AALBORG UNIVERSITET
STUDENTERRAPPORT

Kandidatspeciale

De juridiske udfordringer ved tredjelandsoverførsel til USA

Gruppe: Joakim Andersen, Lærke Eliasen, Mads Jensen

Vejleder: Tanja Kammersgaard Christensen

Fagområde: Databeskyttelsesret

Erhvervsjura, Cand.merc.(jur.), 10. semester: Kandidatspeciale

Billede fra
www.datatilsynet.dk

Afleveringsdato: 15. maj 2025

Antal anslag: 190.106

Abstract

The subject of the Master's thesis is "The legal challenges of third-country data transfers to the U.S.". The research question and purpose of the thesis is as follows: "This thesis analyzes whether the limitations and safeguard established in Executive Order 14086 (EO 14086) ensure an adequate level of data protection and thus permit lawful data transfers between the U.S. and the EU. Furthermore, it analyzes how the use of supplementary measures can ensure that Standard Contractual Clauses (SCCs) can be used as a valid data transfer instrument despite the intrusive nature of U.S. surveillance laws and practices. The thesis also examines the complications associated with the CLOUD Act and considers how a data controller should act when engaging processors subject to the CLOUD Act.". The research question will be answered by using the legal dogmatic method and an international comparative approach. The thesis will among other things include a description of Chapter V of the GDPR, Schrems I and II, relevant U.S. laws and an examination of EO 14086. Lastly, the thesis will include an analysis of the research question's contents and provide a conclusion regarding this.

It is concluded that EO 14086 may be criticized for failing to prohibit bulk collection of personal data and due to its underlying legal framework. Furthermore, it may be criticized that the oversight mechanism established through PCLOB and CLPO can be circumvented under certain conditions. The U.S. interpretation of the principle of proportionality is acknowledged, whereas its interpretation of the necessity principle is found to be problematic due to inconsistency with the interpretation under EU law.

It is further concluded that PCLOB may be criticized for its lack of quorum, which also affects the functioning of CLPO and DPRC. Moreover, PCLOB can be criticized for a lack of transparency and independence. While the legally binding nature of decisions by CLPO and DPRC is recognized, the bodies may nonetheless be criticized for insufficient independence, as emphasized in Schrems II, paragraphs 195 and 196. It is also concluded that DPRC's lack of obligation to report and its positioning within the executive branch is accepted. However, DPRC is criticized for failing to provide reasoned decisions to complainants, as well as for the absence of appeal possibilities, transparency, and the extensive use of standardised responses

Regarding the use of SCCs, it is concluded, based on EDPB guidelines, that it is recommended to prepare a comprehensive mapping of all relevans transfers. It is further recommended that the laws and practices of the third country be assessed. Based on such assessment, supplementary measures

must be implemented where necessary. A sufficient level of data protection under SCCs must be ensured through supplementary measures, which may be of a technical, organisational, or contractual nature.

Additionally, it is concluded that SCCs may only serve as a valid data transfer instrument if a sufficient level of data protection is ensured through appropriate safeguards, cf. GDPR Article 46(2)(c). Based on case law, it is further concluded that supplementary measures such as encryption where the decryption key is held by the data importer do not necessarily ensure sufficient data protection.

In relation to the CLOUD Act, it is concluded that the U.S.-owned companies located in the EU may face a jurisdictional conflict between U.S. and EU law. Complying with a CLOUD Act request on the basis of GDPR Article 49(1) (d)-(f) and the last paragraph is found to be inadequate or practically unfeasible. Instead, international agreements should serve as a legal basis for such transfers. Furthermore, it is concluded that the CLOUD Act is incompatible with EU law due to its circumvention of MLAT provisions, and therefore, companies subject to the CLOUD Act should not comply with such requests uncritically

Finally, based on the KOMBIT case, it is concluded that compliance with CLOUD Act requests within the framework of a data processing agreement leads to the processor being subject to the GDPR. It is also concluded that data controllers must in advance assess whether their processors provide adequate data protection. In addition, the controller must ensure sufficient processing security and conduct regular audits of its processor. Moreover, the controller must refuse to comply with CLOUD Act requests if doing so would breach the data processing agreement. It is further concluded, based on the GDPR and legal literature, that any uncertainty of interpretation must be clarified by the controller in advance. The wording of the data processing agreement must also be precise and clear, cf. GDPR Article 28(1).

Indholdsfortegnelse

Forkortelser

AWS	Amazon Web Services
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
CLPO	Civil Liberties Protection Officer
Dataeksportør	Betegnelse for en dataansvarlig eller databehandler, der overfører personoplysninger til en dataimportør[1]
Dataimportør	Betegnelse for fysiske eller juridiske personer i tredjelande, som dataeksportører overfører personoplysninger til[2]
DBL	Den danske databeskyttelseslov (Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger)
DPF	EU-U.S. Data Privacy Framework
DPRC	Data Protection Review Court
DT	Datatilsynsmyndigheden i Danmark
EDPB	Det Europæiske Databeskyttelsesråd
EDPS	Den Europæiske Tilsynsførende for Databeskyttelse
EMD	Den Europæiske Menneskerettighedsdomstol
EMRK	Den Europæiske Menneskerettighedskonvention
EO	Dekret (Executive Order)
EU	Den Europæiske Union
EUC	Den Europæiske Unions Charter om Grundlæggende Rettigheder
EUD	Den Europæiske Unions Domstol

[1] Udsen, *Databeskyttelsesret*, s. 18
[2] Ibid., s. 18

EUK	Europa-Kommissionen
EØS	Det Europæiske Økonomiske Samarbejdsområde
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
GDPR	General Data Protection Regulation (Forordning 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger)
LIBE	Europa-Parlamentets Udvalg om Borgernes Rettigheder og Retlige samt Indre Anliggender
MLAT	Mutual Legal Assistance Treaty
NOYB	None of Your Business (Max Schrems' NGO, som beskæftiger sig med privatlivsrettigheder og databeskyttelse)
PCLOB	Privacy and Civil Liberties Oversight Board
PPD	Presidential Policy Directive
SCC	Standardkontraktbestemmelser (Standard Contractual Clauses)
TEU	Traktat om Den Europæiske Union
TEUF	Traktat om Den Europæiske Unions Funktionsmåde

1 Indledning

Den stigende digitalisering og internationalisering medfører, at overførsel af personoplysninger stadig får en større betydning for virksomheder, offentlige myndigheder og de registrerede. Rettigheder skal beskyttes på tværs af landegrænser, men denne opgave bliver stadig mere kompleks i takt med, at personoplysningers betydning og økonomiske værdi vokser, og deres anvendelse bliver mere omfattende. Dette skaber betydelige juridiske udfordringer, især når personoplysninger overføres fra EU til tredjelande, som ikke nødvendigvis tilbyder en beskyttelse tilsvarende den, som garanteres i EU. USA har i denne forbindelse længe været et omdiskuteret tredjeland, eftersom de forhenværende tilstrækkelighedsafgørelser er blevet ugyldiggjort. I indeværende speciale vil der tages stilling til den nuværende tilstrækkelighedsafgørelse af USA, som har til formål at legitimere en overførsel af personoplysninger ved at sikre, at USA har et tilstrækkeligt beskyttelsesniveau i henhold til GDPR artikel 45. Der vil tages stilling til, om EU-borgere har tilstrækkelig adgang til effektive retsmidler, som de sikres i medfør af EUC. Den nuværende tilstrækkelighedsafgørelse er resultatet af en længerevarende og kompleks proces præget af udfordringer omhandlende manglende effektive retsmidler og USA's omfattende overvågningslove.

I specialet vil gældende ret beskrives, hvilket omfatter relevante artikler fra EUC og indholdet af EO 14086, som er fundamentet for DPF. Det vil blive undersøgt, om den gældende tilstrækkelighedsafgørelse reelt opfylder de kriterier, som EUD har opstillet i forbindelse med ugyldiggørelsen af de tidligere tilstrækkelighedsafgørelser. Dertil om den amerikanske lovgivning og retsstatsprincipper er forenelige med EU-retten, herunder om EU-borgere sikres samme rettigheder og friheder, som de garanteres i EU. Det vil analyseres, om der findes en overensstemmelse mellem de begrænsninger og garantier, som fastsættes i EO 14086, og de rettigheder, som sikres gennem EUC. I kølvandet på en tvivlsom fremtid, hvor den nuværende tilstrækkelighedsafgørelse potentielt kan ugyldiggøres, vil der i specialet yderligere belyses et alternativt overførselsgrundlag, hvorpå en lovlig overførsel kan finde sted, herunder SCC'er. Dertil hvornår og hvordan indførelsen af supplerende foranstaltninger udgør en tilstrækkelig beskyttelse af personoplysninger. I specialet vil det endvidere blive undersøgt, hvilke komplikationer der er forbundet med CLOUD Act, samt hvordan en dataansvarlig bør agere, når vedkommendes databehandlere er omfattet af denne lovgivning.

Gældende ret udledes gennem juridisk metode, herunder retsdogmatisk metode. Denne metodeform anvendes til at analysere, hvordan tredjelandsoverførsel til USA reguleres i lovmæssig forstand. I den

forbindelse anvendes en række EU-retlige kilder, herunder Schrems I- og II-afgørelserne fra EUD, eftersom disse er betydningsfulde for den nuværende tilstrækkelighedsafgørelse og DPF. Ydermere vil en international komparativ rets tilgang anvendes, og for at besvare specialets problemformulering vil gældende ret udfordres for at udlede, om DPF indeholder usikkerheder, som kan underminere EU-borgeres grundlæggende rettigheder.

2 Problemformulering

I dette speciale analyseres, hvorvidt begrænsningerne og garantierne fastsat i EO 14086 sikrer en tilstrækkelig databeskyttelse og dermed en lovlig dataoverførsel mellem USA og EU. Dertil analyseres, hvornår og hvordan anvendelse af supplerende foranstaltninger kan sikre, at SCC'er kan bruges som overførselsgrundlag på trods af de indgribende amerikanske overvågningslove og praksis. I specialet vil komplikationerne forbundet med CLOUD Act endvidere undersøges, og hvordan en dataansvarlig med databehandlere omfattet af CLOUD Act bør agere i denne sammenhæng.

3 Afgrænsning

Dette speciale afgrænses til at omhandle EUC artikel 7, 8, 47 og 52 samt GDPR kapitel V og artikel 28, litra a, c, d og h. Specialet afgrænses yderligere i forbindelse med kapitel V til kun at omfatte artikel 44, 45, 46, 48, 49, stk. 1, litra d-f, og artikel 49 stk. 1, andet afsnit. Disse afgrænsninger er begrundet i, at de nævnte artikler har særlig relevans for besvarelse af specialets problemformulering. Derudover medtages yderligere relevante artikler fra GDPR. DBL inddrages minimalt, eftersom denne lovgivning ikke har relevans for besvarelse af problemformuleringen. Specialet vil også afgrænses i forbindelse med retspraksis, hvor der vil inddrages relevante afgørelser fra EUD, datatilsynsmyndigheder, EMD og nationale domstole. I denne sammenhæng vil der udelukkende inddrages relevante betragtninger og præmisser fra de udvalgte afgørelser for at kunne besvare problemformuleringen.

Specialet afgrænses til at fokusere på tredjelandsoverførsel fra EU til USA. Dette skyldes historikken, væsentligheden og de aktuelle udfordringer, som dataoverførsel til dette tredjeland indebærer. Relevant amerikansk lovgivning vil i denne sammenhæng inddrages, beskrives og diskuteres, hvilket består af FISA 702, EO 12333, EO 14086 og CLOUD Act. PPD-28 vil ikke undersøges nærmere, eftersom EO 14086 i praksis har erstattet PPD-28, og endvidere er PPD-28 delvist ophævet.[3] FISA 702 og EO 12333 vil ikke blive analyseret dybdegående, eftersom de allerede er diskuteret og vurderet gennem Schrems I- og II-afgørelserne. I specialet vil der imidlertid fokuseres på EO 14086, eftersom dette dekret er fundamentet for den nuværende tilstrækkelighedsafgørelse samt DPF, og fordi EUD endnu ikke har taget stilling til dekretet gennem en afgørelse. Den udvalgte lovgivning inddrages, eftersom det har væsentlig relevans for besvarelse af problemformuleringen, herunder ved analyse af Schrems-afgørelserne. Amerikansk retspraksis og retsprincipper inddrages ligeledes i specialet, såfremt det findes relevant. Det skal i denne kontekst bemærkes, at specialets forfattere ikke besidder væsentlig og dybdegående kendskab til amerikansk lovgivning, hvorfor fortolkningen og forståelsen er begrænset.

Specialet afgrænses derudover til at fokusere på SCC'er som det eneste overførselsgrundlag i GDPR artikel 46. Denne afgrænsning skyldes, at SCC'er udgør det mest udbredte og praktisk relevante alternative overførselsgrundlag i forhold til en tilstrækkelighedsafgørelse.[4] Derudover afgrænses

[3] Gerhard og Woolley, *National Security Memorandum on Partial Revocation of Presidential Policy Directive 28*
[4] www.commission.europa.eu/new-standard-contractual-clauses-questions-and-answers-overview, afsnit 3

specialet til at fokusere på CLOUD Act i forbindelse med GDPR artikel 48 og 49 samt KOMBIT-sagen.

4 Metode og retskilder

4.1 Metode

Følgende speciales metodiske grundlag består af juridisk metode med anvendelse af en retsdogmatisk tilgang. Retsdogmatisk metode anvendes til henholdsvis at beskrive, systematisere og fortolke materiale af retlig karakter.[5] Ydermere anvendes retsdogmatisk metode til at analysere og beskrive de retsregler, som har relevans for specialet, og således udlede gældende ret.[6] Dette sker på baggrund af anerkendte retskilder, såsom traktater, forordninger, direktiver, national lovgivning, retspraksis fra nationale og internationale domstole samt administrative afgørelser. Disse retskilder indeholder informationer, som er af normativ karakter og bidrager til at skabe eller bekræfte juridiske informationer.[7] Retsdogmatisk metode anvendes således til at analysere, hvordan overførsel af personoplysninger fra EU/EØS til tredjelande, herunder USA, reguleres i lovmæssig forstand. Udover ovenstående retskilder anvendes retslitteratur i form af juridiske artikler og fagbøger omhandlende tredjelandsoverførsler. Sådanne anses imidlertid ikke som værende egentlige retskilder, hvorfor artiklerne og fagbøgerne udelukkende kan tjene til inspiration ved at indeholde en retlig argumentation eller ved at indeholde anerkendte videnskabelige resultater.[8]

Specialets problemformulering undersøges på baggrund af relevante EU-retlige kilder, herunder GDPR, EUC og de centrale afgørelser fra EUD, henholdsvis Schrems I (C-362/14) og Schrems II (C-311/18). Disse danner grundlag for specialets analyse af de krav, som stilles til EU-borgeres beskyttelse af de pågældendes grundlæggende rettigheder og friheder. I forlængelse heraf inddrages amerikansk lovgivning med henblik på at vurdere, om EO 14086 sikrer EU-borgeres grundlæggende rettigheder og friheder, herunder adgang til effektive retsmidler. Derudover inddrages EDPB og DT's anbefalinger samt vejledninger, herunder EDPB's vejledning om supplerende foranstaltninger og anvendelse af SCC'er. Således muliggøres en vurdering af, hvornår og hvordan sådanne foranstaltninger kan opveje de retlige mangler i tredjelande, herunder USA, og dermed sikre en tilstrækkelig databeskyttelse for EU-borgere.

[5] Munk, *Den juridiske løsning*, s. 13-14
[6] Ibid., s. 13-14
[7] Blume, *Retssystemet og juridisk metode*, s. 179
[8] Munk, *Den juridiske løsning*, s. 74

Juridisk metode anvendes til at finde de gældende retsregler, *de lege lata*, og forsøger at fastlægge henholdsvis regel, faktum og resultat.[9] I specialet anvendes *retlig sumption*, eftersom faktiske forhold angående de amerikanske overvågningslove og EU-borgeres retsmidler henføres under relevante retsregler, herunder navnlig EUC artikel 7, 8, 47 og 52 og en række bestemmelser i GDPR.[10] Således muliggøres en vurdering af, om disse forhold lever op til de krav, som EU-lovgivning stiller for lovlig overførsel af personoplysninger til tredjelande.

I specialet vil der anvendes retsdogmatisk metode, herunder retlig argumentation ved løsning af de angivne problemstillinger, som problemformuleringen indebærer. Ydermere vil en international komparativ rets tilgang anvendes i den forstand, at nødvendigheds- og proportionalitetsprincipperne samt national sikkerhed som begreber sammenlignes, herunder med fokus på forskelle og ligheder i begrebernes fortolkning i henholdsvis EU og USA.[11] Denne sammenligning foretages for at vurdere, om USA lever op til de standarder, som følger af europæisk databeskyttelse, herunder EUC artikel 7, 8, 47 og 52.

