rettigheder sikres i databehandleraftalen eller handelsvilkårene, men selvom en dataimportør kontraktuelt forpligter sig til, at de registrerede kan udøve deres rettigheder efter GDPR skal dataeksportøren stadig vurdere om dette konkret kan garanteres på baggrund af lovgivningen i tredjelandet.

EDPB har i sin 43. anbefaling introduceret en mulighed for, at dataeksportøren kan foretage overførslen uden at implementere supplerende foranstaltninger. Dette betyder, at en dataeksportør kan foretage overførslen, hvis at denne ikke har nogen grund til at tro, at den problematiske lovgivning bliver anvendt i praksis på de personoplysninger der overføres eller imod den dataimportør, som der overføres til. Der følger dog et dokumentationskrav med til denne mulighed, som generelt gør sig gældende ud fra princippet om ansvarlighed. Dataeksportøren skal således kunne dokumentere detaljere, hvorfor denne og dennes dataimportør ikke har nogen grund til at tro, at den problematiske lovgivning kan påvirke overførslen. Dokumentationen skal baseres på den tilgængelige information om lovgivningen i tredjelandet og dernæst på øvrige informationer. Der stilles dog krav om at disse informationer er relevante, objektive, pålidelige, verificerbare og offentligt tilgængelige (herefter "kvalitetskrav"). Dataeksportøren skal også

[115] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 16.
[116] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 17.

vurdere og dokumentere, at informationerne opfylder kvalitetskravene[117]. Det bør desuden indgå i vurderingen, om dataimportøren har haft nogle tidligere erfaringer med offentlige myndigheders anmodninger. En mangel på erfaringer kan ikke anvendes til at udlede noget om risikoen for om sådanne myndighedsanmodninger kan risikere at blive fremsendt til dataimportøren i praksis. Det skal ses i sammenhæng med de øvrige informationer og beslutningen på baggrund af vurderingen skal således altid træffes på et fuldt oplyst grundlag.
Når vurderingen er færdiggjort, kan konklusionen enten være, at overførslen kan ske lovligt henset til de registreredes mulighed for effektivt at håndhæve sine rettigheder i tredjelandet eller at den kun kan ske, såfremt der implementeres supplerende foranstaltninger til at kompensere for den manglende databeskyttelse i tredjelandet.

Virksomhed X: Problematisk lovgivning i teorien

I Virksomhed X's situation er tredjelandet – ligesom i Schrems II-dommen – USA. Det gør roadmappets tredje skridt nemmere, da Schrems og den irske tilsynsmyndighed allerede har fundet frem til den problematiske lovgivning. Der kan potentielt set være introduceret ny lovgivning siden de præjudicielle spørgsmål blev forelagt EUD i forbindelse med dommen og det ville derfor ikke være nok, at Virksomhed X alene konkluderer noget med baggrund i netop denne dom. Det lægges dog til grund i det følgende, at Virksomhed X grundigt har undersøgt USA's lovgivning og nået frem til at kun CLOUD Act er kommet til siden da, men at den øvrige problematiske lovgivning forsat eksistere.
Det væsentligste fokus i Virksomhed X's situation skal lægges på om de aktuelle personoplysninger og/eller dataimportøren falder indenfor både det teoretiske- og praktiske anvendelsesområde af disse overvågningsprogrammer.
Hvis man alene kigger på den teoretiske del, tyder alt på at lovgivningen bag overvågningsprogrammerne i USA kan anvendes meget bredt. Det blev blandt andet anført af den forelæggende ret i Schrems II-dommen, at National Security Agency (herefter "NSA") kan tvinge sig til at kopiere og filtrere internettrafikken hos CSP'er[118]. Desuden blev det også anført, at EO 12.333 i nogle tilfælde giver mulighed for at få adgang til personoplysninger, som er i transit til USA. Dette sker inden, at oplysningerne ankommer til USA, hvor de først i det øjeblik er underlagt FISA's bestemmelser. I denne del af overførslen, hvor data endnu ikke er ankommet til USA, og hvor der kan udføres efterretningsaktiviteter på baggrund af EO 12.333, er der ingen lovregulering[119]. Det afgørende her er dog om FISA's bestemmelser i det hele taget omfatter Microsoft, som er Virksomhed X's CSP.
Der skal, jf. FISA, være tale om en *ECSP* for at man er indenfor FISA's anvendelsesområde[120]. Det er således relevant for Virksomhed X at undersøge om Microsoft er en ECSP, i FISA's forstand, for at vide om overførslen juridisk er omfattet af FISA. Under FISA defineres det, jf. 50 U.S.C. § 1881 som fem forskellige aktører. Henset til undersøgelsens omfang, vil der blive fokuseret på "*(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18"*, da de

[117] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 18.
[118] C-311/18, præmis 62 og jf. 50 U.S.C. § 1881(b)(4).
[119] C-311/18, præmis 63.
[120] https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap36-subchapVI-sec1881.htm

andre ikke har relevans i denne forbindelse[121]. Definitionen i *section 2510 of title 18* indebærer det "*…any service which provides to users thereof the ability to send or receive wire or electronic communications*[122]". Termen *electronic communications* indebærer blandt andet enhver overførsel af "*… data … transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system*". Disse to definitioner er begge formuleret på en måde, så de dækker bredt. For at undgå fejlfortolkning og for at foretage vurdering på det bedst oplyste grundlag, i tråd med EDPB's anbefalinger, bør man også inddrage andre kilder. Blandt andet har Datenschutzkonferenz (herefter "DSK"), som er en sammenslutning af samtlige tyske databeskyttelsesmyndigheder udgivet en "Expert Opinion", hvor de har bedt ekspert i amerikansk national sikkerhedslov*, Professor* Stephen I. Vladeck, kommentere på især omfanget af FISA's anvendelsesområde. Vladecks kommentarer i udtalelsen bakker også op om, at anvendelsesområdet er meget bredt, som det også kan udledes af formuleringerne ovenfor. Ifølge Vladeck skal definitionen i 18 U.S.C. § 2510(15), forstås således, at enhver virksomhed der forsyner sine ansatte med en e-mail tjeneste skal betragtes, som en ECSP. Dette er lagt til grund af amerikanske domstole i en række sager[123].

Delkonklusion

Det må således kunne konkluderes, at Microsoft er en ECSP i den amerikanske lovgivnings forstand og er således omfattet af FISA 702. Virksomhed X's brug af Microsoft som CSP medfører dermed – ifølge lovgivningen – at der ikke kan garanteres et tilstrækkeligt beskyttelsesniveau. Henset til EDPB's anbefalinger har Virksomhed X dog stadig to muligheder for at kunne fortsætte overførslen. Den første mulighed er, at Virksomhed X kan vælge at lade overførslen fortsætte alligevel såfremt denne ikke har nogen grund til at tro, at førnævnte problematiske lovgivning ikke i praksis vil blive anvendt overfor Microsoft eller på de personoplysninger, som der overføres[124].

Virksomhed X: Problematisk lovgivning i praksis

Ifølge anbefalingerne kan denne vurdering, udover fortolkningen og anvendelsen af loven, foretages på baggrund af al information som der findes relevant. En liste med eksempler er blandt andet oplistet i bilag 3 til anbefalingerne. Også her gælder det, at informationen der anvendes i vurderingen, lever op til kvalitetskravene. For at få en forståelse for hvordan lovgivningen anvendes i praksis henset til myndighedsanmodninger mod en ECSP, er det relevant at inddrage erfaringer fra både Microsoft selv og fra andre sammenlignelige dataimportører.
Hvis man eksempelvis tager et kig på dokumentationen fra Microsofts største konkurrent, Amazon Web Services (herefter "AWS"), vil man kunne få et indblik i, hvilke erfaringer de – en lignende virksomhed - har med anmodninger fra myndigheder. AWS' opdeling af oplysningerne i *non-content,* som overordnet set må udledes at svare til almindelige ikke-følsomme oplysninger efter GDPR og *content,* som groft sagt må udledes at udgøre både ikke-følsomme og følsomme personoplysninger efter GDPR, har ikke nogen nævneværdig betydning da de begge indeholder