Specialets problemformulering besvares fortrinsvis med grundlag i EU-retlige perspektiver, eftersom amerikansk lovgivning er kompleks, og således vanskeliggør en fuldstændig retlig forståelse af amerikansk lovgivning. I specialet vil retsdogmatisk metode anvendes med henblik på at redegøre for gældende ret. For at kunne besvare specialets problemformulering vil gældende ret udfordres, eftersom den nuværende tilstrækkelighedsafgørelse potentielt kan indeholde retlige usikkerheder, som kan underminere og krænke de grundlæggende rettigheder, som EU-borgere sikres i medfør af EUC.

I specialet vil udvalgte domme fra EMD inddrages som fortolkningsbidrag, eftersom EU-lovgivning skal fortolkes i overensstemmelse med EMRK, herunder praksis fra EMD.[12] Dette valg uddybes nærmere nedenfor, jf. kapitel 4.2.

[9] Munk, *Den juridiske løsning*, s. 11
[10] Ibid., s. 11
[11] Ibid., s. 78
[12] www.eur-lex.europa.eu/forklaringer-til-euc, forklaring ad artikel 52

4.2 Retskilder

Retskilder er de elementer, som danner grundlag for at fastslå, hvad der udgør gældende ret. Retskilder kan opdeles i henholdsvis primære og sekundære retskilder, og følgende kapitel vil beskrive de anvendte retskilder.[13] EU er i sig selv en retskilde, men opdeles i henholdsvis den primære og sekundære lovgivning. Den primære lovgivning, navnlig EU's traktater og Charter, ligger til grund for alle EU-tiltag, mens den sekundære lovgivning, navnlig EU's forordninger, direktiver og afgørelser, beror på traktaternes principper og mål.[14] EU's primære lovgivning består af EUC og traktaterne, TEU og TEUF. Denne sondring er vigtig, eftersom den afspejler retskilders juridiske forrang og deres betydning ved fastlæggelse af en retsstilling.

Traktat om Den Europæiske Unions Funktionsmåde

EU hviler på traktatretlige grundlag, herunder på multilaterale traktater mellem stater. De enkelte medlemsstater overdrager imidlertid lovgivningskompetence, som kendetegnes derogation, og delvis suverænitetsafgivelse.[15] I Danmark følger denne suverænitetsafgivelse af grundlovens § 20, som muliggør, at der ved lov overlades beføjelser, der ellers ville tilkomme henholdsvis den lovgivende, udøvende og dømmende magt i Danmark.[16] I medfør af § 20 har EU beføjelse til at gøre mere end bare at vedtage love. Den lovgivende, udøvende og dømmende magt kan således overlades til EU, som ses ved eksempelvis EU-lovgivning og EUD.[17] EU som retsdannelse er således supranational og skabes i EU-institutioner, der fastsætter regler for medlemsstaterne, men også indirekte og direkte for borgerne.[18] Som følge heraf skal EU medtages som en del af gældende dansk lovgivning.

EU's retsakter nævnes i TEUF artikel 288 og angår forordninger, direktiver, afgørelser, henstillinger og udtalelser. Sådanne kan kun vedtages, når en traktatbestemmelse giver EU-institutionerne hjemmel hertil. Principper om forrang, loyalitet og solidaritet skal ligeledes sikre, at EU's retsakter ikke strider imod EU's mål og værdier.[19] Den såkaldte loyalitetsforpligtelse eller solidaritetsprincip indebærer, at medlemsstaterne skal træffe alle egnede foranstaltninger for at sikre opfyldelse af de forpligtelser, som EU's fællesskab indebærer. Denne loyalitetsforpligtelse gælder for såvel

[13] Hamer og Daniel, *Juridisk metode når EU-retten er i spil*, s. 139-146
[14] Ibid., s. 139-146
[15] Munk, *Den juridiske løsning*, s. 39
[16] www.ft.dk/da/dokumenter/mingrundlov/kapitel3/paragraf20
[17] www.eu.dk/danmark-i-eu/eu-i-danmark/suverænitet
[18] Munk, *Den juridiske løsning*, s. 39
[19] Reimann, *EU-traktaternes hovedprincipper*

medlemsstater som EU-institutioner. Sådanne foranstaltninger kan bestå i at retsforfølge og sanktionere overtrædelser af EU-forbud.[20]

Endelig forpligtes Unionens fællesskab, jf. TEU, til at respektere de grundlæggende menneskerettigheder, medlemsstaternes nationale identitet og deres demokratiske styreformer.[21]

Den Europæiske Unions Charter om Grundlæggende Rettigheder

EUC indeholder rettigheder, hvad angår frihed, lighed, solidaritet, unionsborgerskab og retfærdighed.[22] Disse grundrettigheder og friheder tilhører alle i EU og fastlægger nogle minimumsstandarder, som skal sikre, at enhver behandles med værdighed.[23] EUC har samme retskildeværdi som traktaterne, jf. TEU artikel 6, og blev juridisk bindende for medlemsstaterne i forbindelse med Lissabon-traktatens vedtagelse i 2009.[24] [25] EUC spiller en central rolle, hvad angår databeskyttelse, eftersom artikel 8 omhandler beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.[26] Denne beskyttelse omtales ligeledes i GDPR artikel 1, stk. 2: "*Denne forordning beskytter fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger.*".[27] Endvidere tydeliggør præambelbetragtning 4, at GDPR overholder alle de grundlæggende rettigheder og følger de frihedsrettigheder og principper, der anerkendes i EUC.[28] EUC danner således retsgrundlag for EU-borgeres beskyttelse af privatliv og personoplysninger, mens GDPR er den primære lovgivning.

Beskyttelse af personoplysninger er en grundlæggende rettighed i EU, som eksempelvis anerkendes i EUC. EU har således retsgrundlag til at vedtage lovgivning for at beskytte denne grundlæggende rettighed. GDPR er en sådan lovgivning, eftersom den netop sikrer beskyttelse af fysiske personer i forbindelse med behandling og udveksling af personoplysninger.[29] Nedenfor vil relevante artikler i EUC gennemgås og forbindes med GDPR.

---

[20] Reimann, *EU-traktaternes hovedprincipper*
[21] Ibid.
[22] Næsborg og Khalaf, *Europæiske menneskerettigheder*, s. 251-254
[23] www.eur-lex.europa.eu/den-europæiske-unions-charter-om-grundlæggende-rettigheder (herefter EUC)
[24] www.eur-lex.europa.eu/traktat-om-den-europæiske-union (herefter TEU) artikel 6
[25] Hamer og Daniel, *Juridisk metode når EU-retten er i spil*, s. 141
[26] EUC artikel 8
[27] www.eur-lex.europa.eu/forordning-(eu)-2016/679 (herefter *GDPR*) artikel 1
[28] GDPR præambelbetragtning 4
[29] Ibid.

Artikel 7

Artikel 7 indeholder en fundamental frihedsrettighed for EU-borgere og har følgende ordlyd:

Respekt for privatliv og familieliv [30]

Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation

Der søges således at beskytte mod uberettigede indgreb i EU-borgeres personlige liv. Offentlige myndigheder må kun begrænse den i artikel 7 nævnte rettighed, såfremt dette sker i overensstemmelse med en lovgivning og anses som nødvendigt. Sådanne indgreb kan retfærdiggøres af hensyn til den nationale sikkerhed, den offentlige tryghed, den økonomiske velfærd, forebyggelse af uro eller forbrydelser, beskyttelse af den overordnede sundhed eller sædelighed eller for at beskytte andres rettigheder og friheder.[31] De rettigheder, som sikres, har en direkte sammenhæng med EMRK artikel 8, som ligeledes sikrer EU-borgeres rettighed til privatliv.[32] GDPR bygger videre på disse rettigheder og friheder og er den primære lovgivning, som sikrer beskyttelse af EU-borgeres personoplysninger.

Artikel 8

Artikel 8 sikrer beskyttelse af EU-borgeres personoplysninger og har følgende ordlyd:

Beskyttelse af personoplysninger [33]

1. Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.

2. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf.

3. Overholdelse af disse regler er underlagt en uafhængig myndigheds kontrol.

Artikel 8 fastlægger således EU-borgeres rettighed til databeskyttelse og danner grundlag for GDPR. Artikel 8, stk. 2, fastlægger, at behandling af personoplysninger skal foregå på lovlige grundlag og kan således forbindes til GDPR artikel 6, som indeholder seks forskellige hjemmelsgrundlag til

[30] EUC
[31] Ibid., artikel 7
[32] Ibid.
[33] Ibid., artikel 8

behandling af almindelige personoplysninger.[34] Ligeledes fastlægger artikel 8, stk. 2, at de registrerede skal have adgang til indsamlede oplysninger, som vedrører disse, og til berigtigelse heraf. GDPR giver de registrerede rettigheder, som enhver virksomhed skal efterleve ved behandling af personoplysninger, herunder en indsigtsret og en ret til berigtigelse, jf. GDPR artikel 15 og 16. Endnu vigtigere kræves der i medfør af artikel 8, stk. 3, at der er en form for uafhængig myndighedskontrol ved behandling af personoplysninger. Disse uafhængige datatilsynsmyndigheder reguleres i GDPR artikel 51-59, som angiver de roller, som de nationale datatilsynsmyndigheder skal påtage sig, herunder at føre tilsyn med, at GDPR's regler efterleves.[35]

Artikel 47

Artikel 47 sikrer, at EU-borgere har adgang til effektive retsmidler samt upartisk domstolsprøvelse og har følgende ordlyd:

Adgang til effektive retsmidler og til en upartisk domstol [36]

Enhver, hvis rettigheder og friheder som sikret af EU-retten er blevet krænket, skal have adgang til effektive retsmidler for en domstol under overholdelse af de betingelser, der er fastsat i denne artikel.

Enhver har ret til en retfærdig og offentlig rettergang inden en rimelig frist for en uafhængig og upartisk domstol, der forudgående er oprettet ved lov. Enhver skal have mulighed for at blive rådgivet, forsvaret og repræsenteret.

Der ydes retshjælp til dem, der ikke har tilstrækkelige midler, hvis en sådan hjælp er nødvendig for at sikre effektiv adgang til domstolsprøvelse.

Artikel 47 fastlægger således EU-borgeres retsstilling, hvis deres rettigheder krænkes. I GDPR artikel 77 indeholdes en klageadgang til tilsynsmyndigheder, mens GDPR artikel 79 indeholder en adgang til effektive retsmidler over for en dataansvarlig eller databehandler. GDPR artikel 77 og 79 implementerer således EUC artikel 47 ved at give EU-borgere klageadgang og adgang til en upartisk domstolsprøvelse.

[34] Udsen, *Databeskyttelsesret*, s. 148
[35] GDPR kapitel 6
[36] EUC artikel 47

Artikel 52

Artikel 52 sætter rammerne for, hvornår begrænsning af grundlæggende rettigheder kan finde sted i overensstemmelse med såkaldte proportionalitetsprincip og har følgende ordlyd:

Rækkevidde og fortolkning af rettigheder og principper [37]

1. Enhver begrænsning i udøvelsen af de rettigheder og friheder, der anerkendes ved dette charter, skal være fastlagt i lovgivningen og skal respektere disse rettigheders og friheders væsentligste indhold. Under iagttagelse af proportionalitetsprincippet kan der kun indføres begrænsninger, såfremt disse er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder.

3. I det omfang dette charter indeholder rettigheder svarende til dem, der er sikret ved den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder, har de samme betydning og omfang som i konventionen. Denne bestemmelse er ikke til hinder for, at EU-retten kan yde en mere omfattende beskyttelse.

Artikel 52, stk. 1, er således særdeles central i den overordnede afvejning mellem databeskyttelse og andre samfundsinteresser. Enhver begrænsning af EU-borgeres private fred og databeskyttelse skal være lovlig, nødvendig og proportionel for at beskytte EU-borgeres rettigheder. Den i artikel 52, stk. 1, fastsatte ramme skal juridisk søge at afgrænse og balancere EU-borgeres rettighed til privatliv og databeskyttelse, jf. EUC artikel 7 og 8, med andre samfundsmæssige legitime hensyn. Dette princip findes i GDPR med krav om eksempelvis dataminimering, lovlig behandling, strenge krav til behandling af personfølsomme oplysninger, og endelig at overførsler ikke må finde sted til tredjelande, som ikke kan garantere en proportionel beskyttelse, jf. GDPR kapitel V, som vil gennemgås senere.[38]

I specialet inddrages udvalgte domme fra EMD som fortolkningsbidrag, hvorfor EUC artikel 52, stk. 3, ligeledes er en central bestemmelse.[39] Stk. 3 skal sikre en sammenhæng mellem EUC og EMRK og fastslår endvidere, at de rettigheder i EUC, som svarer til rettigheder i EMRK, skal tillægges samme betydning. Endvidere indebærer stk. 3, at EU-lovgivning skal fortolkes i overensstemmelse

[37] EUC artikel 52
[38] https://www.ft.dk/samling/2024-25/bilag-149
[39] www.eur-lex.europa.eu/forklaringer-til-euc, forklaring ad artikel 52

med EMRK, herunder praksis fra EMD.[40] Artikel 52, stk. 3, danner således grundlag for specialets inddragelse af domme fra EMD som fortolkningsbidrag i henhold til EU-retlige spørgsmål, herunder fortolkning af nødvendigheds- og proportionalitetsprincipperne. Endelig kræver stk. 3, at EUC's beskyttelsesniveau under alle omstændigheder aldrig må være lavere end EMRK's, hvorfor inddragelse af EMD's praksis understøtter specialets fokus på beskyttelse af EU-borgeres grundlæggende rettigheder og friheder.[41]

Forordning (EU) 2016/679 - GDPR

Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, GDPR, afløste med virkning fra den 25. maj 2018 direktiv 95/46/EF, som tidligere regulerede databeskyttelse i EU.[42] Forordninger har i modsætning til direktiver umiddelbar virkning i medlemsstaterne, hvorfor sådanne ikke kræver national implementering.[43] GDPR's fremsættelse bidrog således til en større harmonisering og ensartethed mellem EU's medlemsstater, eftersom de fik en fælles ramme for databeskyttelse.[44] GDPR gav imidlertid medlemsstaterne mulighed for at opretholde eller indføre egne regler, og i den forbindelse supplerede Danmark med DBL.[45] Fortolkning af GDPR skal tage højde for de retsgrundlag, som betinger GDPR, herunder TEUF artikel 16 og EUC artikel 8 omhandlende databeskyttelse. Endvidere må fortolkningsresultaterne ikke være i strid med EMRK.[46]

GDPR indledes med en præambel, som indeholder 173 betragtninger. Disse præambelbetragtninger giver væsentlige bidrag i henhold til fortolkning og angiver retsaktens baggrund og formål.[47] EUD tillægger ofte præambler betydning ved fortolkning af retsakter, hvorfor præambelbetragtningerne medfører en betydelig forståelse for GDPR's bestemmelser.[48] GDPR som retskilde er en stadig bevægende retskilde, som karakteriseres på samme måde som andre EU-retskilder ved at have en bredere adressatkreds end ved nationale retskilder.[49] GDPR's indhold, anvendelse og rækkevidde

[40] www.eur-lex.europa.eu/forklaringer-til-euc, forklaring ad artikel 52
[41] Ibid.
[42] GDPR
[43] Tvarnø m.fl., *Retskilder og retsteorier*, s. 105
[44] Udsen, *Databeskyttelsesret*, s. 42
[45] Blume, *Persondatarettens kilder og metode*, s. 35
[46] Ibid., s. 58-59
[47] www.datatilsynet.dk/behandling-af-personoplysninger-om-hjemmesidebesøgende
[48] Lando, *Præambel*
[49] Blume, *Persondatarettens kilder og metode*, s. 61

udvikles således løbende gennem eksempelvis praksis fra EUD, hvorfor GDPR er en dynamisk retskilde.