[121] https://www.law.cornell.edu/uscode/text/50/1881
[122] Section 2510 of title 18, nr. 12 (https://www.law.cornell.edu/uscode/text/50/1881)
[123] Expert Opinion on the Current State of U.S. Surveillance Law and Authorities from Prof. Stephen I. Vladeck, University of Texas School of Law (https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf), side 5.
[124] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 18.

personoplysninger, jf. GDPR art. 4, nr. 1. Der har alene i andet halvår af 2021 været udleveret oplysninger i 753 tilfælde. Det fremgår at lidt 52,2% af disse anmodninger stammer fra USA. Det fremgår dog ikke af rapporten, hvor mange af disse der stammer fra en anmodning under FISA, da rapporten viser antallet af anmodninger baseret på ransagningskendelser, øvrige retskendelser og stævninger[125]. Microsoft udgiver også denne slags rapporter, hvor de er inddelt efter typen af anmodninger. Dette betyder med andre ord, at de har en rapport der kun vedrører anmodninger under FISA. Det fremgår af Microsofts' rapport, at der i første halvår af 2021[126] var mellem 0 og 499 anmodninger om udlevering/adgang til både *content* og *non-content* oplysninger. Der har på baggrund af disse været imellem 12000 og 12499 konti, som har været berørt af disse FISA-anmodninger. På samme måde, som ved AWS, er der ingen forlydender om hvor ejerne af disse konti er lokaliseret, men der må antageligvis være kunder fra EU/EØS i blandt. Selv hvis denne undersøgelse var nået frem til, at der ikke var nogen grund til at tro, at Microsoft eller personoplysningerne ville blive genstand for FISA-anmodninger, ville det ifølge anbefaling 47 ikke være brugbart såfremt, at lovgivningen i tredjelandet kan forbyde Microsoft at offentliggøre information, eller notificere sine kunder, om udleveringen af disses personoplysninger. Ved et nærmere eftersyn af både Microsofts og AWS' rapporter, oplyser de begge, at de er underlagt nogle *"constraints on what we can publish"* [127] og *" Unless prohibited from doing so…"* [128].

Virksomhed X kan derfor ikke fortsætte overførslen henset til EDPB's anbefaling 43.3 og 47. I så fald er den eneste mulighed for at fortsætte overførslen på lovlig vis, ved at implementere supplerende foranstaltninger, som også EUD slog fast i Schrems II-dommen.

3.2.2.4 Step 4: Adopt supplementary measures

Supplerende foranstaltninger er tiltag, som bliver implementeret af dataeksportøren alene, eller i samarbejde med dataimportøren, for at kompensere for den manglende databeskyttelse der er konkluderet under tredje skridt i dette roadmap. Du supplerende foranstaltninger er netop "supplerende" da de skal fungere, som et ekstra værn i forlængelse af det overførselsgrundlag i GDPR's art. 46, som danner det juridiske fundament for overførslen. De supplerende foranstaltninger kan opdeles i tre forskellige kategorier[129]:

- **Kontraktuelle foranstaltninger**
  Et eksempel kunne være at aftale en *warrant canary*-ordning. Dette betyder, at udbyderen af en cloudtjeneste enten kan advare om at de har modtaget en myndighedsanmodning – eller hvis de er forbudt denne praksis – advarer om at de "ikke" har modtaget en[130]. Generelt set vil der være tale om kontraktuel forpligtelse for dataimportøren, som led i at sikre en tilstrækkelig databeskyttelse.[131]

[125] https://d1.awsstatic.com/Information_Request_Report_December_2021_bia.pdf
[126] Tallene for andet halvår af 2021 er ikke blevet offentliggjort endnu.
[127] https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report?activetab=pivot_1:primaryr2
[128] https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF
[129] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 22 (anbefaling nr. 52)
[130] https://www.comparitech.com/blog/vpn-privacy/warrant-canary/
[131] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 22 (anbefaling nr. 92)

- **Tekniske foranstaltninger**
  Tekniske og organisatoriske foranstaltninger er en velkendt term fra GDPR, hvor det er nævnt mange gange og formentlig bedst kendt fra art. 32, stk. 1 omkring behandlingssikkerhed. Det er ikke defineret i GDPR, som mange andre af dens termer er, men der er givet eksempler i blandt andet art. 32, stk. 1. En teknisk foranstaltning kan således være implementering af en teknisk funktion i virksomhedens IT-infrastruktur, som gør at personoplysningerne bliver krypteret eller pseudonymiseret, så de ikke længere er personhenførbare.

- **Organisatoriske foranstaltninger**
  Andet led af termen beskrevet ovenfor vil være en foranstaltning, som man implementerer i sin organisation. Her er der altså tale interne politikker, procedurer, kontroller, *audits* og andre værktøjer, som anvendes til at sikre en bestemt adfærd og ensrettet behandling blandt aktørerne i virksomheden. Dette kunne, henset til eksemplet givet omkring tekniske foranstaltninger, være en procedure der skal sikre, at krypteringen er effektiv – eksempelvis en politik der regulerer virksomhedens håndtering af krypteringsnøgler eller lign.

Det fremgår dog af anbefalingerne, at kontraktuelle- og organisatoriske foranstaltninger alene generelt ikke tilstrækkeligt kan kompensere for manglerne i forbindelse med den problematiske lovgivning. Årsagen hertil finder man blandt andet i Schrems II-dommen, hvor en af forudsætningen for de forelagte spørgsmål, blandt andet var, at man jo ikke kan binde en tredjepart (offentlige myndigheder) på baggrund af en aftale indgået mellem dataimportøren og dataeksportøren. Så uanset hvor meget man forsøger at aftale sig ud af i medfør af standardkontraktsbestemmelser eller hvor mange procedurer og politikker man implementerer hos begge parter, så vil det næppe være nok til at sikre personoplysningerne mod adgang fra myndigheder i tredjelandet, jf. de identificerede love i tredje skridt. De kan dog fungere, som et supplement og til at styrke den samlede beskyttelse såfremt der er implementeret en form for tekniske foranstaltninger, som kan sikre et tilstrækkeligt beskyttelsesniveau[132].
Dermed er det vigtigste for Virksomhed X i denne henseende at finde frem til en teknisk foranstaltning, som effektivt kan sikre et tilstrækkeligt beskyttelsesniveau - selvom Microsoft har lovet kontraktuelle forpligtelser. Microsoft forklarer blandt andet at man vil "*challenge every government request for an EU public sector or commercial customer's personal data—from any government—where there is a lawful basis for doing so.*"[133]. Dette har de gjort til en kontraktuel forpligtelse i deres databehandleraftale, hvor det fremgår af Appendix C – Additional Safeguards Addendum[134]. Desuden har de truffet flere kontraktuelle forpligtelser så som skadesløsholdelse af den registrerede hvis denne har lidt enten økonomisk eller ikke-økonomisk tab. Sådanne kontraktuelle foranstaltninger er dog ikke effektive, idet at myndighederne ultimativt kan få adgang til personoplysninger uanset Microsofts bestræbelser.

[132] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 22 (anbefaling nr. 53)
[133] https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/
[134] https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

For at finde frem til, hvilken teknisk foranstaltning der er effektiv, bør man kigge på karakteren af overførslen. Herunder kan man inddrage i sin vurdering om personoplysningerne er *plain text* eller krypteret, om de er af særlig følsom karakter, om de overføres videre til en underdatabehandler i tredjelandet eller til et andet tredjeland mv.[135]
At vurdere ud fra eksemplerne, som er angivet i bilag 3 til anbefalingerne samt øvrige kilder, er det primært kryptering og pseudonymisering der er relevante kandidater til effektive tekniske foranstaltninger[136].
For Virksomhed X er udfordringen, at Microsoft kan blive bedt om at udlevere personoplysninger til amerikanske myndigheder under FISA 702. Hvis Microsoft kan læse eller tilgå personoplysninger, så kan amerikanske myndigheder ultimativt også. Derfor skal Microsoft slet ikke have mulighed for at læse personoplysningerne. Den eneste måde det kan ske på er at gøre personoplysningerne ikke-personhenførbare ved at pseudonymisere dem. Den anden mulighed er, at Microsoft ikke skal kunne læse personoplysningerne da de er krypteret og således ikke-personhenførbare.
Ved nærmere eftersyn af bilag 3 til anbefalingerne, kan man ved *Use Case 6* se, at Virksomhed X ikke kan anvende kryptering, som teknisk foranstaltning i tilfælde af at personoplysninger skal være læselige for at CSP'en kan tilvejebringe ydelsen. Dette vil eksempelvis være, hvis CSP'en i sin behandling af data bliver nødsaget til at behandle navn, lokation, e-mailadresse mv. for at udføre en handling. Dette er tilfældet ved Virksomhed X da de har brug for funktionaliteten, så som support ydelser mv., hvilket ikke er muligt, hvis der ikke kan opereres med det de fornødne personoplysninger. Desuden besidder Microsoft også krypteringsnøglerne, kan dekryptere personoplysningerne[137]. Det afgørende for at krypteringen er effektiv, er således om CSP'en kan dekryptere personoplysningerne. Henset til netop denne diskussion er det relevant at inddrage en relativ ny vejledning (Marts 2022) udgivet af Datatilsynet omkring brugen af netop cloudtjenester, som Microsoft Azure jo netop er.

I Datatilsynets cloudvejledning oplistes der en række eksempler på foranstaltninger der er effektive og på foranstaltninger som ikke er effektive. Heriblandt er der ét enkelt eksempel som adskiller sig fra de andre. Det er et eksempel, hvor kryptering udgør en tekniske foranstaltning og som Datatilsynet vurderer som værende effektivt i forbindelse med brug af en cloudtjeneste. Eksemplet tager udgangspunkt i en virksomhed, som ud fra beskrivelsen er identisk med Virksomhed X. Virksomheden udvikler en applikation, som anvendes til tracking af sundhedsoplysninger. Når brugerne indtaster informationer i applikationen, sendes disse direkte til en svensk virksomhed, som krypterer personoplysningerne og opbevarer krypteringsnøglen. Når personoplysningerne er krypteret, videresendes de til CSP'ens datacentre, som ligger i EU, selvom at virksomheden har hovedkvarter i USA. Når brugeren skal læse data i applikationen hentes de kryptererede data fra clodutjenestens datacenter og dekrypteres herefter af det svenske firma, som endeligt sender personoplysningerne i klartekst ud til brugeren af applikationen. På denne måde er det kun krypteret rådata, som sendes til behandling eller

[135] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 22 (anbefaling nr. 54)
[136] Vejledning: Overførsel af personoplysninger til tredjelande, Juli 2021, 3. udgave, Datatilsynet; https://kromannreumert.com/nyheder/bliv-klogere-paa-nye-anbefalinger-om-krav-til-dataoverfoersel-til-tredjelande, https://www.pwc.dk/da/artikler/2021/06/nyt-om-schrems-ii.html og GDPR, art. 32, stk. 1, litra a)
[137] Jf. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 35

opbevaring hos CSP'en. Når CSP'en kun har adgang til den krypterede rådata, er der således ikke længere tale om personhenførbare personoplysninger indtil de igen er dekrypteret. Selvom CSP'en skulle blive pålagt at udlevere bestemte oplysninger, er der ikke tale om en overførsel af personoplysninger, da hverken CSP'en eller den offentlige myndighed kan læse dataen[138]. For at læse dataen vil det kræve at de har dekrypteringsnøglen, som netop er opbevaret hos det svenske firma i EU. Dette er også helt i tråd med kravet i EDPB's 84. anbefaling, hvorefter kryptografiske nøgler skal være "*retained solely under the control of the data exporter, or by an entity trusted by the exporter in the EEA or under a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA*"[139]. Denne måde hvorpå man helt afskærer sin CSP fra at få adgang til personoplysninger i klartekst viser sig derfor således som en af de få effektive tekniske foranstaltninger, som man kan anvende ved amerikanske cloudtjenester uden at handle i strid med GDPR's kapitel V og således også Chartrets art. 7, 8 og 47.
For Virksomhed X betyder det, at de med den fornødne dokumentation og supplerende tekniske foranstaltninger, juridisk set, godt kan fortsætte sin anvendelse af Microsoft Azure til hosting af deres applikation. Dette er dog ikke uden konsekvenser. Hvis Virksomhed X vælger af følge eksemplet, fra Datatilsynets, vil de give afkald på nogle væsentlige funktioner, som blandt andet også er en årsag til at de har valgt at anvende Microsoft Azure i første omgang. I det netop nævnte eksempel har Virksomhed X ikke længere mulighed for at anvende nogle funktioner, som fordrer oplysninger i klartekst. Et håndgribeligt eksempel kunne være support fra CSP'en. Hvis Virksomhed X står med en udfordring, som kræver at en supporter hos Microsoft Azure skal hjælpe, vil det som udgangspunkt være nødvendigt at der er adgang til personoplysninger. Selvom der er flere CSP'er, som planlægger at lave en "EU-cloud", hvor man også kun anvender support personale, som er placeret i EU, ville dette fortsat ikke være nok så længe selskabet har base i USA og personoplysningerne er tilgængelige i klartekst for support personalet[140].
Der er generelt set tale om enhver behandlingsaktivitet, som CSP'en skal udføre, som ikke kan anvendes, såfremt personoplysningerne er fuldt krypteret, men support eksemplet er fremhævet for forståelsens skyld. Anvendelsen af cloudtjenesten er således reduceret til kun at være til opbevaring af data med henblik på at hoste og drifte applikationen, mens de fleste andre funktioner i Microsoft Azure ikke kan anvendes[141]. For mange virksomheder, herunder Virksomhed X, er dette ikke en virksom løsning. Det forretningsmæssige formål med at etablere eller fortsætte anvendelsen af Microsoft Azure er netop for at anvende de mange tjenester som Microsoft udbyder. Flere aktører i det private og offentlige ønsker netop ikke at skifte udbyder da eksempelvis Microsoft og Googles produkter er en integreret del af deres IT setup, lige fra Microsoft Teams, Outlook, 365, Gmail, Google Workspace, Google Analytics mv. Det er ikke altid muligt at finde en leverandør der kan tilbyde lige så gode produkter i EU/EØS, som det er fra de førende CSP'er fra USA. Dette bliver behandlet nærmere i afsnit 3.3.

Det kan således konkluderes, at der findes en mulighed, rent juridisk, til at træffe effektive supplerende foranstaltninger ved hjælp af kryptering med opbevaring af krypteringsnøglen hos en

[138] Vejledning: Overførsel af personoplysninger til tredjelande, Juli 2021, 3. udgave, Datatilsynet; https://www.version2.dk/artikel/datatilsynet-saadan-kan-du-bruge-amerikansk-cloud-lovligt
[139] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 30 (anbefaling nr. 84)
[140] https://www.version2.dk/artikel/datatilsynet-tech-giganternes-eu-cloud-goer-dig-ikke-gdpr-sikker
[141] https://azure.microsoft.com/en-us/overview/what-is-azure/

betroet tredjepart indenfor EU/EØS. I praksis betyder det dog, at man som dataeksportør giver afkald på vigtige funktioner, da brugen reelt set bliver reduceret til opbevaring og derfor bliver de store anstrengelser for at sikre lovligheden også lidt forgæves, da man i så fald lige så godt kan finde en leverandør i EU.

3.2.2.5 Step 5: Procedural steps if you have identified effective supplementary measures

Femte skridt drejer sig om anbefalinger til hvilke formelle skridt der bør tages, såfremt man har fundet en effektivt supplerende foranstaltning. Det kunne eksempelvis være, at man skulle underrette den lokale tilsynsmyndighed eller indhente en tilladelse fra disse henset til det overførselsgrundlag man anvender. Ifølge anbefalingerne er det ikke nødvendigt at involvere tilsynsmyndigheden så længe de supplerende klausuler i kontrakten ikke er i modstrid med standardkontraktsbestemmelser. Begge parter skal desuden også sikre sig at de nye supplerende bestemmelser ikke kan fortolkes på en sådan måde, at de begrænser de rettigheder, som følger af GDPR's kapitel V.

3.2.2.6 Step 6: Re-evaluate at appropriate intervals

Det sjette skridt i anbefalingerne er blot til for at sikre, at dataeksportøren forstår, at man aktivt skal foretage sig evalueringer og ikke blot passivt kan forvente, at man efterlever kravene i lovgivningen. Dataeksportøren skal således med jævne mellemrum reevaluere situationen og eksempelvis holde sig opdateret på ny relevant lovgivning i tredjelandet. Hvis tredjelandet en dag vedtager ny lovgivning som begrænser brugen af krypteringen, ville det være nødvendigt for Virksomhed X at kontrollere om virksomhedens supplerende tekniske foranstaltninger der involverer kryptering fortsat er effektive til at sikre et tilstrækkeligt beskyttelsesniveau.