Retspraksis fra EUD

Retspraksis fra EUD har stor betydning for den databeskyttelsesretlige udvikling og forståelse, hvorfor sådan også vil medtages i specialet, navnlig afgørelserne Schrems I og Schrems II.[50] EUD skal i medfør af TEU artikel 19 sikre "*overholdelse af lov og ret*" ved fortolkning og anvendelse af traktaterne.[51] GDPR giver anledning til mange fortolkningsspørgsmål, hvorfor EUD ligeledes skal tage stilling til fortolkningsspørgsmål af mere grundlæggende karakter.[52] Fortolkningstvivl hos andre medlemsstaternes nationale datatilsynsmyndigheder vil således ofte medføre en præjudiciel forelæggelse for EUD, eftersom en stor del af de databeskyttelsesretlige regler dækkes af GDPR.[53] EUD's afsigelse af sådanne afgørelser har således stor betydning for virksomheders og organisationers forståelse af de databeskyttelsesretlige regler. EUD tildeler den primære lovgivning, herunder bestemmelserne i EUC, væsentlig betydning i deres afgørelser.[54] Dette kom til udtryk i Schrems I- og Schrems II-afgørelserne, hvor EUD lagde til grund, at de grundlæggende rettigheder og frihedsrettigheder i EUC skal respekteres ved overførsel af personoplysninger til tredjelande.[55] [56] EUD's afgørelser har stor betydning for fortolkningen af GDPR, hvorfor også nationale præjudicielle forelæggelser samt afgørelser afventer EUD's stillingtagen, som kan have betydning for sagens retsstilling.[57] Dette kan begrundes i, at EU-lovgivning får en stadig større betydning i national lovgivning, hvorfor nogle jurister argumenterer for, at EU som sådan ikke er en selvstændig retsdisciplin, men derimod en del af national lovgivning.[58] Afgørelser fra EUD har således betydning for den databeskyttelsesretlige udvikling, hvorfor Schrems I- og II-afgørelserne vil medtages, eftersom de var afgørende for at skabe de nuværende rammer for tredjelandsoverførsel mellem EU og USA.

EDPB og tilsynsafgørelser

Medlemsstaterne skal i medfør af GDPR etablere en national tilsynsmyndighed, som skal føre tilsyn med overholdelse af de databeskyttelsesretlige regler, jf. artikel 51, og disse datatilsynsmyndigheder

[50] Blume, *Persondatarettens kilder og metode*, s. 68
[51] Hamer og Daniel, *Juridisk metode når EU-retten er i spil*, s. 155
[52] Udsen, *Databeskyttelsesret*, s. 48
[53] Ibid., s. 50
[54] Blume, *Persondatarettens kilder og metode*, s. 68
[55] www.curia.europa.eu/c-362/14 (herefter Schrems I)
[56] www.curia.europa.eu/c-311/18 (herefter Schrems II)
[57] Hamer og Daniel, *Juridisk metode når EU-retten er i spil*, s. 162
[58] Ibid., s. 162

skal fungere i fuld uafhængighed, jf. artikel 52.[59] [60] [61] Denne uafhængige kontrol følger ligeledes af EUC artikel 8, stk. 3.[62] I Danmark reguleres denne uafhængighed efter DBL § 27, hvorefter der skal føres tilsyn med enhver behandling, der omfattes af DBL, GDPR eller andre særregler om behandling af personoplysninger.[63] GDPR regulerer i samspil med nationale regler kravene til de nationale datatilsynsmyndigheder og deres opgaver og kompetencer. DT's kompetencer og beføjelser består eksempelvis i at træffe afgørelser og udarbejde vejledninger om overholdelse af de databeskyttelsesretlige regler.[64] DT pålægges også en række undersøgelsesbeføjelser, jf. GDPR artikel 58, stk. 1, hvorefter DT eksempelvis kan give dataansvarlige og databehandlere påbud.[65] De nationale datatilsynsmyndigheder pålægges således en omfattende rolle i henhold til overholdelse af GDPR og de nationale regler og særregler. Administrativ praksis, herunder praksis fra DT, anerkendes i dansk ret som en retskilde, selvom den ikke er af bindende karakter som lovgivning og bekendtgørelser.[66]

For at understøtte den ønskede harmonisering og ensartethed mellem medlemsstaterne opstod EDPB med GDPR. EDPB består af repræsentanter for medlemsstaternes datatilsynsmyndigheder og EDPS.[67] EDPB udstyres i medfør af GDPR artikel 70 med en lang række opgaver, herunder at sikre den såkaldte sammenhængsmekanisme ved at afgive udtalelser, træffe afgørelser og give generel vejledning for at præcisere GDPR.[68] [69]

Vejledninger og anbefalinger fra de nationale tilsynsmyndigheder, herunder DT, og EDPB er imidlertid ikke autoritative retskilder, hvorfor sådanne ikke er bindende for domstolene.[70] Vejledninger og anbefalinger skal således opfattes som de uafhængige databeskyttelsesmyndigheders fortolkninger af de databeskyttelsesretlige regler. Udtalelser fra EDPB kvalificeres imidlertid som soft law, eftersom de anses for at have væsentlig betydning for fortolkning af databeskyttelsesretten, og således bør tillægges en betydelig vægt.[71]

---

[59] Udsen, *Databeskyttelsesret*, s. 377
[60] GDPR artikel 51
[61] Ibid. artikel 52
[62] EUC artikel 8
[63] www.retsinformation.dk/2018/502 (herefter DBL) § 27
[64] Udsen, *Databeskyttelsesret*, s. 50
[65] GDPR artikel 58
[66] Blume, *Persondatarettens kilder og metode*, s. 48
[67] www.datatilsynet.dk/det-europæiske-databeskyttelsesråd-edpb
[68] GDPR artikel 70
[69] Udsen, *Databeskyttelsesret*, s. 383
[70] Ibid.
[71] Næsborg og Hjerrild, *Juridisk metode anvendt på persondataretten*, s. 269-270

Juridisk litteratur

I Specialet medtages juridisk litteratur i form af faglige bøger og artikler. Juridisk litteratur udgør imidlertid ikke en retskilde, men kan tjene til inspiration ved at indeholde en juridisk argumentation eller ved at indeholde anerkendte videnskabelige resultater.[72]

[72] Munk, *Den juridiske løsning*, s. 74

5 Struktur

Følgende kapitel har til formål at skabe et overblik over specialets opbygning samt beskrive sammenhængen og formålet i relation til strukturen og indholdet. Gennem en indledning i kapitel 1 vil specialets baggrund samt relevans beskrives og præsenteres. Herefter vil specialets problemformulering, som ligger til grund for specialets analyse, præsenteres i kapitel 2. I kapitel 3 følger en afgrænsning, hvor der redegøres for henholdsvis til- og fravalg, eftersom alle aspekter af tredjelandsoverførsler som emne ikke kan behandles. I kapitel 4 behandles specialets metode, de relevante retskilder og EUC artikler, som specialets analyse bygger på.

I kapitel 6 gennemgås de relevante artikler i GDPR kapitel V, eftersom kapitlet omhandler overførsel af personoplysninger til tredjelande eller internationale organisationer. Artiklerne behandles, eftersom disse udgør retsgrundlagene for alle overførsler af personoplysninger fra EU til et tredjeland, herunder USA. Efterfølgende vil kapitel 7 indledes med en retshistorisk belysning af baggrunden for databeskyttelsesrammerne mellem EU og USA. Dette medtages for at uddybe konteksten, som ligger bag de relevante elementer for dataoverførsel til USA. I kapitel 7 vil de tidligere ugyldiggjorte tilstrækkelighedsafgørelser og dataoverførselsaftaler mellem USA og EU, herunder Safe Harbor og Privacy Shield, endvidere gennemgås. Dertil vil relevante amerikanske overvågningslove også inddrages, herunder FISA 702 og EO 12333. Dette indhold medtages for at skabe en nærmere forståelse af Schrems I- og II-afgørelserne, eftersom der i kapitel 7 vil tages udgangspunkt i disse afgørelser med henblik på at forklare de væsentligste præmisser, som blev udledt af EUD. I kapitel 7 vil den nye tilstrækkelighedsafgørelse og DPF afslutningsvist præsenteres. I kapitel 8 vil EO 14086 forklares og uddybes med henblik på at præsentere de krav, begrænsninger og garantier, som dekretet indeholder, herunder relevante organer samt fokus på proportionalitets- og nødvendighedsprincipperne. Dekretet vil blive beskrevet, eftersom dette er fundamentet for stiftelsen af DPF. Denne dataoverførselsaftale er nuværende gældende ret for overførsel af personoplysninger mellem EU og USA, hvorfor en gennemgang af EO 14086 er betydningsfuld.

I kapitel 9 vil det analyseres og diskuteres, hvorvidt begrænsningerne og garantierne i EO 14086 medfører, at der foreligger en overensstemmelse med EU-retten, herunder tilstrækkelig databeskyttelse. Formålet her er at vurdere, om tiltagene i dekretet afhjælper de mangler, som blev konstateret i Schrems I- og II-afgørelserne for tidligere dataoverførselsaftaler. I kapitel 10 undersøges, hvordan og hvornår implementering af supplerende foranstaltninger kan medføre, at SCC'er kan anvendes som et alternativt tilstrækkeligt overførselsgrundlag på trods USA's

problematiske lovgivning og praksis. Dette vil bestå af udvalgt retspraksis fra individuelle datatilsynsmyndigheder og nationale domstole samt EDPB's vejledning vedrørende supplerende foranstaltninger med henblik på at besvare problemformuleringen. Formålet og begrundelsen for medtagelsen af dette er af samme grundlag som i afgrænsningen, jf. kapitel 3. I kapitel 11 vil der indledningsvis foretages en gennemgang af kravene til en databehandleraftale, grundet relevansen dette har i relation til CLOUD Act. Derefter vil udfordringerne ved anvendelsen af CLOUD Act analyseres og beskrives med inddragelse af MLAT, relevante GDPR artikler samt KOMBIT-sagen. Formålet med dette kapitel er at undersøge baggrunden for de aktuelle komplikationer, som kan opstå, såfremt en databehandler bliver omfattet af CLOUD Act. Dertil udledes, hvordan en dataansvarlig bør agere eller sikre sig mod sådanne situationer. CLOUD Act medtages, eftersom denne amerikanske lovgivning ligeledes kan komplicere en lovlig tredjelandsoverførsel til USA.

I kapitel 12 følger en diskussion af fremtidige forhold og forventninger til en potentiel Schrems III-afgørelse samt dataoverførsel til USA generelt. Dertil vil en række praktiske anbefalinger og konsekvenser for virksomheder diskuteres på baggrund af den generelle usikkerhed vedrørende DPF. Afslutningsvis indeholder kapitel 13 en konklusion på specialets problemformulering.

6 Databeskyttelsesforordningens kapitel V

Overførsel af personoplysninger til tredjelande eller internationale organisationer

Dette kapitel vil fastlægge GDPR's bestemmelser, krav og generelle principper samt relevante retningslinjer af EDPB vedrørende tredjelandsoverførsler. Indholdet i disse retskilder danner tilsammen grundlaget for overførsel af personoplysninger til tredjelande eller internationale organisationer. Derudover indeholder kapitel V en udtømmende liste over overførselsgrundlag.[73]

Betydning af overførsel og tredjeland

Uagtet overførselsbegrebet og tredjelandsbegrebets væsentlighed findes der ikke en legaldefinition i GDPR for disse betegnelser, jf. GDPR artikel 4. Definitionen af *tredjelande* kan imidlertid udledes gennem juridisk litteratur som værende en betegnelse af lande, som ikke er en del af EU-medlemsstaterne eller EØS-landene.[74] I forhold til overførselsbegrebet har EDPB gennem deres retningslinjer statueret tre kumulative kriterier, som medfører, at en behandlingsaktivitet anses som værende en *overførsel*: 1) Den pågældende dataansvarlige eller databehandlers (dataeksportør) behandlingsaktiviteter omfattes af GDPR, 2) Ved den pågældende behandlingsaktivitet videregiver (eller på anden vis stiller til rådighed) dataeksportøren de aktuelle personoplysninger til andre dataansvarlige, databehandlere eller fælles dataansvarlige (dataimportør), 3) Den pågældende dataimportør er beliggende i et tredjeland eller en international organisation. Det er i denne kontekst irrelevant, om den givne behandlingsaktivitet omfattes af GDPR.[75] [76]

Artikel 44 - Generelle princip for overførsel

Denne artikel beskriver det generelle princip ved overførsel af personoplysninger til tredjelande eller internationale organisationer, som indebærer, at øvrige artikler samt bestemmelserne i GDPR kapitel V skal overholdes, før en tredjelandsoverførsel kan finde sted. Disse bestemmelser har til formål at sikre, at det databeskyttelsesniveau, som finder anvendelse inden for EU og EØS, ikke undermineres ved overførsel af personoplysninger til tredjelande, jf. artikel 44.

Artikel 45 - Overførsler, som baseres på en afgørelse om tilstrækkelighed af beskyttelsesniveau

Artikel 45 fastsætter, at en overførsel af personoplysninger til et tredjeland eller en international organisation kan udføres, såfremt EUK har fastslået dette gennem en tilstrækkelighedsafgørelse. For

[73] Udsen, *Databeskyttelsesret*, s. 328-331
[74] Ibid., s. 28 og s. 331-342
[75] www.edpb.europa.eu/retningslinjer-05/21-om-internationale-overførsler
[76] www.datatilsynet.dk/Vejledning-om-overførsel-til-tredjelande, s. 6

at sådanne beslutninger kan træffes, skal det afgøres, om databeskyttelsesniveauet er væsentligt tilsvarende det niveau, som sikres i EU- og EØS-landene. Dette kan besluttes for et givent område, en sektor eller generelt for hele tredjelandet. EUK skal i denne henseende foretage en udførlig vurdering af det juridiske og institutionelle grundlag for databeskyttelse i det pågældende tredjeland. I denne kontekst skal det eksempelvis undersøges, hvorvidt der findes tilstrækkelighed vedrørende de registreredes rettigheder, adgangen til personoplysninger for myndigheder og uafhængige tilsynsmyndigheder. I tilfælde af en afgørelse om en tilstrækkelig databeskyttelse, indgår tredjelandet under betegnelsen *sikkert tredjeland*, jf. artikel 45. I forbindelse med overførsler til USA kan dette ske, såfremt den pågældende modtager af personoplysningerne er certificeret under DPF.[77]

Artikel 46 - Overførsler, som omfattes af fornødne garantier

Denne artikel fastlægger, at det stadig er muligt at overføre personoplysninger til et tredjeland eller en international organisation i situationer, hvor der ikke er vedtaget en tilstrækkelighedsafgørelse. Overførslen kan kun finde sted, såfremt den dataansvarlige eller databehandleren stiller fornødne garantier. Dertil er det betinget af, at de registrerede har adgang til effektive retsmidler samt håndhævelse af deres rettigheder. Dette kan muliggøres gennem diverse retlige bindende instrumenter som SCC'er, jf. artikel 46. Denne artikel har væsentlig indflydelse i praksis, eftersom den introducerer adskillige muligheder for overførsel til tredjelande eller internationale organisationer i mangel af en tilstrækkelighedsafgørelse.[78]

Artikel 48 - Overførsel eller videregivelse, som ikke har en EU-retlig hjemmel

Artikel 48 fastsætter, at en videregivelse eller overførsel af personoplysninger til tredjelande på baggrund af en dom eller afgørelse afsagt af en autoritet i et tredjeland kun kan finde sted, såfremt dommen eller afgørelsen hjemles i en international aftale mellem medlemsstaten eller EU og tredjelandet, jf. artikel 6 og 48. Denne artikel er med til at sikre, at autoriteter i et tredjeland ikke ensidigt kan forlange adgang til personoplysninger fra EU.[79] Det er væsentligt at pointere, at EDPB har fastlagt, at artikel 48 ikke i sig selv kan udgøre et grundlag for overførsel.[80]

[77] www.datatilsynet.dk/international/tredjelandsoverførsler
[78] www.gdprhub.eu/Article-46-GDPR
[79] www.gdprhub.eu/Article-48-GDPR
[80] www.edpb.europa.eu/EDPB-Guidelines-02/2024-Article-48, (10)

Artikel 49 - Undtagelser i særlige situationer

I fraværet af en tilstrækkelighedsafgørelse, jf. GDPR artikel 45, stk. 3, og fornødne garantier, jf. GPDR artikel 46, findes der en udtømmende liste af undtagelser i denne bestemmelse. Disse undtagelser skal anses som en sidste mulighed og kan således kun benyttes, såfremt de andre overførselsgrundlag er uanvendelige.[81] Brug af undtagelserne skal desuden overholde det generelle princip for overførsel til tredjelande, jf. artikel 44. Derudover skal anvendelsesområdet for undtagelserne fortolkes indskrænkende, så de dermed ikke benyttes regelmæssigt, eftersom der kan forekomme en øget risiko for de registrerede.[82]

Relevante undtagelser i artikel 49 omfatter, at en overførsel skal være:
(d) Nødvendig for væsentlige samfundsinteresser
(e) Nødvendig for fastlæggelse, udøvelse eller forsvar af retskrav
(f) Nødvendig for beskyttelse af den registreredes eller andre personers vitale interesser

Der findes en endelig undtagelse i artikel 49, stk. 1, andet afsnit, som udelukkende kan benyttes, såfremt de ovenstående undtagelser i litra a-g også er uanvendelige. Denne undtagelse kræver, at der foreligger vægtige legitime interesser for den dataansvarlige. Derudover må overførslen af personoplysninger ikke gentages og må kun involvere en begrænset mængde af registrerede. Det er ligeledes et krav, at den registreredes rettigheder og interesser ikke går forud for den legitime interesse for den dataansvarlige. Endelig skal den dataansvarlige foretage risikovurderinger, indføre passende sikkerhedsforanstaltninger og dokumentere samt underrette den registrerede og tilsynsmyndigheden om relevant information.[83]

[81] www.edpb.europa.eu/EDPB-Guildelines-2/2018-Article-49, s. 3-4
[82] www.gdprhub.eu/Article-49-GDPR
[83] Ibid.