3.2.2.7 Opsamling

Der eksisterer fortsat problematisk lovgivning i USA. Det er således nødvendigt med supplerende foranstaltninger for at kompensere for de "huller" der er i beskyttelsen som følge af disse love. Dog er det for Virksomhed X muligt at træffe tilstrækkeligt effektive supplerende foranstaltninger for at sikre et beskyttelsesniveau der i det væsentligste svarer til det som følger af EU-retten. Dette kan kun sikres ved rent teknisk at gøre det umuligt for både Microsoft og dermed også de amerikanske myndigheder at læse personoplysninger. Dette kan således gøres ved at pseudonymisere eller kryptere oplysningerne. I Virksomhed X's situation kan en kryptering, som håndteres af en betroet tredjepart i EU/EØS, hvor krypteringsnøglen også er opbevaret hos denne, være et effektivt værn mod problematisk lovgivning, da Microsoft kun selv har adgang til krypteret rådata. Dog ville en sådan løsning i praksis betyde, at cloudtjenesternes anvendelse er reduceret til opbevaring, hvilket ofte blot udgør en brøkdel af den ønskede anvendelse for Virksomhed X. Hvis ikke en sådan supplerende foranstaltning træffes skal dataeksportøren straks suspendere overførslen og kræve alt personoplysningerne tilbageleveret[142].

Spørgsmålet er så om dataeksportører i Danmark (og EU generelt) enten har truffet sådanne relativt vidtgående foranstaltninger eller om de har valgt at udskifte deres amerikanske

[142] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, side 23, anbefaling 57.

cloudtjenester med et GPDR-compliant alternativ. En tredje mulighed er jo også, at dataeksportørerne har valgt at fortsætte overførslerne selvom de fornødne supplerende foranstaltninger ikke er truffet og således bryder GDPR.
Hvordan en kompleks juridisk problemstilling bevirker en så stor del af private- og offentlige aktører i en fundamental del af deres IT-infrastruktur, er en meget relevant diskussion ud fra et praktisk og samfundsøkonomisk synspunkt. Det er ikke utænkeligt at en udskiftning af amerikanske cloudtjenester er en bekostelig affære, imens man også kunne forestille sig, at det kan være en anelse konkurrenceforvridende for EU-baserede virksomheder at disse ikke længere kan anvende markedets bedste IT-produkter – eller i hvert fald ikke til deres fulde potentiale.

3.3 Tilsynsmyndighedernes praksis efter Schrems II-dommen

Man har siden Schrems II-dommen set flere aktører, som har fortsat brugen af flere af de amerikanske cloudtjenester, herunder Helsingør Kommune, som fortsat anvender Googles læringsværktøjer, på trods af identificeret risiko for elevernes ret privatliv krænkes, jf. Schrems II-dommen[143]. Helsingør Kommune mener blandt andet at de ikke kan drive folkeskole uden Googles tjenester[144]. Desuden har man også set, hvordan store aktører som Dansk Erhverv og Dansk Industri har været ude og forklarer hvordan sanktionering ved brug af Google Analytics ville have store konsekvenser for små- og mellemstore virksomheder[145]. Region Hovedstaden har eksempelvis også haft problemer med Sundhedsplatformen, som bliver udviklet og driftet af den amerikanske leverandør Epic via AWS. En sådan løsning kan også være svær at udskifte på grund af omkostningerne. Man argumenterer blandt andet i Kommunernes Landsforening for at en udskiftning af alle amerikanske cloudtjenester, ville være medfører "*voldsomme beløb*" og forklarer at de føler, at de er i et "*limbo, hvor vi afventer, at der kommer et nyt overførselsgrundlag*"[146].
Alt dette peger på, at flere aktører både i det private og i det offentlige fortsat ønsker at bruge amerikanske cloudtjenester – også selv om det har vist sig problematisk og måske endda i strid med GDPR.

Det er tydeligt at se ud fra ovenstående eksempler, at der fortsat er mange offentlige- og private aktører, som fortsat anvender amerikanske cloudtjenester. Ifølge Eurostat brugte 41% af europæiske virksomheder cloudtjenester i 2021[147]. Med tanke på at over 70% af cloud computing markedet er domineret af amerikanske udbydere af cloudtjenester[148], kan det med rimelighed antages, at der fortsat er mange private- og offentlige aktører, som fortsat anvender amerikanske

[143] https://www.version2.dk/artikel/helsingoer-skoler-beholder-google-vi-maa-leve-med-risici-boernenes-databeskyttelse
[144] https://www.version2.dk/artikel/helsingoer-kommune-folkeskolen-kan-ikke-koere-uden-google
[145] https://www.version2.dk/artikel/analytics-forbud-truer-det-vil-have-store-konsekvenser-danske-virksomheder og https://www.version2.dk/artikel/dansk-virksomhed-frygter-analytics-forbud-vi-bliver-fuldstaendig-blaendet
[146] https://www.version2.dk/artikel/kl-om-afsked-med-amerikansk-cloud-det-har-store-oekonomiske-og-administrative-konsekvenser
[147] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises
[148] https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

cloudtjenester på trods af Schrems II-dommen. Det kan også med rimelighed antages, at mange europæiske aktører ikke har truffet effektive supplerende foranstaltninger, henset til det, som er konkluderet i afsnit 3.2.2.7. Hvis man udelukkende anvendte, Microsoft til opbevaring ville det ikke være muligt for aktører i EU, at anvende eksempelvis Microsoft Teams, som jo netop er et meget udbredt samarbejdsværktøj i Danmark[149].
Det interessante er så, hvorfor mange fortsat anvender amerikanske cloudtjenester, når det nu er slået fast, at det ikke kan gøres lovligt, så længe udbyderne af disse, har adgang til personoplysninger i fritekst.

Den åbenlyse forklaring er, at der er tale om en omkostningstung proces, som påvirker afgørende funktioner i virksomhedens IT-infrastruktur. Men det blotte faktum, at noget er ulovligt, plejer som regel netop at afholde virksomheder og offentlige aktører fra at gøre noget. Dog forholder det sig ikke således denne gang. En del af forklaringen kan formentligt også findes i, at det kan være en kompleks øvelse at udfører en dybdegående juridisk analyse af et andet lands lovgivning. Især lande, som ligger udenfor EU. Dette bør dog ikke være nogen undskyldning. Der er også tale om store virksomheder og kommuner, som anvender amerikanske cloud, herunder Helsingør Kommune med Microsoft og eksempelvis Netcompany, som bruger AWS[150]. Desuden har EUD også gjort meget af vurderingsarbejdet på forhånd i Schrems II-dommen.

Lige nu virker der til at være fornemmelse af, at europæiske aktører befinder sig i et limbo, hvor man venter på, at der kommer en politisk løsning imellem EU og USA, som en slags "Privacy Shield version 2.0"[151].
Kilden til denne lidt "laissez faire" tilgang, som der hersker kan formentlig findes flere steder, men et klassisk adfærdsregulerende værktøj, til at få virksomheder til at følge loven, er økonomiske sanktioner. Økonomiske sanktioner er netop en af årsagerne til at GDPR har fået den status, som den har i modsætning til sin forgænger i Direktiv 95/46. Ifølge GDPR, art. 83, stk. 5, kan virksomheder risikere en bøde på helt op mod 4% af deres globale omsætning. Med økonomiske sanktioner, som potentielt set kan komme op i denne størrelsesorden skulle man tro, at de fleste ville være på den sikre side. Det fremgår netop af art. 83, stk. 1, at en administrative bøde pålagt af de nationale tilsynsmyndigheder skal være effektiv, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning. Desuden, som det også er anført i Schrems II-dommen, har de nationale tilsynsmyndigheder også pligt til at suspendere eller forbyde tredjelandsoverførsler, som de ikke mener lever op til et tilstrækkeligt databeskyttelsesniveau. Man skulle derfor foranlediges til at tro, at praksis fra de nationale tilsynsmyndigheder kunne tilskynde dataeksportører til at arrangere sig anderledes med henblik på deres cloud-infrastruktur.

Det er således relevant at kigge på myndighedsudøvelsen i EU omkring tredjelandsoverførsler set i lyset af Schrems II-dommen, for at få en idé om, hvilke – hvis nogen – konsekvenser det har ikke at udskifte sin amerikanske cloud, såfremt effektive foranstaltninger ikke er truffet.

[149] https://itwatch.dk/ITNyt/Brancher/cloud/article12668868.ece
[150] https://www.computerworld.dk/art/260557/kombit-i-dialog-med-netcompany-og-kommunerne-om-aula-efter-schrems-ii-afgoerelse-kan-vaere-i-strid-med-gdpr
[151] https://www.k-news.dk/nyheder/eksperter-schrems-ii-afgoerelsen-efterlader-virksomheder-i-juridisk-limbo; https://www.computerworld.dk/art/259787/eu-er-paa-trapperne-med-loesning-for-schrems-ii

Kigger man udenfor Danmarks grænser, i EU, er stemningen lidt en anden end den som netop er beskrevet ovenfor. Her har 35 svenske myndigheder blandt andet besluttet at droppe amerikanske cloudtjenester og foreslår i en rapport en række alternative løsninger, som myndighederne kan anvende uden at skulle spekulere på om de går på kompromis med borgernes rettigheder [152]. For det første mener de ikke, at det er grund til at bruge en masse tid og ressourcer på, det der i princippet er at sikre sig imod sin egen leverandør, og i stedet vælge en leverandør, hvor brud på GDPR ikke skal være en bekymring og ressourcetung opgave. De forklarer desuden, at brugen af Microsoft Teams vil "*… afsløre store mængder oplysninger for Microsoft på en måde, der er uforenelig med reglerne om databeskyttelse og fortrolighed".* Her har man således taget konsekvensen og begyndt udskiftningen, da man har indset, at den eneste løsning vil være en politisk aftale, som man ikke ved om nogensinde kommer. Da der ikke er tale om en aktør, som har nogen myndighedsbeføjelse indenfor persondataretten, skal dette således ikke anvendes som fortolkningsbidrag til, hvad de nationale tilsynsmyndigheder gør. Dog
har de lokale tilsynsmyndigheder i Østrig, Datenschutzbehörde, afsagt en skelsættende afgørelse i januar 2022, som vil blive kommenteret på i det følgende. Afgørelsen er vigtig fordi den er en af de første afgørelser, siden Schrems II-dommen, som konkret inddrager de omstændigheder, som er relevante i forbindeles vurderingerne fra EDPB's roadmap, step 3 og step 4.

3.3.1 Google Analytics-afgørelserne

Den østrigske tilsynsmyndighed har i januar 2022 grundlæggende dømt brugen af Google Analytics ulovligt, da hverken Google eller dataeksportøren i sagen, ikke har formået at træffe effektive supplerende foranstaltninger imod den problematiske lovgivning. I sagen argumenterede Google for, at de informationer, som der blev indsamlet, ikke var personoplysninger og således ikke omfattet af GDPR. Dette afviste den østrigske tilsynsmyndighed, da man ved kombination af de oplysninger som indsamles, kan identificere en person. Google har også truffet en række supplerende foranstaltninger, som ligesom Microsoft og AWS, lover at udfordre og granske enhver myndighedsanmodning. Dette afviste den østrigske tilsynsmyndighed, som værende effektivt, da det stadig ikke effektivt forhindre de amerikanske myndigheder i at få udleveret personoplysningerne. Desuden har Google truffet en række tekniske foranstaltninger til at kryptere og sikre personoplysningerne ved opbevaring og ved overførsel, men Google har stadig mulighed for at tilgå og læse personoplysningerne i klartekst og derfor også udlevere dem til amerikanske myndigheder. Den østrigske tilsynsmyndighed måtte således også dømme disse foranstaltninger for ikke-effektive. Brugen af Google Analytics er derfor ulovligt i EU ifølge Datenschutzbehörde[153].
På helt samme måde har Frankrigs tilsynsmyndigheder, CNIL, dømt brugen af Google Analytics ulovlig, såfremt man ikke har truffet effektive supplerende foranstaltninger, som den anonyme virksomhed i sagen ikke havde. Dog mener Henning Mortensen, formand for Rådet for Digital Sikkerhed, i tråd med denne opgaves konklusion i afsnit 3.2.2.7, at det ikke er realistisk, at dataeksportørerne kan træffe så effektive foranstaltninger, at man stadig kan bruge Google Analytics til fulde og samtidig afskærme amerikanske myndigheder fra at få adgang til personoplysningerne[154].

[152] https://www.version2.dk/artikel/svenske-myndigheder-vil-skrotte-amerikansk-cloud-her-er-alternativerne
[153] https://www.version2.dk/artikel/skelsaettende-afgoerelse-derfor-dumper-google-analytics-paa-gdpr
[154] https://www.version2.dk/artikel/frankrig-strammer-nettet-om-google-kunder-ulovligt-bruge-analytics-i-eu

Senest har Liechtensteins tilsynsmyndigheder også frarådet virksomhederne i landet at anvende Google Analytics og bakker således op om de østrigske og franske tilsynsmyndigheders afgørelser[155].

Det fremgår af pressemeddelelsen fra den franske tilsynsmyndigheds afgørelse, at man "…*in cooperation with its European counterparts, analysed the conditions under which data collected through the use of Google Analytics was transferred to the United States*"[156]. Man har således samarbejdet med de øvrige europæiske tilsynsmyndigheder undersøgt denne sag. Netop dette samarbejde er nøglen til at anvende GDPR på en ensartet måde, som det er ønsket jf. GDPR, art. 61, stk. 1. Google Analytics-afgørelserne er en del af et sagskompleks, som Schrems står bag igennem sin nonprofitorganisation NOYB, hvor de har indgivet klager til samtlige europæiske tilsynsmyndigheder og således også til Datatilsynet. Dog forholder det sig således, at de danske (og estiske) tilsynsmyndigheder ikke har samme beføjelse, som de øvrige tilsynsmyndigheder, til at udstede administrative bøder direkte, som er bindende, såfremt disse ikke appelleres. Dette betyder blandt andet også, at sagerne ved Datatilsynet ofte vil tage længere tid i modsætning til de øvrige til tilsynsmyndigheder i EU[157]. Slagsiden herved er også, at der kan gå lang tid før man får etableret bødeniveauerne for forskellige overtrædelser[158]. Dermed er det nærliggende at overveje om Datatilsynets manglende kompetence til at udstede administrative bøder direkte kan betyde, at aktører, som ikke har suspenderet sine tredjelandsoverførsler tør at fortsætte, da man ikke frygter en bøde af nogen særlig karakter. Siden GDPR trådte i kraft har en lang række større- og mindre private danske virksomheder og offentlige myndigheder været indstillet til bøder af Datatilsynet. Ud af disse sager, som tæller over 20 sager (maj 2022), er kun ganske få endt med en bøde i sidste ende. Lejre Kommune blev, som den første offentlige myndighed, af Retten i Roskilde dømt til at betale en bøde på 50.000 kr for manglende behandlingssikkerhed[159]. Nordbornholms Byggeforretning, som omsætter for et trecifret millionbeløb årligt, blev idømt at skulle betale 100.000 kr for videregivelse af personoplysninger om strafbare forhold uden hjemmel. Dog var Nordbornholms Byggeforretning oprindeligt indstillet til at betale 400.000 kr i bøde. Det er således en betragtelig reduktion af bøden. Sat i forhold til virksomhedens omsætning vil bøden næsten kunne kategoriseres, som værende ubetydelig. Det samme skete da Ilva blev indstillet til en bøde af Datatilsynet på 1.500.000 kr, som endte med at blive idømt betaling af 100.000 kr. Henset til Ilvas omsætning på 1,7 mia. i samme regnskabsår[160] er der da heller ikke tale om nogen bøde, som skulle have en præventiv effekt og "*afskrækkende virkning*", som det er ønsket i 151. betragtning til GDPR og art. 83, stk. 1. Det skal dog bemærkes at Datatilsynet ikke kan bestemme, hvad bødeniveauet skal dømmes til i den pågældende ret, men de har dog indflydelse på, hvor stor en bøde den private virksomhed eller den offentlige myndighed skal indstilles til. Ser man eksempelvis på den relativt nye sag om Danske Bank, hvor Danske Bank ikke har kunnet