7 Schrems I og II

Følgende kapitel vil belyse den databeskyttelsesretlige baggrund og udvikling forbundet med Schrems I- og II-afgørelserne. I det nedenstående vil Schrems-afgørelserne blive analyseret, og der vil redegøres for, hvordan rammerne for tredjelandsoverførsel til USA har ændret sig i takt med udfaldet af disse domme. Dette inkluderer også beskrivelser af Safe Harbor (2000), Privacy Shield (2016) og Data Privacy Framework (2023), som er de dataoverførselsaftaler, som USA og EU har indgået igennem årene. Endelig vil relevant amerikansk lovgivning inddrages i relevant rækkefølge for Schrems-afgørelserne for at skabe en forståelse bag de præmisser, begrundelser og beslutninger, som EUD har lagt til grund for sine konklusioner i Schrems I- og II-afgørelserne.

7.1 Historisk databeskyttelsesbaggrund for Schrems I- og II-afgørelserne

Edward Snowden afslørede i 2013, hvordan amerikanske efterretningstjenester som National Security Agency overvågede og tilgik EU-borgeres personoplysninger gennem den amerikanske overvågningslovgivning, FISA 702. Denne omfattende overvågning og adgang blev anset som særlig kritisk, eftersom mængden af personoplysninger fra EU til USA var af væsentlig stigende karakter grundet virksomheder som Facebook, Microsoft og Google. FISA 702 muliggjorde, at efterretningstjenesterne i USA kunne kræve udlevering af personoplysninger fra EU-borgere i forbindelse med telekommunikationsudbydere. Der var i denne kontekst tale om masseovervågning frem for specifik og konkret overvågning, eftersom overvågning af EU-borgere ikke krævede specifikke godkendelser. Snowdens offentliggørelser markerede begyndelsen på Schrems-afgørelserne, eftersom Max Schrems indgav en klage på baggrund af anfægtelsen om, at USA's databeskyttelse ikke var tilstrækkelig.[84]

7.2 Foreign Intelligence Surveillance Act 702

Efter en gennemgang af den historiske databeskyttelsesbaggrund for Schrems I- og II-afgørelserne er det relevant at inddrage FISA 702, eftersom EUD tog stilling til USA's generelle databeskyttelsesniveau, og om det var tilsvarende de EU-retlige standarder, jf. GDPR artikel 45. FISA 702 udgør det juridiske grundlag for amerikanske efterretningstjenesters overvågningsaktiviteter og dataindsamling, herunder godkendelse af amerikanske overvågningsprogrammer som Prism og

[84] www.noyb.eu/eu-us-data-transfers

Upstream.[85] Section 702 i FISA giver nationale efterretningstjenester omfattende adgang til at indsamle, analysere og dele udenlandske efterretningsoplysninger vedrørende trusler mod den nationale sikkerhed. Dette omfatter indhentelse af efterretningsoplysninger, såsom oplysninger om international terroisme eller erhvervelse af masseødelæggelsesvåben. Section 702 giver kun adgang til at målrette en indsamling til *non-U.S persons*,[86] mens den daværende Section 215 gav en udvidet adgang til masseindsamling.[87] Denne Section blev imidlertid fjernet i forbindelse med vedtagelsen af USA Freedom Act fra 2015, som yderligere medførte, at der skulle forekomme mere transparente forhold for FISC. Dertil skulle tech-giganter som Google og Facebook underrette befolkningen, når efterretningstjenester fik videregivet data. Der er imidlertid fastsat en begrænsning i forhold til Section 702, eftersom der ikke kan foretages masseindsamling af efterretningsoplysninger. Indsamlingen skal således være præciseret, individualiseret og dokumenteret. Selvom Section 702 udelukkende kan anvendes over for *non-U.S persons*, vil den alligevel kunne anvendes, såfremt en udenlandsk terrorist indikerer, at en amerikansk borger er et centralt medlem af en terrorhandling.[88]

7.3 Safe Harbor

EUK vedtog den 26. juli 2000 tilstrækkelighedsafgørelse 2000/520, som etablerede certificeringsordningen Safe Harbor.[89] Såfremt amerikanske virksomheder blev certificeret gennem denne ordning, blev det vurderet, at databeskyttelsesniveauet var tilstrækkeligt ækvivalent med databeskyttelsesniveauet i EU, som var sikret gennem det daværende persondatadirektiv.[90] På dette grundlag kunne personoplysninger fra EU-borgere lovligt overføres til de certificerede amerikanske virksomheder. Safe Harbor-ordningen blev imidlertid ugyldiggjort i Schrems I-afgørelsen af 6. oktober 2015, hvorefter den i 2016 blev erstattet af Privacy Shield-ordningen.[91]

[85] www.cdt.org/wp-2017/02/Section-702
[86] *Defineres som personer, der ikke har amerikansk statsborgerskab eller befinder sig i USA*
[87] www.intelligence.gov/foreign-intelligence-surveillance-act-fisa-section-702
[88] www.intelligence.gov/fact-sheet-implementation-of-the-usa-freedom-act-of-2015
[89] www.eur-lex.europa.eu/beslutning-2000/520
[90] www.eur-lex.europa.eu/direktiv-95/46/EF
[91] Udsen, *Databeskyttelsesret*, s. 344-345

7.4 Schrems I

I EUD's afgørelse af den 6. oktober 2015, som er refereret i C-362/14, var et væsentligt emne, hvorvidt tilstrækkelighedsafgørelsen i forbindelse med Safe Harbor-ordningen var gyldig grundet anfægtelserne af Max Schrems vedrørende databeskyttelsesniveauet i USA.

> Personoplysninger tilhørende EU-borger og Facebook-bruger Max Schrems blev overført til Facebooks servere i USA af Facebook Irland. Facebook anvendte i denne kontekst den daværende tilstrækkelighedsafgørelse som overførselsgrundlag. Schrems påstod, at databeskyttelsesniveauet i USA ikke var tilstrækkeligt grundet blandt andet Edward Snowdens afsløringer og amerikansk lovgivning. På baggrund af dette mente Schrems, at EU-borgeres rettigheder var tilsidesat, eftersom de amerikanske efterretningstjenester havde omfattende adgang til EU-borgeres personoplysninger. Schrems klagede i 2013 til den irske databeskyttelseskommissær, hvorefter sagen blev forelagt for den irske højesteret som følge af kommissærens afgørelse. Højesteretten i Irland forelagde herefter en række spørgsmål for EUD ved en præjudiciel afgørelse.[92] [93]

Tilstrækkeligt databeskyttelsesniveau

EUD fastslog, at det var forbudt at overføre personoplysninger til tredjelande, såfremt der ikke var et tilstrækkeligt databeskyttelsesniveau, jf. persondatadirektivet artikel 25, stk. 1.[94] Uagtet dette fandtes der ikke en direkte definition af, hvad et *tilstrækkeligt databeskyttelsesniveau* indebar. Det var derimod en vurdering, som skulle bedømmes med grundlag i adskillige forhold, som havde betydning for en overførsel, jf. persondatadirektivet artikel 25, stk. 2.[95] Dertil skulle tilstrækkelighedsvurderingen ske med det formål at sikre beskyttelse af individers grundlæggende rettigheder og friheder samt privatliv. Dette skulle sikres gennem et tredjelands lovgivning eller internationale forpligtelser, som her var et væsentlig grundlag for en tilstrækkelighedsvurdering, jf. artikel 25, stk. 6.[96]

[92] www.datatilsynet.dk/international/sager-ved-eud
[93] Schrems I
[94] Ibid., præmis 68
[95] Ibid., præmis 70
[96] Ibid., præmis 71

EUD fastlagde desuden, at betydningen af *et tilstrækkeligt databeskyttelsesniveau* indebar, at det som i det væsentlige er ækvivalent med det sikrede databeskyttelsesniveau i EU, således at persondatadirektivet ikke kunne tilsidesættes. Der var dermed ikke et krav om, at databeskyttelsesniveauet skulle være identisk med det i EU.[97] Det påhviler i denne sammenhæng EUK at kontrollere et tredjelands lovgivning, forpligtelser samt retspraksis vedrørende databeskyttelsesområdet regelmæssigt. Dette gælder især, når tilstrækkeligheden i tredjelandet kan betvivles grundet aktuelle omstændigheder.[98]

Gyldighed af beslutning 2000/520

I henhold til beslutning 2000/520 blev det fastlagt, at hensynene til national sikkerhed, offentlig interesse eller retshåndhævelse havde forrang over de databeskyttelsesretlige principper i Safe Harbor. Dette betød, at de amerikanske certificerede virksomheder var forpligtede til at efterleve national lovgivning, såfremt der blev indgivet krav begrundet i de ovennævnte hensyn. EUD fandt, at dette muliggjorde indgreb i de grundlæggende rettigheder hos EU-borgere ved overførsel. I denne sammenhæng var det ikke tydeliggjort, hvorvidt der forelå begrænsninger i disse indgreb eller hvilke ingrebsformer, som kunne anvendes. Hertil bemærkede EUD, at beslutning 2000/520 ikke indeholdt tilstrækkelige garantier for effektiv domstolsbeskyttelse eller tilgængelige retsmidler for de registrerede, som blev berørt af de nævnte indgreb.[99]

EUD fandt endvidere, at beslutning 2000/520 muliggjorde en behandling af personoplysninger i et omfang, som gik ud over, hvad der var strengt nødvendigt. Dette var begrundet i en tilsidesættelse af overførslernes formål og de omfattende hensyn til national sikkerhed.[100] Omstændighederne stod i kontrast til EUD's retspraksis, hvori ethvert indgreb i de grundlæggende rettigheder forudsætter en fastlæggelse af de krav, der kontrollerer forholdene for indgrebene. Dette er med til at sikre, at berørte registrerede har mulighed for at beskytte deres personoplysninger i tilfælde, hvor dette findes begrundet og aktuelt. Dette forhold skærpes ved involvering af automatisk databehandling, eftersom der foreligger en forøget risiko for de registrerede.[101] EUD fandt, at der på baggrund af de ovenstående forhold ikke var tale om begrænsninger med forbehold for streng nødvendighed. Indgrebene udgjorde således en tilsidesættelse af EUC artikel 7 på baggrund af deres generelle karakter i forhold til

[97] Schrems I, præmis 73
[98] Ibid., præmis 75-76
[99] Ibid., præmis 86-87
[100] Ibid., præmis 88-90
[101] Ibid., præmis 91-92

adgangen til personoplysninger. Endvidere fandtes rettighederne i EUC artikel 47 også krænket, eftersom der ikke var adgang til effektive retsmidler ved en krænkelse.[102]

EUD erklærede på baggrund af de ovenstående beskrevne omstændigheder, som fulgte af beslutning 2000/520 sammenholdt med amerikansk lovgivning, at artikel 1 i beslutning 2000/520 var ugyldig. Denne ugyldighed skyldtes beslutningens tilsidesættelse af persondatadirektivet artikel 25, stk. 6, samt de grundlæggende rettigheder i EUC.[103] EUD fastlagde yderligere, at de nationale datatilsynsmyndigheder i EU-medlemsstater skulle operere i fuld uafhængighed med henblik på at beskytte EU-borgeres rettigheder og friheder på baggrund af indgivne anmodninger. Dette var relevant for databeskyttelse og anfægtelser mod tilstrækkelighedsafgørelser med hensyn til persondatadirektivet artikel 25, stk. 6, jf. persondatadirektivet artikel 28 og EUC artikel 8. Dermed fandtes der ikke lovhjemmel til at indskrænke tilsynsmyndighedernes beføjelser. Det blev imidlertid vurderet, at artikel 3 i beslutning 2000/520 fastsatte, at de nationale datatilsynsmyndigheder var afskåret fra at sikre overholdelse af persondatadirektivet artikel 25 gennem foranstaltninger, som bestred en tilstrækkelighedsafgørelses forenelighed med de grundlæggende rettigheder i EUC. EUD fastslog på baggrund af dette, at indskrænkningen i artikel 3 i beslutning 2000/520 var en overskridelse af EUK's kompetence, og at artikel 3 dermed var ugyldig.[104]

Ovenstående medførte, at Safe Harbor-ordningen i sin helhed blev erklæret for ugyldig af EUD, eftersom både artikel 1 og 3 i beslutning 2000/520 var uadskillelige fra beslutningens øvrige bestemmelser, og individuelt blev fastslået til at være ugyldig.[105]

7.5 Executive Order 12333

For at forstå nogle af de udfordringer, som var centrale i Schrems II, er det nødvendigt at inddrage EO 12333, eftersom denne giver de amerikanske efterretningstjenester vidtrækkende beføjelser til indsamling af oversøiske overvågningsaktiviteter uden de retssikkerhedsgarantier, som kræves i medfør af EUC. Inddragelsen af EO 12333 er således essentiel for en fuldstændig analyse af de udfordringer, som blev adresseret i Schrems II.

[102] Ibid., præmis 93-96
[103] Ibid., præmis 98
[104] Schrems I, præmis 99-104
[105] Ibid., præmis 105-106

Dekreter, herunder 12333, bliver udstedt af den amerikanske præsident, hvorfor Kongressen ikke skal vedtage dem, før de har virkning. Kongressen kan ydermere ikke ugyldiggøre dekreter, eftersom de ikke anses for at være lovgivning, fordi aktualiseringen af disse ikke er sket gennem Kongressen.[106] EO 12333 er et amerikansk juridisk grundlag for indsamling af oversøiske overvågningsaktiviteter. I modsætning til FISA 702 kan EO 12333 benyttes til masseindsamling af data og målrettet indsamling af bestemte grupper eller personer. Eftersom EO 12333 er et dekret, er anvendelsen af denne ikke underlagt tilsyn af den amerikanske domstol eller Kongressen. Yderligere kræves der ikke en dommerkendelse for at kunne anvende dette juridiske grundlag som hjemmel for indsamling. FISA 702 giver udelukkende hjemmel til præciseret og målrettet overvågning eller indsamling, hvor der yderligere kræves en godkendelse af domstolene, såsom FISC. Denne indsamling kan ske gennem masseindsamling af signaldata gennem overvågning af undervandskabler, satellitter eller andre trådløse kommunikationsmidler uden for USA. Anvendelsesområdet for EO 12333 giver amerikanske efterretningstjenester adgang til at overvåge stort set alle former for kommunikation uden for USA. Dette giver efterretningstjenesterne vide beføjelser til at indsamle og udnytte personoplysninger uden for USA. Brugen af EO 12333 har været diskutabel, eftersom den kun kan benyttes på områder eller lande uden for USA. Begrænsningen forhindrer imidlertid ikke, at data indsamles om amerikanske statsborgere, der befinder sig udenfor landets grænser.[107]

Fra et amerikansk synspunkt er forskellen mellem EO 12333 og FISA 702 dermed, at efterretningstjenesterne er underlagt strengere regelsæt, såfremt de har en potentiel chance for at indsamle data eller personoplysninger om personer inden for de amerikanske grænser, hvilket hjemles i FISA 702, hvorfor reglerne deri er mere omfattende.

7.6 Privacy Shield

EUK vedtog den 12. juli 2016 tilstrækkelighedsafgørelse 2016/1250, som etablerede certificeringsordningen Privacy Shield.[108] Denne ordning skulle adressere de problematikker, der havde ført til Safe Harbor-ordningens ugyldighed, herunder ved at etablere en amerikansk ombudsmandsmekanisme som et uafhængigt tilsyn af de amerikanske efterretningstjenester. Ligesom den tidligere certificeringsordning skulle Privacy Shield fungere som retsgrundlaget for overførsel af

[106] www.americanbar.org/what-is-an-executive-order
[107] Toh, Patel og Goitein, *Overseas Surveillance in an Interconnected World*
[108] www.eur-lex.europa.eu/gennemførelsesafgørelse-2016/1250

personoplysninger fra EU til USA. Privacy Shield-ordningen blev imidlertid erklæret ugyldig ved Schrems II-afgørelsen af den 16. juli 2020, hvorefter den i 2023 blev erstattet af DPF.[109] [110]

7.7 Schrems II

I EUD's afgørelse af den 16. juli 2020, som er refereret i C-311/18, var et centralt spørgsmål, om Privacy Shield-ordningen og SCC'er kunne udgøre et gyldigt retsgrundlag for overførsel af personoplysninger til USA.