[155] https://www.version2.dk/artikel/endnu-et-datatilsyn-opfordrer-hjemmesideejere-til-skrotte-analytics
[156] https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply
[157] Hamer og Schaumburg-Müller (2020), 1. udgave, Juraens Verden, side 274; https://www.datatilsynet.dk/Media/637807663119686422/Vejledning%20om%20udmåling%20af%20bøder%20til%20fysiske%20personer%20-%20februar%202022.pdf
[158] https://ing.dk/artikel/gdpr-fumleri-smaboder-gor-loven-ligegyldig-256763
[159] https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/mar/foerste-gdpr-boede-til-offentlig-myndighed
[160] https://ing.dk/artikel/gdpr-fumleri-smaboder-gor-loven-ligegyldig-256763

dokumentere, at de har slettet personoplysninger i overensstemmelse med GDPR, har Datatilsynet indstillet Danske Bank til en bøde på 10 mio. kr[161]. Danske Bank havde i 2021 samlede indtægter for 42,6 mia. kr[162] og en bøde på 10 mio. kr, vil sandsynligvis ikke virke afskrækkende for dem. Dog skal det også bemærkes at den offentlige omtale som sjusk med personoplysninger medfører naturligvis også medfører et økonomisk tab, som ikke kan nærmere defineres på nuværende tidspunkt. Domstolen har ikke taget stilling til bøden endnu, men fortsætter man i samme spor, som hidtil kan Danske Bank nok forvente en – set i kontekst af virksomheden – ubetydelig bøde. Dette kan blandt andet være en af årsagerne til at der ikke har været en stærkere reaktion endnu på, at den lovlige brug af amerikanske cloudtjenester ser ud til at være stærkt begrænset indenfor rammerne af GDPR .

Der er endnu ingen afklaring på Datatilsynets holdning til Google Analytics. Indtil videre har Datatilsynet ikke kommenteret ret meget på disse afgørelser. De har ikke udtalt sig siden midten af januar, hvor man ikke forholdt sig særligt til afgørelserne fra de østrigske- og franske tilsynsmyndigheder. På trods af deres udtrykte forståelse i deres pressemeddelelse, har de ikke oplyst andet end at de nu vil "*…nærlæse afgørelsen fra vores østrigske kollegaer og løbende følge de øvrige afgørelser fra vores europæiske kollegaer i de 101 klagesager fra NOYB"*[163]. De har ikke kommenteret på opbakningen fra tilsynsmyndighederne i Frankrig og Liechtenstein. Dog indrømmer de, i samme pressemeddelelse, at det er "*…afgørende, at de europæiske tilsynsmyndigheder har en fælles fortolkning af reglerne*". Man har derved svært ved at forestille sig, at Datatilsynet skulle nå frem til en anden afgørelse end sine kollegaer ved de østrigske- og franske tilsynsmyndigheder. Dog kommer der også udtalelser, som er modstridende, hvilket især gør, at dataeksportører må antages at være endnu mere tilbageholdende med at træffe en endelig beslutning omkring deres brug af amerikanske cloudtjenester. En af eksemplerne herpå er Datatilsynets håndtering af Helsingør Kommune-sagen.

I denne sag har en fremtrædende figur fra Datatilsynet, jurist og IT-sikkerhed specialist, Allan Frank, i forbindelse med dettes afgørelse fra september 2021, om at danske folkeskoler fortsat kan anvende Google til undervisningsopgaver, blandt andet forklaret, at personoplysningerne kan blive udleveret til amerikanske myndigheder under CLOUD Act, men "…den eventualitet må man tage efterfølgende". Han følger op med at, det reelt set ville være tilstrækkeligt, hvis man som dataeksportør, kan få sin CSP til at skrive under på, at denne overholder GDPR. Da han bliver spurgt om man som dataeksportør har gjort det man skal, såfremt eksempelvis Google har skrevet under på det førnævnte, svarer han

"Ja, hvis man ellers er betrygget i, at Google vil overholde GDPR. For eksempel duer det ikke, hvis man på forhånd ved, at lige de oplysninger, der behandles, altid eller ofte er genstand for anmodninger, der efterfølges. Herudover skal man, så godt man kan, i øvrigt prøve på at kontrollere, at der ikke sker videregivelse"[164].

[161] https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/apr/danske-bank-indstilles-til-boede
[162] https://www.euroinvestor.dk/nyheder/danske-bank-leverer-bedre-end-ventet
[163] https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/jan/afgoerelse-om-brug-af-google-analytics-fra-det-oestrigske-datatilsyn
[164] https://www.version2.dk/artikel/datatilsynet-tech-giganternes-eu-cloud-goer-dig-ikke-gdpr-sikker

Her lægger han således op til to ting. Det første er, at kontraktuelle foranstaltninger kan have afgørende betydning, i form af, at Google kan garantere, at de vil overholde GDPR. Det andet er, at man kan tillægge det afgørende betydning, om den slags personoplysninger der behandles, behandles "altid eller ofte". I forhold til løftet om overholdelse af GDPR, som værende en effektiv foranstaltning, har man netop i EDPB's vejledninger fået bekræftet, at dette ikke er nok. Her anførte EDPB, at sådanne kontraktuelle foranstaltninger kun kunne være tilstrækkeligt effektive i kombination med især tekniske foranstaltninger, som beskrevet tidligere i afsnit 3.2.2.4. Denne udtalelse kan læses som værende modstridende i forhold til det, som Allan Frank udtaler i december 2021 – altså ganske få måneder senere. Her siger han i forbindelse med step 3-vurderingen fra EDPB i Helsingør Kommune-sagen, at "*Man kan ikke bare tro på sin leverandør alene. Man er nødt til at stykke det sammen med nogle andre datakilder*" med henvisning til praktiske erfaringer omkring myndigheders interesse i de pågældende personoplysninger. Han følger op med at sige, at "*Leverandøren har jo en særlig interesse – ikke fordi det er forbudt at bruge leverandøren som én af sine datakilder – man kan bare ikke støtte sin ret på leverandøren alene*" [165]. I den første udtalelse fra september 2020 nævner da trods alt også, at man også skal kontrollere leverandøren og man ellers skal være betrygget i at denne overholder GDPR. Dermed må man udlede, at det skal gøres ved at tage højde for hvilken type personoplysninger der behandles kontra dem som "*altid eller ofte er genstand for anmodninger*". Det er dog slået fast i roadmappet, at man ikke kan lægge vægt på i et land, hvor sådanne praktiske erfaringer kan være underlagt en gag-order, som gør, at Google og andre ikke må oplyse om dem i nogle rapporter mv. Det er en vanskelig opgave at kontrollere leverandøren, når kontrollen potentielt altid vil være mangelfuld, da der kan være myndighedsanmodninger som er genstand for en gag-order. Desuden bør dataeksportøren ved en sådan aftale undersøge om en kontrakt der indebærer, at den ene part kategorisk afviser at overholde national sikkerhedslovgivning, er en kontrakt der kan tilsidesættes, som ugyldig. Det vil denne fremstilling ikke beskæftige sig yderligere med, da det blandt andet rækker ind i amerikansk aftaleret. Indenfor dansk ret ville man i yderste konsekvens forestille sig, at en sådan aftale ville stride imod lov eller ærbarhed og tilsidesættes som ugyldig jf. Danske Lov 5-1-2 eller AFTL § 36.

Uanset ovenstående; skulle man som dataeksportør lykkes med at få CSP'en til at underskrive, at de vil efterleve GDPR og der hvor amerikansk lovgivning modstrider, vil man sætte sig imod, så ville man i udgangspunktet juridisk set have sikret sin overførsel ifølge Datatilsynets udtalelser i Helsingør Kommune-sagen. Spørgsmålet er dog i praksis, om en stor CSP ville kunne blive tvunget til at udlevere personoplysningerne uanset, igennem en retskendelse i USA.
Dette spørgsmål blev bragt op af DSK i deres ekspertudtalelse med Vladeck, som blev anvendt i afsnit 3.2.2.3. Vladeck svarer til spørgsmål 2, at en ECSP udover at blive pålagt betydelige økonomiske sanktioner, også blive "*subject to an adversary judicial proceeding brought in the FISA Court by the Attorney General to enforce the directive*"[166], således at ECSP'en i yderste konsekvens kan blive tvunget til at udlevere ved tvangsfuldbyrdelse ved FISA-domstolen.