> Efter Schrems I-afgørelsen annullerede den irske højesteret afgørelsen om at afvise Max Schrems' klage og hjemviste sagen til den irske databeskyttelseskommissær. I forbindelse med genoptagelsen af sagen forklarede Facebook Irland, at de anvendte SCC'er som overførselsgrundlag, hvorfor ugyldiggørelsen af Safe Harbor-ordningen ikke var relevant i denne kontekst. Max Schrems indgav herefter en revideret klage, hvor det blev anfægtet, at Facebooks tvungne videregivelse af personoplysninger til amerikanske efterretningstjenester med hjemmel i amerikansk lovgivning var i strid med EUC artikel 7, 8 og 47. Den irske databeskyttelseskommissær indbragte sagen for den irske højesteret, som derefter forelagde sagen for EUD med henblik på at vurdere gyldigheden af SCC'er ved en præjudiciel afgørelse.[111]

Tilstrækkeligt databeskyttelsesniveau

EUD blev anmodet om at præcisere, hvilke krav der gælder for SCC'er i forhold til at sikre et tilstrækkeligt databeskyttelsesniveau, samt hvilke hensyn der skal indgå i vurderingen heraf.[112] EUD fremhævede, at der ved overførsel af personoplysninger skal foreligge fornødne garantier, herunder adgang for de registrerede til effektive retsmidler og håndhævelse af deres rettigheder, jf. GDPR artikel 46, stk. 1.[113] Dertil fastslog EUD, at artikel 46 skal sammenholdes med det generelle princip i GDPR artikel 44, hvor det beskrives, at databeskyttelsesniveauet ikke må undermineres.[114] EUD

[109] Udsen, *Databeskyttelsesret*, s. 345-346
[110] Schrems II, præmis 43
[111] Ibid.
[112] Ibid., præmis 90
[113] Ibid., præmis 91
[114] Ibid., præmis 92

bestyrkede i Schrems II desuden Schrems I, præmis 73, om tilstrækkelig ækvivalent databeskyttelse, jf. GDPR og EUC.[115]

Såfremt der ikke foreligger en tilstrækkelighedsafgørelse i henhold til GDPR artikel 45, påhviler det dataeksportøren at sikre et tilsvarende databeskyttelsesniveau gennem fornødne garantier, som svarer til det beskyttelsesniveau, som ville være sikret ved en tilstrækkelighedsafgørelse.[116] [117] EUD fandt, at forhold som kontraktvilkår, dataimportøren generelt, de offentlige myndigheders adgang til personoplysninger i tredjelandet samt de lovmæssige omstændigheder i denne kontekst har betydning for vurderingen af databeskyttelsesniveauet. De lovmæssige omstændigheder svarer i denne sammenhæng til de forhold, som er fremlagt i artikel 45, stk. 2, dog uden at denne bestemmelse udgør en udtømmende liste.[118]

Gyldighed af SCC'er

EUD blev anmodet om en afgørelse vedrørende gyldigheden af SCC'er i betragtning af EUC artikel 7, 8 og 47.[119] Dette var begrundet i tvivlen vedrørende den tilstrækkelige databeskyttelse ved anvendelse af SCC'er, eftersom myndigheder i tredjelande ikke er bundet af disse bestemmelser.[120]

EUD udledte, at der potentielt kan forekomme situationer, hvor anvendelsen af SCC'er ikke med garanti kan sikre en tilstrækkelig databeskyttelse. Dette scenarie kan opstå, når tredjelandes lovgivninger muliggør indgreb af myndigheder i rettighederne tilhørende de registrerede.[121] EUD fastslog endvidere, at EUK ikke er forpligtet til at undersøge databeskyttelsesniveauets tilstrækkelighed i de tredjelande, hvor SCC'er kan benyttes som overførselsgrundlag i forbindelse med vedtagelsen af en sådan aftale.[122] Det påhviler dermed enten den dataansvarlige eller databehandleren at sikre de fornødne garantier ved anvendelse af SCC'er.[123] [124] EUD udledte, at en dataeksportør kan forpligtes til at indføre supplerende foranstaltninger, såfremt omstændighederne for dataoverførslen taler for dette.[125] [126] Såfremt de supplerende foranstaltninger ikke kan indføres på

[115] Schrems II, præmis 94
[116] Ibid., præmis 95-96
[117] GDPR betragtning 108
[118] Schrems II, præmis 104
[119] Ibid., præmis 122
[120] Ibid., præmis 123 og 125
[121] Ibid., præmis 126
[122] Ibid., præmis 130
[123] Ibid., præmis 131 og 95-96
[124] GDPR, betragtning 108 og 114
[125] Schrems II, præmis 132-134
[126] GDPR, betragtning 109

trods af nødvendigheden grundet tredjelandes lovgivning, er dataeksportørerne eller subsidiært datatilsynsmyndighederne forpligtet til at afbryde eller forbyde den pågældende overførsel.[127]

EUD fastslog yderligere, at den dataansvarlige, dataimportørerne samt eventuelle databehandlere er forpligtede til at sikre overensstemmelse med GDPR ved behandling og videregivelse af personoplysninger.[128] I medfør af standardbestemmelserne skal dataimportørerne desuden informere dataeksportørerne, såfremt modtageren ikke længere kan sikre efterlevelse af SCC'erne. Personoplysninger skal i en sådan situation tilintetgøres eller returneres til dataeksportøren. Dette kan forekomme, såfremt dataimportøren med begrundet tro indser, at potentielle lovændringer eller omstændigheder vedrørende fortrolighed i tredjelandet vil have betydning for efterlevelse af krav og forpligtelser.[129] Dataeksportører er i denne henseende forpligtede til at afbryde eller forbyde den pågældende overførsel, såfremt SCC'erne ikke kan efterleves.[130] Før en overførsel igangsættes, påhviler det desuden dataeksportøren og dataimportøren at sikre, at tredjelandets lovgivning muliggør efterlevelse af SCC'erne. Dog finder undtagelserne vedrørende offentlig sikkerhed, staten og forsvaret anvendelse i denne sammenhæng, såfremt de opfylder proportionalitetsprincippet.[131]

EUD udledte på baggrund af ovenstående, at SCC'er kunne opretholde sin gyldighed som overførselsgrundlag, eftersom der ikke fandtes belæg for en tilsidesættelse af de grundlæggende rettigheder eller GDPR på baggrund af de fremførte betragtninger.[132]

Gyldighed af Privacy Shield

EUD blev anmodet om at tage stilling til gyldigheden af Privacy Shield, eftersom det blev anfægtet, at USA som tredjeland ikke sikrede et tilstrækkeligt databeskyttelsesniveau.[133] Det skulle derfor afklares, om tilstrækkelighedsafgørelsen fastslog, at USA som tredjeland opretholdt et databeskyttelsesniveau, som var væsentligt ækvivalent med det, der er garanteret inden for EU.[134]

EUD fastlagde, at selve indholdet i Privacy Shield sikrede et tilstrækkeligt databeskyttelsesniveau gennem de principper, som var udformet af det amerikanske handelsministerium.[135] Principperne

[127] Schrems II, præmis 135
[128] Ibid., præmis 138
[129] Ibid., præmis 139 og 144
[130] Ibid., præmis 140
[131] Ibid., præmis 141
[132] Ibid., præmis 149 og 202
[133] Schrems II, præmis 159-160
[134] Ibid., præmis 162
[135] Ibid., præmis 163

kunne imidlertid fraviges, såfremt der forelå hensyn, som var begrundet i retshåndhævelse, offentlig interesse eller national sikkerhed. I denne sammenhæng vurderede EUD, at sådanne hensyn havde forrang for principperne i Privacy Shield, ligesom det var tilfældet med Safe Harbor-ordningen.[136] EUD udledte, at disse hensynsundtagelser var af generel karakter, og dermed muliggjorde indgreb i de registreredes grundlæggende rettigheder. Dette blev nærmere præciseret ved efterretningstjenesternes generelle adgang til personoplysninger gennem overvågningssystemer som Upstream og Prism på baggrund af EO 12333 og FISA 702.[137]

EUD udledte ydermere i Schrems II, at tilstrækkelighedsafgørelsen vedrørende Privacy Shield fandtes at være tvivlsom, eftersom USA's lovgivning skabte en usikkerhed i forhold til det tilstrækkelige databeskyttelsesniveau, som sikres gennem GDPR artikel 45 og EUC artikel 7, 8 og 47. Denne tvivl var begrundet i, at de tilladte indgreb i de registreredes rettigheder ikke var begrænset, og at de registrerede ikke var sikret en effektiv domstolsbeskyttelse i denne sammenhæng. Dertil vurderede EUD, at indførelsen af ombudsmandsmekanismen gennem stiftelsen af Privacy Shield ikke kunne anses som en udbedrende foranstaltning i forbindelse med de tidligere nævnte problematikker. Denne vurdering skyldtes, at Ombudsmanden ikke kunne agere som en uafhængig domstol.[138]

EUD præciserede yderligere, at de omtalte indgreb, som involverede anvendelse eller opbevaring af de registreredes personoplysninger, tilsidesatte rettighederne i EUC artikel 7 og 8. Dette var begrundet i, at artikel 7 og 8 henholdsvis beskytter retten til privatliv og kommunikation samt retten til databeskyttelse vedrørende egne personoplysninger. I denne forbindelse var der tale om registrerede, som enten var identificerede eller identificerbare på baggrund af personoplysningerne, samt behandling af disse oplysninger gennem de pågældende indgreb.[139] EUD fastslog hertil med henvisning til EUC artikel 52, at begrænsninger af rettigheder og friheder skal have hjemmel i lov, samt at sådanne indgreb skal være nødvendige og stå i rimeligt forhold til det tilsigtede mål i overensstemmelse med proportionalitetsprincippet.[140] Derudover skal tredjelandes lovgivning præcist og klart definere anvendelsen, omfanget, omstændighederne samt betingelserne for udførelse af foranstaltninger, som indebærer rækkevidden for begrænsninger af rettigheder og friheder. Dette omfattede en definition af mindstekrav, således at de registrerede var sikret visse garantier ved

[136] Schrems II, præmis 164
[137] Ibid., præmis 165
[138] Ibid., præmis 168
[139] Ibid., præmis 170
[140] Ibid., præmis 174

potentiel misbrug af deres personoplysninger.[141] EUK skulle i denne sammenhæng medtage disse forhold i sin vurdering ved tilstrækkelighedsafgørelser, eftersom der skulle sikres en effektiv retshåndhævelse såvel som en beskyttelse af rettigheder.[142]

EUD tog herefter stilling til de overvågningssystemer, som anvendes i USA gennem amerikansk lovgivning. EUD vurderede, at FISA 702 ikke fastlægger tilstrækkelige begrænsninger og garantier for efterretningstjenesternes adgang til overførte personoplysninger vedrørende *non-U.S persons*. Hertil vurderede EUD, at der gennem bestemmelser ikke kunne sikres et tilstrækkeligt databeskyttelsesniveau, eftersom de omtalte krav i præmis 175-176 ikke var tilstedeværende.[143] Endvidere gav PPD-28 ikke de registrerede mulighed for retshåndhævelse ved amerikanske domstole, hvilket tilsidesatte kravene i GDPR artikel 45, stk. 2, litra a, og dermed ikke sikrede et tilstrækkeligt databeskyttelsesniveau.[144] PPD-28 muliggjorde desuden gennem EO 12333, at der kunne foretages masseindsamling af personoplysninger, hvilket hverken opfyldte proportionalitetsprincippet eller kravet om streng nødvendighed, og samtidig kunne det forekomme uden retligt tilsyn. Der var således efter EUD's vurdering ikke sikret et tilstrækkeligt databeskyttelsesniveau gennem EO 12333 eller PPD-28.[145] Endvidere anså EUD fraværet af effektive retsmidler ved domstolene under tredjelandets lovgivning som en tilsidesættelse af kravene i EUC artikel 47, uagtet indførelsen af Ombudsmanden.[146] EUD vurderede desuden, at der kunne rejses tvivl om Ombudsmandens uafhængighed, eftersom stillingen var tilknyttet det amerikanske udenrigsministerium.[147] Herudover fandtes der intet belæg for, at Ombudsmanden kunne afsige bindende afgørelser over for efterretningstjenesterne ved manglende efterlevelse af krav.[148]

På baggrund af ovenstående betragtninger blev Privacy Shield-ordningen i sin helhed erklæret for ugyldig af EUD, eftersom artikel 1 i tilstrækkelighedsafgørelsen blev vurderet til at have tilsidesat GDPR artikel 45, stk. 1, sammenholdt med EUC artikel 7, 8 og 47.[149]

[141] Schrems II, præmis 175-176
[142] Ibid., præmis 177
[143] Ibid., præmis 178-180
[144] Ibid., præmis 181
[145] Ibid., præmis 182-184 og 192
[146] Ibid., præmis 186-187 og 190
[147] Ibid., præmis 195
[148] Ibid., præmis 196
[149] Ibid., præmis 198-201

7.8 Data Privacy Framework

EUK vedtog den 10. juli 2023 tilstrækkelighedsafgørelse 2023/1795, som etablerede den tredje certificeringsordning mellem EU og USA.[150] DPF skulle ligesom sin forgænger adressere de aktuelle problematikker, som medførte ugyldighed ved den tidligere ordning. Den nye dataoverførselsaftale mellem USA og EU blev etableret gennem EO 14086, som har til formål at styrke databeskyttelsen for EU-/EØS-borgere gennem inkorporering af principperne om nødvendighed og proportionalitet samt stiftelse af en klageinstans og et tilsynsorgan. DPF udgør den nuværende gældende ordning for overførsel af personoplysninger mellem EU og USA.[151] [152]

[150] www.eur-lex.europa.eu/gennemførelsesafgørelse-2023/1795
[151] Udsen, *Databeskyttelsesret*, s. 346-347
[152] www.dataprivacyframework.gov/Program-Overview

8 Executive Order 14086

På baggrund af ovenstående underskrev og indførte Joe Biden i 2022 dekretet, EO 14086, som skulle være det bærende fundament til en imødekommelse af EU's krav om effektive retsmidler, uafhængige klagemyndigheder og beskyttelse af personoplysninger, jf. kapitel 7.8. I det følgende afsnit vil dekretet indholdsmæssigt blive uddybet og analyseret med henblik på at skabe en forståelse af nødvendigheds- og proportionalitetsprincippernes samt begrænsningerne og garantierne, herunder organerne PCLOB, CLPO og DPRC. Dette udføres for at skabe en baggrundsforståelse for vurderingen af overensstemmelse, som finder sted i kapitel 9.