[165] https://www.version2.dk/artikel/datatilsynet-om-helsingoers-google-forklaring-man-kan-ikke-bare-tro-paa-sin-leverandoer
[166] Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework

Dette ville dog være en utilsigtet overførsel af personoplysningerne, som dataeksportøren i princippet ikke kan gardere sig imod og som ej heller er omfattet af GDPR's kapitel V[167]. Men her bør det overvejes om en sådan tvangsfuldbyrdelse ikke ville være til at forudse i sin risikovurdering, som man foretager sig i EDPB's roadmap. Anvendelsen af GDPR er trods alt overordnet set baseret på såkaldt "risikobaseret tilgang"[168]. Med dette in mente virker det ikke i nogen henseende forsvarligt som dataeksportør at foretage en overførsel på et sådant grundlag, med tanke på, at leverandøren ultimativt kan udlevere personoplysningerne ved tvangsfuldbyrdelse. Omvendt vil der som nævnt være tale om en utilsigtet overførsel i yderste konsekvens, hvorfor der juridisk set ikke er et brud på GDPR. Man kan dog argumentere for, at der fra den registreredes perspektiv ikke er nogen synderlig forskel på om den ulovlige overførsel af ens personoplysninger sker som led i en myndighedsanmodning eller en tvangsfuldbyrdelse af denne ved en FISA-domstol. Dette er en gråzone og i skrivende stund ikke nogen nævneværdig relevant problemstilling at udforske nærmere, da det er vanskeligt at forestille sig, at nogen CSP skulle skrive ind i deres vilkår, at de modsætter sig national lov.

Førnævnte praksis afspejler et broget billede af nuværende retstilstand. I udgangspunktet er det ikke foreneligt at anvende cloudtjenesterne til andre funktioner en opbevaring, da de i så fald skal være tilgængelige i klartekst for udbyderen af denne. Dog ser man stadig en lang række aktører, som anvender produkter som Microsoft Azure, Google Analytics, Google Workspace og AWS. Datatilsynet er forsigtige med at sige noget definitivt om brugen af de amerikanske cloudtjenester, men har dog givet nogle retningslinjer i deres cloudvejledning, som viser, at brugen af amerikanske cloudtjenester kan anvendes i et meget begrænset omfang med henblik på det beskrevne krypteringsscenarie. Alligevel har Datatilsynet, i form af Allan Frank, i slutningen af marts åbnet døren på klem for, at dataeksportører, alene ved udbyderens kontraktuelle forpligtelse til ikke at følge den problematiske lovgivning, kan sikre sig et tilstrækkeligt beskyttelsesniveau. Dette er alene en udtalelse fra en fremtrædende medarbejder og ikke en officiel vejledning, men den afspejler, at der kommer modstridende informationer ud – også fra Datatilsynet.
Samtidig ser man andre europæiske tilsynsmyndigheder gå forrest med en klar holdning om, at der ikke er nogle "smutveje" udenom den problematiske lovgivning så snart personoplysninger er tilgængelige, for CSP'erne, i klartekst.

Det er således ikke et entydigt billede der tegner sig omkring retstilstanden. En mulig forklaring kan være, at man hos Datatilsynet er klar over, hvilke økonomiske- og konkurrencemæssige, udfordringer det ville medføre, hvis man gik ud og indstillede en større virksomhed til en bøde på baggrund af brug af amerikanske cloudtjenester. Hvis man i praksis ikke længere kan holde sig indenfor lovgivningen ved brug af vitale værktøjer så som Google Analytics, Microsoft Teams mv., så skal man for det første udskifte dette, hvilke er en ressourcetung affære. Dernæst skal man finde alternative værktøjer, som ikke nødvendigvis kan erstatte værktøjerne til fulde. Der er altså ikke blot data om persondataret, men et større politisk spil, hvor Datatilsynet er fanget imellem EUD's klare dom på den ene side og en tung amerikansk cloud-lobby samt erhvervsmæssige-,

[167] Vejledning: Overførsel af personoplysninger til tredjelande, Juli 2021, 3. udgave, Datatilsynet, afsnit 3.6
[168] Hamer og Schaumburg-Müller (2020), 1. udgave, Juraens Verden, side 269; https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/risikovurdering/risikovurdering-emne

samfundsøkonomiske- og politiske interesser på den anden side. Der er ingen klare beviser på, at Datatilsynet er tilbageholdende med at sige noget definitivt i sager omkring anvendelsen af amerikanske cloudtjenester, som de østrigske- og franske tilsynsmyndigheder har gjort det, men det er ikke utænkeligt, at man hos Datatilsynet tænker sig om en ekstra gang før man kommer ud med en skelsættende afgørelse, som dem vi har set i Østrig og Frankrig. Dette bør dog ikke være en hindring jf. GDPR, art. 52, stk. 2, der fastslår at de nationale tilsynsmyndigheder ikke må påvirkes af udefrakommende interesser. Om Datatilsynet bliver påvirket på en sådan måde, er umuligt at gisne om, men der er ingen tvivl om, at der er mange udefrakommende faktorer, som kan påvirke Datatilsynet. Henset til diskussionen tidligere i nærværende fremstilling, er der ikke megen tvivl om at kommuner, uddannelsesinstitutioner, erhvervsorganisationer og private firmaer bestemt ikke ønsker, at brugen af amerikanske cloudtjenester skal blive yderligere besværliggjort, hvis ikke umuliggjort i forhold til GDPR.

4. Konklusion

Undersøgelsen nåede frem til, at overførslerne fortsat kan ske. Dog er den også nået frem til, at der ikke er ret stort albuerum, for hvordan sådanne løsninger i praksis kan sættes sammen, pga. den meget bredt anvendelige problematiske lovgivning. Lovgivningen gør nemlig, at så længe personoplysningerne er tilgængelige i klartekst for CSP'en, så vil personoplysningerne kunne blive udleveret på anmodning fra en. CSP'en kan nemlig ikke udlevere noget, som den ikke selv har adgang til. Var disse oplysninger krypteret på en måde, hvor kun en betroet tredjepart opbevarede og krypterede personoplysningerne, ville dette være en effektiv supplerende foranstaltning, som sikrer et tilstrækkeligt beskyttelsesniveau. Denne løsning er vel nok det nærmeste man kommer på den "rigtige" løsning. Problemet med denne løsning er imidlertid, at CSP'en ikke rent teknisk kan behandle data, de ikke kender og brugen af cloudtjenesterne er derfor ved denne løsning reduceret til opbevaring udelukkende. En sådan brug er ikke den primære årsag til at mange aktører vælger at anvende disse. Derfor er denne løsning juridisk korrekt, men vanskeligt anvendelig i praksis.

Udover den førstnævnte løsning har undersøgelsen udforsket nogle ganske få andre muligheder. EDPB's roadmap åbner muligheden for også at inddrage en vurdering af om personoplysninger er i risiko for udlevering i praksis, selvom de juridisk set er omfattet af den problematiske lovgivning. Kan man som dataeksportør tilstrækkeligt og grundigt godtgøre for denne ikke har grund til at tro, at personoplysningerne på ingen måde har interesse for de amerikanske myndigheder, kan man lovligt fortsætte overførslen. Hertil ser man at Google, Microsoft og AWS alle udgav rapporter, som dataeksportører kunne anvende i sin vurdering af, hvor vidt disses personoplysninger i praksis ville blive genstand for en myndighedsanmodning. Dog oplyser EDPB i deres 47. anbefaling, at sådanne praktiske erfaringer fra dataimportøren i tredjelandet ikke må indgå i vurderingen, såfremt tredjelandet har love som kan forbyde denne at oplyse om anmodninger. Med andre ord, ville sådanne erfaringers sandhed aldrig kunne kontrolleres. Det kan dog netop på baggrund af dette være en næsten umulig opgave for europæiske aktører, at påvise, at amerikanske myndigheder i praksis aldrig ville have interesse i de personoplysninger man overfører.