8.1 Generelt om indholdet i Executive Order 14086

På samme måde som EO 12333 er EO 14086 et dekret, som er udstedt af den amerikanske præsident, hvorfor dekretet har et svagere lovgivningsmæssigt retsgrundlag end eksempelvis FISA, eftersom det ikke er vedtaget som lov gennem Kongressen. Dekreter kan tillige ophæves eller ændres af amerikanske præsidenter uden involvering af Kongressen.[153] Selvom EO 12333 og FISA 702 tildeler de amerikanske efterretningstjenester vidtrækkende beføjelser med ganske få begrænsninger, er disse rammer for dataindsamling nu underlagt begrænsninger gennem EO 14086. EO 14086 er en af byggestenene i DPF, og dens formål er at styrke *non-U.S persons*' sikkerhed og beskyttelse.[154] Endvidere medfører dette dekret yderligere indskrænkninger af signalefterretningsaktiviteter, eftersom der indføres passende sikkerhedsforanstaltninger, som skal beskytte *non-U.S persons'* privatliv, grundlæggende rettigheder og friheder. For at beskytte de grundlæggende rettigheder i forbindelse med efterretningsaktiviteter foretaget i USA, skal der indføres en række sikkerhedsforanstaltninger.[155] Disse foranstaltninger beror på, at signalefterretning alene må udføres på baggrund af en forudgående afgørelse. Afgørelsen skal baseres på en række elementer, som bidrager til vurderingen af, om efterretningsaktiviteten er nødvendig for at fremme en valideret efterretningsprioritet, og denne må alene gennemføres, såfremt den står i rimeligt forhold til efterretningsprioriteten.[156]

Det væsentligste er, at efterretningstjenester ikke må indsamle personoplysninger gennem signalefterretningsaktiviteter, medmindre indsamlingen er relevant. Efterretningsindsamlingen skal

[153] www.americanbar.org/what-is-an-executive-order
[154] Mildebrath, *Reaching the EU-US Data Privacy Framework: First reactions to Executive Order 14086*, s. 1
[155] www.govinfo.gov/executive-order-14086
[156] Ibid.

være så målrettet som muligt for at understøtte den validerede prioritet, og der skal desuden tages hensyn til privatlivets fred og de grundlæggende rettigheder i EUC.[157] For at en indsamling kan anses for at være i overensstemmelse med en valideret efterretningsprioritet, skal flere relevante faktorer vurderes. Dette er begrundet i, at fraværet heraf kan medføre ugyldighed, særligt hvis indsamlingen har en uforholdsmæssig indvirkning på privatlivets fred eller de grundlæggende rettigheder. Sådanne faktorer kan være indsamlingens indgribende karakter, oplysningernes følsomhed samt potentielle konsekvenser for den registrerede. Afgørelsen skal træffes af et udvalg bestående af ledere af efterretningstjenesterne, chefer for ministerierne eller disses repræsentanter. Udvalget skal tage stilling til de relevante faktorer, som kan påvirke privatlivets fred eller de grundlæggende rettigheder, og yderligere stilles der krav om tilegnelsen af kilder og oplysninger. Der tages udgangspunkt i tilgængeligheden, gennemførligheden og hensigtsmæssigheden af mindre indgribende metoder til indsamling eller tilegnelse af personoplysninger.[158] Ovenstående beror på principperne om nødvendighed og proportionalitet, som er fastlagt i EO 14086.[159]

De legitime mål i henhold til anvendelse af signalefterretningsaktiviteter findes i Section (2)(b)(i)(a), og denne liste skal autoriseres af den amerikanske præsident, såfremt der sker ændringer. Direktøren for National Intelligence udarbejder de validerede efterretningsprioriteter for det amerikanske efterretningsfællesskab, med henblik på at sikre en rettidig og effektiv indsamling af oplysninger gennem signalefterretningsaktiviteter. Efterretningsprioriteterne skal dokumenteres i National Intelligence Priorities Framework, som er et klassificeret nationalt efterretningsdokument, som løbende revideres og fremlægges for præsidenten.[160] Før de validerede efterretningsprioriteter dokumenteres og fremlægges for præsidenten, skal de præsenteres for CLPO for at sikre, at de er i overensstemmelse med principperne i Section (2)(a)(ii)(A) og (B), og at de legitime mål er opfyldt.[161] [162] I tilfælde af uoverensstemmelser mellem CLPO's vurdering og direktørens vurdering forelægges dette for præsidenten i forbindelse med udarbejdelsen af dokumentationen under National Intelligence Priorities Framework.[163] I medfør af Section (2)(b)(i)(B) har præsidenten mulighed for at opdatere listen over legitime formål i Section (2)(b)(i)(A), såfremt dette skyldes nye eller øgede trusler mod den nationale sikkerhed.[164]

[157] www.govinfo.gov/executive-order-14086, section 2(c)(i)(B)
[158] Ibid., section 2(c)(i)(A)
[159] Ibid, section 2(a)(ii)(A) og (B)
[160] www.dni.gov/National-Intelligence-Priorities-Framework
[161] Ibid.
[162] www.govinfo.gov/executive-order-14086, section 2(b)(iii)(A)
[163] Ibid., section 2(b)(iii)(B)
[164] Ibid., section 2(b)(i)(B)

Der skelnes mellem indsamling af udvalgte data og masseindsamling af data. Ifølge EO 14086 Section (2)(c)(iii)(A), skal indsamling af udvalgte data prioriteres, eftersom denne form for indsamling er mindre indgribende og medfører mindre dataopbevaring. Masseindsamling må derimod kun benyttes på baggrund af en konkret vurdering foretaget af efterretningsfælleskabets ledere. Vurderingen skal foretages på baggrund af nødvendighedsprincippet, hvorfor der skal fremlægges saglige og juridiske argumenter, som tydeliggør, om signalefterretningsaktiviteten er nødvendig og står i rimeligt forhold til proportionalitetsprincippet. Såfremt masseindsamling godkendes, skal der desuden implementeres tekniske foranstaltninger og metoder, som sikrer, at der udelukkende indsamles oplysninger, som er strengt nødvendigt for det pågældende formål. Dette bidrager samtidig til at minimere omfanget af dataopbevaring i overensstemmelse med princippet om dataminimering i GDPR artikel 5, stk. 1, litra c. Masseindsamling skal være samhørigt til et af de formål, som er nævnt i Section (2)(c)(ii)(B), som vedrører beskyttelsen af national sikkerhed. Denne liste er udtømmende, men kan ændres af USA's præsident, såfremt nye nationale trusler opstår. Efterretningstjenester, som indsamler data, hvad enten dette sker gennem masseindsamling eller målrettet indsamling, skal indføre politikker og procedurer, som minimerer udbredelsen og opbevaringen af data.[165] For at beskytte de registrerede er det kun lovligt at videregive data indsamlet gennem signalefterretningsaktiviteter, såfremt modtageren er autoriseret og har den fornødne erfaring med behandlingssikkerhed.[166] Videregivelsen skal ydermere bero på en konkret vurdering af formålet, omfanget og de potentielle skader, som videregivelsen kan forvolde de registrerede.[167]

8.2 Proportionalitets- og nødvendighedsprincipperne

For at de amerikanske efterretningstjenester kan udføre signalefterretningsaktiviteter skal principperne om proportionalitet og nødvendighed være opfyldt. Principperne, der blev indført med EO 14086, har traditionelt ikke haft en tæt tilknytning til amerikansk databeskyttelsesret, hvorfor principperne vil blive fortolket på baggrund af anden amerikansk lovgivning. Nærværende afsnit vil således undersøge og skabe en forståelse af principperne. Dette udføres for at vurdere, om der findes en overensstemmelse mellem den EU-retlige og den amerikanske fortolkning af principperne i kapitel 9.1.1.

[165] www.govinfo.gov/executive-order-14086, section 2(c)(iii)(A)
[166] Ibid., section 2(c)(iii)(A)(1)(c)
[167] Ibid., section 2(c)(iii)(A)(1)(d)

Proportionalitets- og nødvendighedsprincipperne findes i EUC såvel som i EO 14086. Disse to principper skal fortolkes efter henholdsvis love, retspraksis og retsgrundsætninger i henholdsvis EU og USA. I EU-retten betragtes proportionalitets- og nødvendighedsprincipperne som samhørige, hvilket kommer til udtryk ved, at princippet om proportionalitet udelukkende anses for opfyldt, såfremt en begrænsning af friheder eller rettigheder er nødvendig. I EUC artikel 52, stk. 1, findes der ingen yderligere definition af begrebet nødvendighed, hvorfor en fortolkning af dette begreb må findes andetsteds i EU-lovgivningen. EMRK artikel 8, stk. 2, har følgende ordlyd: "*Ingen offentlig myndighed kan gøre indgreb i udøvelsen af denne ret, undtagen for så vidt det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres ret og frihed.*".[168] Denne formulering bidrager til, hvornår en begrænsning af rettigheder og friheder er mulig. Formuleringen bidrager imidlertid ikke konkret til, hvornår de ovennævnte omstændigheder er legitime. EMD fastlagde i sagen Dudgeon v. The United Kingdom, at nødvendighedsprincippet ikke skal forstås som værende "nyttig", "rimelig" eller "ønskeligt", men kræver derimod et overhængende samfundsmæssigt behov, jf. præmis 51 og 52 i sagen.[169] Dette behov skal bero på et skøn, som fastsættes af de nationale myndigheder, og i skønnet skal de registreredes grundlæggende rettigheder og friheder tillægges betydelig vægt. Myndighedernes skøn er ikke bindende og er dermed stadig underlagt domstolsprøvelse. Det overhængende samfundsmæssige behov, som de nationale myndigheder skal påvise, skal endvidere være proportionelt med indgrebet i de berørte friheder og rettigheder, jf. EMD-sagen Piechowicz v. Poland, præmis 212.[170] Når der foretages et indgreb i de grundlæggende rettigheder eller privatlivets fred med henblik på beskyttelse af den nationale sikkerhed, skal indgrebet begrænses til det strengt nødvendige, jf. kapitel 7.7.[171] Ifølge EMD-sagen Szabó And Vissy v. Hungary beror princippet om streng nødvendighed på, at anvendelsen af overvågningsteknologier i en efterforskning skal være strengt nødvendig for beskyttelsen af de demokratiske institutioner. Desuden kræves det, at efterforskningen er strengt nødvendig for at opnå det legitime mål.[172]

[168] www.retsinformation.dk/Lov-om-Den-Europæiske-Menneskerettighedskonvention, artikel 8, stk. 2
[169] www.hudoc.echr/DUDGEON-v.-THE-UNITED-KINGDOM, præmis 51-52
[170] www.hudoc.echr/PIECHOWICZ-v.-POLAND
[171] Schrems II, præmis 167
[172] www.hudoc.echr/SZABÓ-AND-VISSY-v.-HUNGARY, betragtning 73

Selvom det ikke fremgår af EMRK artikel 8, stk. 2, at der skal indføres passende foranstaltninger, må data indsamlet i medfør af national lovgivning ikke blive genstand for misbrug.[173] Ligesom inden for EU-retten har principperne om proportionalitet og nødvendighed været anvendt i amerikansk lovgivning og er blevet videreudviklet gennem retspraksis. USA og EU's udvikling af disse principper har bevæget sig i forskellige retninger, hvilket har bragt udfordringer ved udformningen af EO 14086, eftersom principperne i amerikansk ret skal anvendes på en måde, som harmoniserer med EU-retten.[174] En af udfordringerne har været fortolkningen af disse begreber. DCRP, som uddybes i kapitel 8.4, er eksplicit underlagt kravet om, at fortolkningen skal ske i overensstemmelse med ordlyden af EO 14086, suppleret af relevant amerikansk lovgivning og retspraksis.[175] Som tidligere nævnt findes der en samhørighed mellem principperne i den EU-retlige fortolkning. I modsætning hertil er EO 14086 konciperet ud fra en forståelse af, at principperne betragtes individuelt.[176] Ifølge EO 14086 er princippet om nødvendighed opfyldt, såfremt der ikke findes tilgængelige, gennemførlige eller hensigtsmæssige alternativer til at indsamle oplysninger, der er nødvendige for at gennemføre en valideret efterretningsprioritet.[177] Efter Section 2(a)(ii)(A) skal signalefterretningsaktiviteter bero på en vurdering af konkrete faktorer.[178] Endvidere kræves det ifølge Section 2(c)(iii)(E), at det skal dokumenteres, at der foreligger et samfundsmæssigt behov i form af national sikkerhed, ligesom princippet om nødvendighed kræver det i henhold til EU-retten.[179]

Ifølge EO 14086 Section 2(a)(ii)(B) defineres proportionalitet som følgende: "*Signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.*". Selvom proportionalitetsprincippet ikke er defineret i amerikansk overvågningslovgivning, er begrebet hyppigt anvendt i anden amerikansk lovgivning. Selv om begreberne ifølge EO 14086 skal forstås individuelt, betragtes de i amerikansk retstradition som samhørige og overlappende i retspraksis. Det er særligt væsentligt at forstå, at nødvendighedsprincippet indebærer, at det mindst

[173] www.echr.coe.int/echr/factsheet-mass-surveillance, s. 3
[174] Mildebrath, *Reaching the EU-US Data Privacy Framework: First reactions to Executive Order 14086*, s. 7
[175] www.govinfo.gov/rules-and-regulations-62303, s. 2
[176] www.digitalcommons.wcl.american.edu/Necessity-Proportionality-and-Executive-Order-14086, s. 13
[177] www.govinfo.gov/executive-order-14086, section 2(c)(i)
[178] Ibid., section 2(a)(ii)(A)
[179] Ibid., section 2(c)(iii)(E)

indgribende middel skal anvendes, mens proportionalitetsprincippet forpligter til en vurdering af, om indgrebet står i rimeligt forhold til det legitime formål.[180]

Proportionalitetsprincippet i EO 14086 er tæt relaterbart til begrebet *strict scrutiny*, som er gennemgående i amerikansk retspraksis. *Strict scrutiny*-testen anvendes til at vurdere, om statslige indgreb krænker visse grundlæggende rettigheder og friheder. Dertil indebærer det, at staten bærer bevisbyrden for, at indgrebet er nødvendigt og præcist tilpasset for at forfølge en legitim statslig interesse.[181] *Strict scrutiny* kan på visse områder omfatte en strengere proportionalitetsvurdering end den, som anvendes i EU-retten.[182] Selvom *strict scrutiny* ikke er nævnt direkte i EO 14086, har det stadig indflydelse på fortolkningen af proportionalitetsprincippet, eftersom principperne skal fortolkes i overensstemmelse med national retspraksis og lovgivning. Selvom *strict scrutiny* kan fungere som en rettesnor for domstolene i afgørelser, der tager afsæt i EO 14086, er det ikke ensbetydende med, at testen skal benyttes direkte. Dette er begrundet i, at proportionalitets- og nødvendighedsprincipperne i EO 14086 ikke er fuldt ud samhørigt med *strict scrutiny*. Afvejningen mellem opnåelsen af et legitimt formål og de deraf følgende indgreb udgør et centralt element i amerikansk lovgivning. Det tilkommer således de amerikanske domstole at fastlægge, hvornår en begrænsning kan anses for at være rimeligt i forhold til hensynet til det legitime formål.[183]

I medfør af ovenstående afsnit kan der udelukkende foretages indgreb i retten til privatliv, såfremt betingelserne i EMRK artikel 8, stk. 2, er opfyldt. Betingelserne indeholder krav om, at indgrebet skal være nødvendigt af hensyn til den nationale sikkerhed. National sikkerhed er ikke defineret i anden lovgivning, hvilket rejser fortolkningsmæssige spørgsmål. EMRK har imidlertid fastslået, at indgreb i frihedsrettigheder i relation til hensynet til national sikkerhed forudsætter en vis grad af forudsigelighed.[184] Forudsigeligheden beror imidlertid ikke på, om det enkelte individ kan forudsige, hvornår der vil foretages indgreb i vedkommendes rettigheder, herunder aflytning af kommunikation. Individet bør eller kan derfor ikke vide, hvornår vedkommende vil blive aflyttet. Kravet om forudsigelighed kræver dog, at ordlyden af lovtekster, der hjemler beføjelser til at foretage indgreb i frihedsrettigheder, er formuleret klart og præcist i sine bestemmelser, således at individet har en tilstrækkelig indikation af, hvornår sådanne indgreb kan foretages.[185] Kommunikation samt trusler

[180] Harmon, *When is Police Violence Justified?*, s. 60
[181] www.digitalcommons.wcl.american.edu/Necessity-Proportionality-and-Executive-Order-14086, s. 14
[182] Ibid., s. 14
[183] Ibid., s. 15
[184] www.hudoc.echr/SZABÓ-AND-VISSY-v.-HUNGARY, betragtning 62
[185] Ibid.

for national sikkerhed ændrer og udvikler sig løbende, hvorfor en afgrænsning til en forhåndsgodkendt liste med legitime formål vil være uhensigtsmæssigt ved forståelsen af national sikkerhed. Den dynamiske fortolkning af begrebet national sikkerhed styrker håndteringen af nye potentielle trusler, eftersom nationale myndigheder har større råderum for bekæmpelse af trusler mod national sikkerhed.[186]

I EMD-sagen Centrum För Rättavisa v. Sweden bliver det fastslået, at nuværende trusler også omfatter global narkotikahandel, terrorisme, menneskehandel og seksuel udnyttelse af børn.[187] Listen for EU er ikke udtømmende, hvilket understøtter den dynamiske fortolkning, som både ses i retspraksis samt lovgivning.

Den amerikanske fortolkning af begrebet national sikkerhed fremgår af den udtømmende liste i EO 14086 Section (2)(b)(i)(A). Som tidligere nævnt har den amerikanske præsident mulighed for at opdatere listen over legitime forhold, såfremt disse udgør nationale sikkerhedsmæssige imperativer. Såfremt USA's præsident foretager ændringer i listen, skal der imidlertid stadig gennemføres en selvstændig vurdering af, om proportionalitets- og nødvendighedsprincipperne er overholdt. Før præsidenten kan autorisere en opdatering af listen, skal to betingelser være opfyldt. For det første skal der foreligge *new national security imperatives*, og for det andet skal det legitime formål have en tilknytning til national sikkerhed. *National security imperatives* indebærer, at der skal foreligge en overhængende fare mod national sikkerhed. Enhver ændring skal desuden offentliggøres, medmindre offentliggørelsen vurderes at være til fare for den nationale sikkerhed. Nye ændringer eller tilføjelser må desuden ikke være i strid med forbuddene fastsat i EO 14086, Section (2)(b)(ii)(A).[188]

8.3 PCLOB

For at privatlivs- og de borgerlige rettigheder kunne opretholdes under en vedvarende skiftende regering, besluttede Kongressen, at der skulle indsættes et uafhængigt agentur inden for den udøvende magt.[189] PCLOB har til opgave at sikre kontrol og balance i forhold til opretholdelsen af de grundlæggende rettigheder, som er gældende i USA. PCLOB's væsentligste opgaver består i at føre tilsyn og rådgive. De skal føre tilsyn med, at regler, politikker og procedurer ikke tilsidesætter de

[186] www.menneskeret.dk/faktaark-reform-af-den-europæiske-menneskerettighedskonvention
[187] www.hudoc.echr/CENTRUM-FÖR-RÄTTVISA-v.-SWEDEN
[188] www.govinfo.gov/executive-order-14086, section (2)(b)(ii)(A)
[189] www.pclob.gov/about/history-and-mission

grundlæggende privatlivs- og frihedsrettigheder, når sådanne foranstaltninger iværksættes af hensyn til national sikkerhed og terrorbekæmpelse. Dette sker ved løbende gennemgange, undersøgelser og vurderinger, som beror på PCLOB's bemyndigelse til at føre tilsyn med den udøvende magts implementering af nye retsakter og procedurer. Bestyrelsen skal sikre, at der ikke sker brud på de grundlæggende privatlivs- og frihedsrettigheder, hvorfor de skal sørge for, at ny lovgivning ikke strider mod allerede gældende regler, som beskytter borgernes rettigheder. PCLOB er desuden bemyndiget til at udøve rådgivning vedrørende foreslået lovgivning, regulativer eller politikker, hvis disse har relevans for national sikkerhed. Den rådgivning, som ydes til præsidenten eller andre forvaltningsorganer, skal have en forebyggende karakter og sikre, at hverken fremtidige eller nuværende tiltag krænker borgernes rettigheder.[190]

Bestyrelsens beføjelser beror på tilsyn og kontrol af agenturer i USA, hvorfor deres egentlige beføjelse er at få adgang til information. Indhentelse af information omfatter adgang til relevant materiale fra afdelinger eller agenturer under den udøvende magt. Dertil muligheden for at anmode om oplysninger fra enhver stat samt at indkalde vidner gennem stævning af enhver person under den udøvende magt. Stævningen kan foretages ved flertal, og såfremt bestyrelsen beslutter at anmode om en stævning, indsendes anmodningen til justitsministeren, som herefter kan vælge henholdsvis at imødekomme eller afvise den.[191]

I henhold til bekendtgørelse 13636 om forbedring af Critical Infrastructure Cybersecurity skal nationale agenturer udarbejde Cybersecurity Frameworks med det formål at minimere risikoen for cyberangreb.[192] Department of Homeland Security skal i samarbejde med PCLOB udarbejde en rapport med anbefalinger til, hvordan risici forbundet med privatlivs- og frihedsrettigheder kan afblødes i forbindelse med udarbejdelsen af sådanne frameworks. Ifølge EO 14086 er bestyrelsen bemyndiget til at gennemgå implementeringen af nye politikker og procedurer for at sikre, at de relevante sikkerhedsforanstaltninger benyttes i signalefterretningsaktiviteter, således borgernes privatlivs- og frihedsrettigheder opretholdes. Derudover skal PCLOB gennemføre en årlig revision af klageprocessen ved DPRC og bistå i udvælgelsen af dommere til DPRC, hvilket vil gennemgås nærmere nedenfor.[193]

[190] www.pclob.gov/about/history-and-mission
[191] Stanley, *What Powers Does the Civil Liberties Oversight Board Have?*
[192] www.pclob.gov/about/history-and-mission
[193] Ibid.

Bestyrelsens rådgivning baseres på en flertalsbeslutning, hvor flertallets holdning er afgørende for, om der skal afgives rådgivning om ny lovgivning, procedurer eller retningslinjer inden for de pågældende agenturer. Bestyrelsesmedlemmerne kan også yde individuel rådgivning, men en sådan rådgivning skal ikke opfattes som en fælles beslutning fra bestyrelsen, hvorfor dette skal tydeliggøres over for modtageren.[194] [195] Bestyrelsen har mulighed for at ændre sine processuelle retningslinjer, hvilket muliggør ændringer af ovenstående.[196] Bestyrelsen har imidlertid ikke beføjelse til at udfordre agenturernes hemmeligholdelsesbeføjelser, herunder skjulte handlinger, selv i tilfælde hvor der er konstateret misbrug for at dække over forseelser eller inkompetence. Endvidere har bestyrelsen ikke en udvidet adgang til retshåndhævelse ud over den almene ret til at anlægge en sag. De kan dermed ikke pålægge et agentur at ændre praksis, selv hvis denne vurderes at være i strid med privatlivs- eller frihedsrettighederne.[197]

8.4 CLPO og DPRC

I henhold til afsnit tre i EO 14086 er der indført en ny todelt klageproces, som giver personer uden for USA mulighed for at indgive klager til en uafhængig domstol. Rammen for denne todelte klageadgang er dannet på baggrund af ugyldiggørelsen af Privacy Shield, og har ydermere til formål at fremme transatlantiske datastrømme.[198] Processen beror på, at en klager indgiver en klage til de kompetente nationale myndigheder i sit hjemland, som herefter videresender klagen til CLPO, såfremt klageren påstår, at de amerikanske efterretningstjenester gennem signalefterforskning har krænket vedkommendes privatliv.[199]

CLPO er forpligtet til at gennemgå, undersøge og modtage klager, såfremt klagen vurderes at være kvalificeret. En klage anses for kvalificeret, når klageren påstår at have været genstand for signalefterretningsaktiviteter, og når personoplysninger er involveret. Ydermere forudsættes det, at CLPO modtager visse grundlæggende oplysninger i forbindelse med klagens indgivelse. Oplysninger vedrørende en konkret overvågning eller misbrug er imidlertid ikke nødvendige ved klagens indgivelse. CLPO og DPRC har fuld bemyndigelse til at få adgang til nationale fortrolige dokumenter, hvorfor de er forpligtet til at indhente og undersøge de nødvendige oplysninger, som kan danne

[194] www.documents.pclob.gov/Advisory-Function-Policy-and-Procedurer, s. 1
[195] Ibid., s. 2
[196] Ibid., s. 4
[197] Stanley, *What Powers Does the Civil Liberties Oversight Board Have?*
[198] www.govinfo.gov/rules-and-regulations-62303
[199] Mantel, *The Civil Liberties Protection Officers: The Gateway to Redress*

grundlag for en afgørelse om, hvorvidt overvågning er sket i strid med EO 14086. CLPO har bemyndigelse til at afsige bindende afgørelser, som omfatter vejledninger og ændringer af praksis. Det væsentlige i denne bemyndigelse er at afgøre, om der er sket en overtrædelse af amerikansk lovgivning.[200] Alle klager behandlet af CLPO skal dokumenteres og opbevares med henblik på en potentiel fremtidig revision foretaget af DPRC. Endvidere har klageren ret til at få sagen revideret af DPRC, såfremt vedkommende er uenig i CLPO's afgørelse.[201] [202]

DPRC blev dannet i henhold til EO 14086, hvor justitsministeren var pålagt at etablere en domstol udelukkende med kompetence inden for databeskyttelse. Organets rolle er afhængig af CLPO, eftersom DPRC foretager revision af CLPO's afgørelser. Revisionen kan iværksættes enten på baggrund af en anmodning fra efterretningsagenturet eller fra klageren. DPRC har kompetence til at træffe bindende afgørelser om passende afhjælpende foranstaltninger, såfremt det konstateres, at signalefterretningsaktiviteter ikke er i overensstemmelse med amerikansk lovgivning.[203] [204]

Dommerne i DPRC udvælges af justitsministeren, som rådfører sig med PCLOB og Secretary of Commerce. Der skal udpeges minimum seks dommere til at varetage DPRC's opgaverne, og udvælgelsen sker på baggrund af dommernes juridiske foretagender, faglige erfaring inden for databeskyttelse samt de kriterier, som den udøvende magt benytter ved udvælgelsen af kandidater til det amerikanske retsvæsen.[205] For at sikre domstolens upartiskhed og uafhængighed må dommerne ikke have en forbindelse til regeringen eller være underlagt tjenestepligt over for denne, og de må heller ikke være underlagt dagligt tilsyn af justitsministeren. Derudover fremgår det ikke af dekretet, at dommerne har en indberetningspligt over for justitsministeren.[206] [207] [208] Justitsministeren må ydermere ikke have indflydelse på afgørelser, som DPRC træffer på baggrund af en tidligere kendelse fra CLPO. Dommerne i DPRC er tildelt beføjelser i medfør af en omfattende beskyttelse, der skal sikre dem mod uberettiget afskedigelse og negative handlinger i forbindelse med varetagelsen af deres tjeneste.[209]

[200] www.govinfo.gov/rules-and-regulations-62303
[201] Mantel, *The Civil Liberties Protection Officers: The Gateway to Redress*[/]
[202] Joel, *Protecting Privacy and Promoting Transparency: The Perspective of a Civil Liberties Protection Officer*
[203] www.govinfo.gov/rules-and-regulations-62303, s. 2
[204] www.govinfo.gov/executive-order-14086, section 3(d)(ii)
[205] www.govinfo.gov/rules-and-regulations-62303, s. 3
[206] www.govinfo.gov/executive-order-14086, section 3(d)(i)(a)
[207] www.govinfo.gov/rules-and-regulations-62303, s. 2
[208] www.govinfo.gov/executive-order-14086, section 3(d)(iv)
[209] www.govinfo.gov/rules-and-regulations-62303, s. 2

Ansøgninger om revidering af en afgørelse fra CLPO vil altid blive behandlet af et panel bestående af tre dommere. Ydermere vil denne revidering bistås af en særlig advokat, hvis opgave er at varetage klagerens interesse. Den særlige advokat har ikke direkte kontakt med klageren, men skal i stedet bero biståelsen på generelle betragtninger, som afspejler klagerens perspektiv. Udvælgelsen af den særlige advokat skal foretages af justitsministeren i samråd med PCLOB og skal ske på baggrund af advokatens juridiske kvalifikationer samt vedkommendes omdømme i advokatsamfundet.[210]

DPRC gennemgår den afgørelse, som er truffet af CLPO, og træffer beslutning om, hvorvidt afgørelsen er saglig og juridisk begrundet i gældende lovgivning. DPRC's afgørelse beror på en fortolkning af EO 14086 i overensstemmelse med amerikansk lovgivning og juridiske retsgrundsætninger, herunder relevante højesteretsafgørelser. Efter klagens behandling modtager klageren ikke en bekræftelse på, om vedkommende har været genstand for signalefterretningsaktiviteter. I stedet udsendes et standardsvar, som enten giver klager medhold eller konstaterer, at DPRC ikke har fundet nogen overtrædelser af amerikansk lovgivning.[211]

[210] www.govinfo.gov/rules-and-regulations-62303, s. 3
[211] Ibid., s. 2

9 Overensstemmelse med USA og EU

Følgende kapitel vil undersøge, om der findes en overensstemmelse mellem de centrale artikler i EUC, henholdsvis artikel 7, 8, 47 og 52, EO 14086 og amerikansk praksis. De centrale spørgsmål er, om USA gennem EO 14086 sikrer en databeskyttelse, som er tilstrækkelig ækvivalent med den, som de EU-borgere garanteres i EU, og om USA's lovgivning, praksis og DPF dermed er i overensstemmelse med de grundlæggende rettigheder og friheder i EUC.

Eftersom EUD allerede tog stilling til de amerikanske overvågningslove, herunder FISA 702 og EO 12333, i Schrems II, vil følgende kapitel have fokus på EO 14086, som er fundamentet for DPF. FISA 702 og EO 12333 fungerer imidlertid stadig som selvstændige retsgrundlag for de amerikanske efterretningstjenesters overvågningsaktiviteter, mens EO 14086 fungerer som en supplerende garantiordning.[212]

9.1 Executive Order 14086

EUD vil sandsynligvis gentage flere af de samme kritikpunkter af FISA 702 og EO 12333 i en potentiel Schrems III-afgørelse, hvorfor hovedfokus i dette kapitel vil være på EO 14086. USA forsøger gennem EO 14086 at forbedre de garantier og mekanismer, som var utilstrækkelige ifølge EUD i Schrems II, herunder indførelse af nødvendigheds- og proportionalitetsprincipperne og etablering af en ny klagemekanisme. Den 9. oktober 2024 offentliggjorde EUK sin første regelmæssige revision af funktionaliteten af DPF.[213] EUK's generelle holdning til DPF var, at " *(...) de amerikanske myndigheder har indført de nødvendige strukturer og procedurer for at sikre, at databeskyttelsesrammen fungerer effektivt.*". EUK bemærkede imidlertid, at det på daværende tidspunkt var vanskeligt at foretage en fyldestgørende vurdering af begrænsningernes og garantiernes effektivitet i praksis som følge af en begrænset mængde af oplysninger.[214] På trods af at EUK og EDPB overordnet anerkender forbedringer i DPF, herunder DPRC's beføjelser og uafhængighed kontra tidligere mekanismer, er der andre aktører, som ikke er af den samme holdning.[215] NOYB udtaler, at en tilstrækkelig databeskyttelse i USA på baggrund af et dekret medfører et svagt fundament, eftersom dekretet uden videre kan afskaffes af USA's præsident.[216] Den amerikanske

[212] www.edpb.europa.eu//edpb-report-on-first-review-of-dpf, s. 15
[213] www.eur-lex.europa.eu/første-regelmæssige-revision-af-dpf
[214] Ibid., kapitel 3
[215] www.edpb.europa.eu/edpb-udtalelse5/2023-eu-us-dpf, s. 6
[216] www.noyb.eu/en/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal

præsident, Donald Trump, har tidligere udtalt, at der ville ske en gennemgang af eksisterende dekreter, hvilket potentielt kan inkludere EO 14086. En afskaffelse af dette dekret vil fjerne fundamentet for DPF, hvorfor dataoverførselsaftalen med al sandsynlighed vil ugyldiggøres.[217] LIBE er af samme holdning som NOYB og konkluderer, at tilstrækkelighedsresultaterne ikke skaber reel ækvivalens i henhold til EU-borgeres beskyttelsesniveau.[218] LIBE påpeger, at USA, i modsætning til andre sikre tredjelande, ikke har en føderal databeskyttelseslovgivning svarende til GDPR.[219] Dette kan skabe udfordringer i henhold til ensartethed, forudsigelighed og gennemsigtighed for EU-borgere, hvis oplysninger behandles i USA. Endvidere fremhæver LIBE, at de i EO 14086 fastsatte rettigheder og begrænsninger ikke er tilstrækkelig klare, præcise eller forudsigelige i praksis, eftersom EO 14086 til enhver tid kan ændres af den amerikanske præsident uden involvering fra Kongressen.[220] Dette rejser i sig selv spørgsmål om retssikkerheden i henhold til de krav, som følger af GDPR artikel 45, stk. 2, hvorefter eksempelvis retsstatsprincippet, menneskerettighederne og de grundlæggende frihedsrettigheder skal respekteres.[221] Når EO 14086 kan ændres ensidigt af den udøvende magt, må det således anses for usikkert, om forudsigeligheden og retssikkerheden består.

Endvidere kritiseres EO 14086 af LIBE for ikke at forbyde masseindsamling af data ved signalefterretning og for at tillade, at listen over legitime nationale sikkerhedsmål kan udvides af den amerikanske præsident uden forpligtelse til offentliggørelse.[222] Som tidligere nævnt, er det dog kun muligt at tilbageholde offentliggørelsen, hvis denne vurderes at være til fare for en efterforskning, jf. kapitel 8.2. Dette kan give anledning til alvorlige retssikkerhedsmæssige spørgsmål og fremhæver en grundlæggende mangel på gennemsigtighed, som er central for opretholdelsen af EU-borgeres grundlæggende rettigheder.

På den ene side er der et hensyn til national sikkerhed, som kan nødvendiggøre en grad af hemmeligholdelse, og EU-retten anerkender ligeledes, at de grundlæggende rettigheder kan begrænses, såfremt begrænsningen er lovlig, nødvendig og proportionel, jf. EUC artikel 52, stk. 1. På den anden side kræves det, at begrænsninger af de grundlæggende rettigheder, herunder retten til privatliv og beskyttelse af personoplysninger, jf. henholdsvis EUC artikel 7 og 8, skal være klart definerede, forudsigelige og underlagt uafhængigt tilsyn. Der kan således argumenteres for, at

[217] Haslund, *Trump ryster EU-aftale: Cloud-løsninger risikerer at blive ulovlige*
[218] www.europarl.europa.eu/LIBE-udkast-til-forslag-til-beslutning
[219] Ibid., præmis 8
[220] Ibid., præmis 8
[221] GDPR artikel 45
[222] www.europarl.europa.eu/LIBE-udkast-til-forslag-til-beslutning, præmis 3

muligheden for udvidelse af listen uden nogen form for offentliggørelse kan underminere gennemsigtigheden. Dertil kan det underminere EU-borgeres mulighed for at forstå, under hvilke omstændigheder og på hvilke betingelser deres oplysninger kan blive indsamlet og behandlet, jf. Schrems II, præmis 176. Den manglende gennemsigtighed kan risikere at underminere EU-borgeres rettigheder til domstolsprøvelse, som kræves i medfør af EUC artikel 47. Afvejningen mellem national sikkerhed og borgernes grundlæggende rettigheder er således særdeles relevant og udgør en svær balance. USA's behov for at beskytte nationale sikkerhedsmål må anerkendes, men denne beskyttelse må ikke ske på bekostning af EU-borgeres grundlæggende rettigheder.