Undersøgelsen har også behandlet praksis fra tilsynsmyndigheder og udtalelser med henblik på, at afklare hvordan disse forholder sig i praksis til den nuværende situation. Det er svært at

konkludere noget konkret ud fra Datatilsynets praksis og udtalelser, men undersøgelsen konkluderer dog, at Datatilsynet ikke har taget endelig stilling til Schrems II-problemstillingen i Danmark i forbindelse med anvendelse af amerikanske cloudtjenester, herunder med henvisning til deres udtalelser omkring den østrigske tilsynsmyndigheds afgørelse omkring Google Analytics. Undersøgelsen behandlede blandt andet mulige årsager til, at man nu – næsten 2 år efter Schrems II-dommen – fortsat står i en lidt uafklaret situation. Blandt mulige årsager blev det især behandlet, hvordan tilsynsmyndighederne rundt omkring i EU's medlemslande ikke fuldstændigt klart anvender GDPR ensartet. Desuden kom undersøgelsen også frem til, at en mulig årsag kan være, at en anvendelse og fortolkning af GDPR og Schrems II-dommen imod amerikanske cloudtjenester vil have relativt store konsekvenser både økonomisk- og konkurrencemæssigt for private- og offentlige aktører indenfor EU.
Endeligt kom undersøgelsen frem til, at en mulig årsag til, at der antageligvis er mange private- og offentlige aktører i Danmark der fortsat anvender amerikanske cloudtjenester i uoverensstemmelse med GDPR og Schrems II-dommen, kan være, at Datatilsynets praksis og domstolenes bødeniveau i relation til dennes praksis ikke har den afskrækkende virkning og således præventive effekt, som har været ønsket med GDPR.

Mange dataeksportører i EU står således fortsat i en uholdbar situation, hvor man enten skal "opfinde den dybe tallerken" eller man skal droppe amerikanske cloudtjenester. Mange håber på, at en politisk løsning – altså en slags Privacy Shield 2.0 – på vil løse problemet. Det er svært at spå om, da der indtil videre kun er kommet en principiel aftale i hus, som ikke nævner noget konkret om det kommende overførselsgrundlag. For at en sådan en aftale skal få nogen effekt og udgøre et nyt overførselsgrundlag på linje med Privacy Shield skal USA formentlig tilbyde betydelige indrømmelser omkring deres overvågningslovgivning. Det er dog svært at forestille sig, at USA opgiver eller indskrænker lovgivningen, til en sådan grad, at der ud fra en risikovurdering efter GDPR ikke ville kunne identificeres en risiko for den registreredes rettigheder.

Litteraturliste

Bøger

- Juraens Verden af Carina Risvig Hamer og Sten Schaumburg-Müller (2020), 1. udgave

Beslutninger og afgørelser fra EU-Kommissionen

- 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

- Kommissionens afgørelse af 5. februar 2010 om standardkontraktbestemmelser for videregivelse af personoplysninger til registerførere etableret i tredjelande i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF

- Kommissionens gennemførelsesafgørelse (EU) 2021/914 af 4. juni 2021 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679

Domme

- Sag C-311/18 - Schrems II-dommen

Henstillinger, vejledninger mv.

- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
- Recommendations 02/2020 on the European Essential Guarantees for surveillance measures
- Vejledning om cloud, Marts 2022, Datatilsynet
- Vejledning: Overførsel af personoplysninger til tredjelande, Juli 2021, 3. udgave, Datatilsynet

Hjemmesider og artikler

- https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/
- https://legaljobs.io/blog/gdpr-statistics/
- https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_da
- https://www.datatilsynet.dk/hvad-siger-reglerne/grundlaeggende-begreber-/hvad-er-personoplysninger
- https://www.complycloud.com/wp-content/uploads/2021/09/FISA-whitepaper-download.pdf
- https://www.eff.org/pages/upstream-prism; https://www.fieldfisher.com/en/insights/us-surveillance-s702-fisa-eo-12333-prism-and-ups
- https://www.linklaters.com/en/insights/blogs/digilinks/2019/september/us-cloud-act-and-gdpr-is-the-cloud-still-safe

- https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Databeskyttelse-standardkontraktbestemmelser-om-videregivelse-af-personoplysninger-til-lande-uden-for-EU-gennemf%C3%B8relsesretsakt-_da
- https://kammeradvokaten.dk/nyheder-viden/nyheder/2021/06/nye-standardkontraktbestemmelser-for-internationale-overfoersler-vedtaget
- https://www.datatilsynet.dk/internationalt/internationalt-nyt/2021/jun/edpb-har-vedtaget-endelige-anbefalinger-om-supplerende-foranstaltninger
- https://ec.europa.eu/commission/presscorner/detail/es/ip_22_2087
- https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/
- Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework (https://edpb.europa.eu/system/files/2022-04/edpb_statement_202201_new_trans-atlantic_data_privacy_framework_en.pdf)
- https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap36-subchapVI-sec1881.htm
- https://www.law.cornell.edu
- Expert Opinion on the Current State of U.S. Surveillance Law and Authorities from Prof. Stephen I. Vladeck, University of Texas School of Law (https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf)
- https://d1.awsstatic.com/Information_Request_Report_December_2021_bia.pdf
- https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report?activetab=pivot_1:primaryr2
- https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF
- https://www.comparitech.com/blog/vpn-privacy/warrant-canary/
- https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/
- https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA
- https://kromannreumert.com/nyheder/bliv-klogere-paa-nye-anbefalinger-om-krav-til-dataoverfoersel-til-tredjelande
- https://www.pwc.dk/da/artikler/2021/06/nyt-om-schrems-ii.html
- https://www.version2.dk/artikel/datatilsynet-saadan-kan-du-bruge-amerikansk-cloud-lovligt
- https://www.version2.dk/artikel/datatilsynet-tech-giganternes-eu-cloud-goer-dig-ikke-gdpr-sikker
- https://azure.microsoft.com/en-us/overview/what-is-azure/
- https://www.version2.dk/artikel/helsingoer-skoler-beholder-google-vi-maa-leve-med-risici-boernenes-databeskyttelse
- https://www.version2.dk/artikel/helsingoer-kommune-folkeskolen-kan-ikke-koere-uden-google
- https://www.version2.dk/artikel/analytics-forbud-truer-det-vil-have-store-konsekvenser-danske-virksomheder
- https://www.version2.dk/artikel/kl-om-afsked-med-amerikansk-cloud-det-har-store-oekonomiske-og-administrative-konsekvenser

- https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises
- https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/
- https://itwatch.dk/ITNyt/Brancher/cloud/article12668868.ece
- https://www.computerworld.dk/art/260557/kombit-i-dialog-med-netcompany-og-kommunerne-om-aula-efter-schrems-ii-afgoerelse-kan-vaere-i-strid-med-gdpr
- https://www.k-news.dk/nyheder/eksperter-schrems-ii-afgoerelsen-efterlader-virksomheder-i-juridisk-limbo
- https://www.computerworld.dk/art/259787/eu-er-paa-trapperne-med-loesning-for-schrems-ii
- https://www.version2.dk/artikel/svenske-myndigheder-vil-skrotte-amerikansk-cloud-her-er-alternativerne
- https://www.version2.dk/artikel/skelsaettende-afgoerelse-derfor-dumper-google-analytics-paa-gdpr
- https://www.version2.dk/artikel/frankrig-strammer-nettet-om-google-kunder-ulovligt-bruge-analytics-i-eu
- https://www.version2.dk/artikel/endnu-et-datatilsyn-opfordrer-hjemmesideejere-til-skrotte-analytics
- https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply
- https://www.datatilsynet.dk/Media/637807663119686422/Vejledning%20om%20udmåling%20af%20bøder%20til%20fysiske%20personer%20-%20februar%202022.pdf
- https://ing.dk/artikel/gdpr-fumleri-smaboder-gor-loven-ligegyldig-256763
- https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/jan/afgoerelse-om-brug-af-google-analytics-fra-det-oestrigske-datatilsyn
- https://www.version2.dk/artikel/datatilsynet-om-helsingoers-google-forklaring-man-kan-ikke-bare-tro-paa-sin-leverandoer
- https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/risikovurdering/risikovurdering-emne
- https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/mar/foerste-gdpr-boede-til-offentlig-myndighed
- https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/apr/danske-bank-indstilles-til-boede
- https://www.euroinvestor.dk/nyheder/danske-bank-leverer-bedre-end-ventet
- https://denstoredanske.lex.dk/retsdogmatik