9.1.1 Proportionalitets- og nødvendighedsprincipperne

Som nævnt ovenfor, skal en begrænsning af rettigheder og friheder være lovlig, proportionel og nødvendig. EDPB anerkender indførelsen af principperne i EO 14086, men det bemærkes, at indførelsen løbende skal vurderes gennem anvendelse i praksis.[223] For at vurdere om begrænsningen er i overensstemmelse med EU-retten, skal principperne i USA underlægges den samme betydning og fortolkning som den, der findes i EU-retten. I nærværende afsnit vil fortolkningen af principperne i henholdsvis EU og USA sammenholdes for at vurdere, om der findes en overensstemmelse, og denne vurdering beror på kapitel 8.2.

På baggrund af kapitel 8.2 om nødvendigheds- og proportionalitetsprincipperne opstår der imidlertid problemer vedrørende princippernes betydning og fortolkning. I EU-retlig forstand anses principperne om nødvendighed og proportionalitet som værende samhørige, eftersom proportionalitetsprincippet udelukkende kan opfyldes, såfremt en begrænsning af rettigheder eller friheder er nødvendig, jf. EUC artikel 52, stk. 1, mens principperne i amerikansk forstand anses som individuelle. Denne forskel kan således give anledning til vedvarende retlige konflikter mellem EU og USA samt kan endvidere danne grundlag for en potentiel Schrems III-sag. Selvom nødvendigheds- og proportionalitetsprincipperne i EO 14086 efter amerikansk praksis og retstradition skal forstås individuelt, kan der stadig drages paralleller mellem EU-retten og amerikansk lovgivning, jf. kapitel 8.2. I EU-retten skal statslige indgreb i frihedsrettighederne, der forfølger et offentligt formål, være snævert tilpasset og må ikke gå længere, end hvad der er nødvendigt. På den anden side vil princippet om nødvendighed, i amerikansk henseende, anses for at afvige den EU-retlige fortolkning og forståelse. Dette er begrundet i, at ordlyden i EO 14086 Section 2(a)(ii)(A) fastslår, at

[223] www.edpb.europa.eu/edpb-udtalelse5/2023-eu-us-dpf, s. 5

signalefterretning ikke nødvendigvis behøver at være det eneste alternativ for at opnå det pågældende mål. Sammenholdt med citatet fra LIBE "*In the US proportionality considerations do not play a decisive role in the determination of restrictions to data protection rights of individuals, thus LE and national security interests typically prevail over the interests of the individual concerned.*" kan det udledes, at frihedsrettighederne for borgere er sekundære efter statslige interesser, såfremt det omhandler national sikkerhed.[224] Dette er ikke foreneligt med EU-rettens forståelse af princippet om nødvendighed, eftersom det fremgår af EMD-sagen Dudgeon v. The United Kingdom, at der skal foreligge et overhængende samfundsmæssigt behov, samt rettighederne og frihederne hos de registrerede skal tildeles betydelig vægt, jf. præmis 51 i sagen og kapitel 8.2. I medfør af EMD-sagen Szabó v. Hungary skal indgrebet være strengt nødvendigt for både den nationale sikkerhed og for at opnå det legitime formål, jf. præmis 73 i sagen og kapitel 8.2. I EO 14086 bliver det ikke præciseret, at nødvendigshedsprincippet skal fortolkes strengt. Efter nærværende afsnit må det konkluderes, at princippet om nødvendighed i amerikansk henseende ikke tildeles den samme fortolkning som i EU-retten. EU's fortolkning må anses for at give en mere omfattende beskyttelse af den registreredes grundlæggende rettigheder og friheder, hvorfor den amerikanske fortolkning ikke tilbyder en tilstrækkelig beskyttelse af disse.

Proportionalitetsprincippet findes ikke reguleret andre steder i den amerikanske databeskyttelseslovgivning, hvorfor fortolkningen heraf må anses for at ligge nært op ad begrebet *strict scrutiny*. Den generelle forståelse af begrebet beror på, at regeringen skal påvise, at den handling eller lovgivning, som skal aktualiseres, er nødvendig eller snævert tilpasset for at fremme en tvingende statslig interesse. *Strict scrutiny* er tilnærmelsesvis foreneligt med samme opfattelse som i EU-retten, jf. kapitel 8.2. Princippet bør derfor anses for at være foreneligt med EU-rettens fortolkning, hvorfor proportionalitetsprincippet ikke synes at have en negativ indvirkning på vurderingen af, om der foreligger en tilstrækkelig databeskyttelse af personoplysninger.

9.1.2 Organerne i Executive Order 14086

I denne del af specialet vil der foretages en vurdering af, hvorvidt organerne, omtalt i EO 14086, gennem deres praksis overholder de garantier og begrænsninger, som er påkrævet. Dette udføres ved at sammenholde relevante udtalelser fra EDPB, EUK, LIBE, NOYB og andre kilder med, hvordan PCLOB, CLPO og DPRC reelt fungerer i praksis. Det konstateres i denne sammenhæng, at EDPB og

[224] www.europarl.europa.eu/a-comparison-between-US-and-EU-data-protection, s. 69

EUK's vurderinger vægtes højere grundet organernes autoritet og beføjelser. Det findes imidlertid relevant at inkorporere andre kilders udtalelser for at danne et overblik over organernes funktionalitet i praksis og dermed danne grundlag for en helhedsvurdering.

PCLOB

I sin udtalelse af den 28. februar 2023 foretog EDPB en vurdering af PCLOB, hvori organet overordnet blev anerkendt. Anerkendelsen var begrundet i, at organet kunne betragtes som behjælpeligt i forhold til vurderingen af overholdelse og implementering af EO 14086 ved dataindsamling gennem FISA 702 og EO 12333 samt tilsynet med DPRC, jf. kapitel 8.3.[225] EDPB nævner imidlertid, at EUK skal være opmærksom på, hvordan PCLOB's anbefalinger gennemføres, samt at PCLOB er begrænset i deres tilsyn, såfremt efterretningstjenester i USA udfører skjulte handlinger, jf. kapitel 8.3.[226] Dertil har PCLOB's tidligere praksis medført, at tilsynsorganet ikke har videregivet yderligere information til EDPB ud over det, som var offentliggjort til den generelle befolkning. EDPB beklagede samtidig PCLOB's manglende opfølgende rapporter vedrørende anvendelsen af PPD-28.[227] Der kan i denne sammenhæng argumenteres for, at PCLOB's manglende mulighed for tilsyn under specifikke omstændigheder samt tidligere praksis medfører usikkerhed vedrørende tilsynsorganets fremtidige udførelse af sine opgaver. Selvom EDPB ikke fremhæver disse bemærkninger som relevante for EUK's fremadrettede vurdering, kan det antages, at de bør tillægges betydning i vurderingen af PCLOB's funktionalitet i praksis. Fremadrettet gennemsigtighed gennem eksempelvis rapportering og omfattende adgang for tilsynsorganet til at udføre sine opgaver, herunder tilsyn med DPRC, vurderes at være af væsentlig betydning, jf. kapitel 8.3.

EDBP anerkendte endvidere PCLOB's uafhængighed samt dets autoritet forhold til efterretningstjenester, navnlig med hensyn til kravet om implementering af tilsynsorganets anbefalinger.[228] EUK konkluderede i deres revisionsrapport, at der ville være særlig opmærksomhed på udviklingen vedrørende PCLOB's fremtidige udnævnelse af medlemmer for at sikre, at tilsynsorganet var beslutningsdygtigt.[229] Dette forhold har vist sig at skabe en større problematik end først forventet, eftersom Trump afsatte tre demokratiske medlemmer fra PCLOB i januar 2025. Dette medførte, at medlemsantallet i tilsynsorganet er under den påkrævede mindstetærskel for at være

[225] www.edpb.europa.eu/edpb-udtalelse5/2023-eu-us-dpf, s. 6 og betragtning 195
[226] Ibid., betragtning 197 og 200
[227] Ibid., betragtning 202
[228] Ibid., betragtning 205
[229] www.eur-lex.europa.eu/første-regelmæssige-revision-af-dpf, kapitel 2.2.2

beslutningsdygtig.[230] Dette kan have væsentlig betydning for gyldigheden af DPF, eftersom dataoverførselsaftalen beror på de garantier, som følger af PCLOB's beslutningsdygtighed. Endvidere lagde EUK vægt på, at netop dette forhold anses som særlig betydningsfuldt. Den norske datatilsynsmyndighed udtaler derimod, at denne udvikling ikke nødvendigvis er et væsentligt problem, eftersom hensigten er at udpege nye medlemmer. Det skal dog tillægges større betydning, såfremt udpegelsen af nye medlemmer bliver væsentligt forsinket. Dermed mener det norske datatilsyn, at virksomheder bør være opmærksom på denne usikkerhed forbundet med PCLOB og i denne sammenhæng forberede en exitstrategi.[231] Den svenske datatilsynsmyndighed opfordrer ligeledes virksomheder til at være opmærksomme på udviklingen med tilsynsorganet.[232] Grundet den nuværende situation vedrørende den manglende beslutningsdygtighed ved PCLOB, findes argumenterne for, at tilsynsorganet kan fungere i overensstemmelse med garantierne i EO 14086 ikke at være overbevisende, jf. kapitel 8.3. Det må antages, at opfyldelse af mindstetærsklen for medlemsantallet er nødvendigt for, at tilsynsorganet kan udføre deres opgaver tilstrækkeligt. Dette vurderes på trods af, at PCLOB selv mener, at de kan varetage deres opgaver i tilfælde af manglende beslutningsdygtighed.[233]

NOYB mener, at ovenstående argumenterer imod PCLOB's uafhængighed som tilsynsorgan, eftersom USA's præsident tilsyneladende uden fremlagt begrundelse kan afsætte medlemmerne.[234] Dette er også af betydning for tilstrækkeligheden af CLPO og DPRC, eftersom PCLOB er involveret i udnævnelsen af dommere for DPRC og vurderingen af håndtering af klageprocessen for CLPO og DPRC, jf. kapitel 8.3.[235] Dermed kan en manglende beslutningsdygtighed for PCLOB medføre, at samtlige væsentlige organers uafhængighed og funktionalitet i praksis ikke findes tilstrækkeligt. Der kan endvidere argumenteres for, at en udnævnelse af nye medlemmer for PCLOB ikke nødvendigvis vil afhjælpe problemet. Det faktum at USA's præsident uden videre kan fjerne medlemmer og dermed sætte tilsynsorganet ud af spil, argumenterer for, at PCLOB's uafhængighed ikke er garanteret ved det nuværende lovgivningsmæssige fundament, hvilket er et dekret. Ifølge NOYB er dette et centralt forhold, eftersom PCLOB udgør det eneste tilsynsorgan, som DPB bygger på. Dertil mener Max Schrems, at såfremt tilsynsorganet kun er ude af funktion midlertidigt, kan det argumentere for, at aftalen ikke nødvendigvis kan anses som mere mangelfuld end tidligere dataoverførselsaftaler.[236]

[230] Olifent, *Danmark er 100 procent afhængig af Microsoft: Nu truer Trump den aftale, der gør det lovligt at bruge*
[231] www.datatilsynet.no/informasjon-om-overføringer-til-usa
[232] Noori, *Det blåser kring datadelningsavtalet med USA*
[233] www.eur-lex.europa.eu/første-regelmæssige-revision-af-dpf, kapitel 2.2.2
[234] www.noyb.eu/en/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal
[235] www.edpb.europa.eu/edpb-udtalelse5/2023-eu-us-dpf, betragtning 196
[236] www.noyb.eu/en/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal

EDPB og EUK har endnu ikke taget stilling til den manglende beslutningsdygtighed og længden på denne periode for PCLOB. Der kan argumenteres for, at den nuværende situation i relation til PCLOB vil medføre, at EDPB og EUK burde anse tilsynsorganets fundament og uafhængighed som uholdbart grundet manglende beslutningsdygtighed over en længere periode. Selvom dette kan betragtes som et midlertidigt problem, er den aktuelle situation, at PCLOB ikke har været officielt beslutningsdygtig siden januar 2025, og at der på nuværende tidspunkt ikke er udsigt til en udnævnelse af nye medlemmer.

CLPO og DPRC

EDBP anerkender, at afgørelser foretaget af CLPO er af bindende virkning.[237] Dette er et forbedret forhold, eftersom det var en mangel i Privacy Shield i forbindelse med ombudsmandsmekanismen, jf. kapitel 7.7.[238] [239] EDPB bemærker imidlertid, at CLPO kan udelades fra processen, såfremt der foreligger en valideret efterretningsprioritet, men forholder sig ikke nærmere til dette.[240] Dette kan argumentere mod, at kravet om effektive retsmidler i EUC artikel 47 er opfyldt. EDBP omtaler imidlertid ikke dette som en bekymring, hvilket kan anses for uhensigtsmæssigt, eftersom CLPO under visse omstændigheder dermed ikke kan efterleve de garantier, som er fastsat i EO 14086, jf. kapitel 8.4. EDPB vurderer dog senere i deres udtalelse, at CLPO ikke er tilstrækkelig uafhængig, og at dette organ dermed ikke i sig selv opfylder kravet om effektive retsmidler og upartisk domstol, som følger af EUC artikel 47. Dertil nævnes, at EUK gentagne gange er kommet frem til samme vurdering.[241] Det bliver imidlertid ikke tydeliggjort af EDPB, hvad baggrunden for denne vurdering er, men det kan antages, at CLPO's tilhørsforhold som regeringsembedsmand til den udøvende magt er årsagen.[242] Såfremt det er begrundelsen, anerkendes dette, eftersom EUD kritiserede Ombudsmandens uafhængighed på baggrund af dette i Schrems II-afgørelsen, jf. kapitel 7.7. [243]

EDPB sætter spørgsmålstegn ved, om DPRC opfylder kravet i EUC artikel 47 omhandlende retten til effektive retsmidler og til en upartisk domstol, jf. kapitel 4.2. Dette er begrundet i, at DPRC er oprettet gennem et dekret frem for gennem Kongressen, hvilket medfører, at der ikke er tale om en almindelig domstol.[244] EDPB konkluderer, at DPRC " *(...) ikke i sig selv [er] utilstrækkelig.*", såfremt organets

[237] www.edpb.europa.eu/edpb-udtalelse5/2023-eu-us-dpf, betragtning 232
[238] Ibid., betragtning 231
[239] Schrems II, præmis 196
[240] www.edpb.europa.eu/edpb-udtalelse5/2023-eu-us-dpf, betragtning 159
[241] Ibid., betragtning 216
[242] Ibid.
[243] Schrems II, præmis 195
[244] www.edpb.europa.eu/edpb-udtalelse5/2023-eu-us-dpf, betragtning 217

uafhængighed garanteres gennem EO 14086.[245] EDPB mener, at EUK bør være opmærksom på, hvorvidt dette sikres gennem praksis. Dertil mener EDPB, at tilstrækkelighedsafgørelsens gyldighed kan afhænge af denne vurdering samt potentielle ændringer i EO 14086.[246] Denne vurdering af EDPB er som udgangspunkt i overensstemmelse med præmisserne i Schrems II-afgørelsen. EUD tog i denne sag ikke stilling til, hvordan ombudsmandsmekanismen var oprettet på det lovgivningsmæssige niveau, jf. kapitel 7.7. Ombudsmanden var oprettet gennem et PPD, som udelukkende kan udstedes af USA's præsident, og ligesom ved dekreter skal det ikke godkendes gennem Kongressen. Ombudsmanden blev dermed stiftet på lignende måde som DPRC, jf. kapitel 8. Det vurderes hermed i denne sammenhæng, at kravet i EUC artikel 47 omhandlende retten til en domstol, som " *(...) der forudgående er oprettet ved lov.*" ikke indebærer, at DPRC nødvendigvis skal oprettes gennem Kongressen. Dette begrundes i, at EUD ikke vurderede dette element i Schrems II-afgørelsen i diskussionen om ombudsmandensmekanismens opfyldelse af kravene i EUC artikel 47. Det er imidlertid ikke fastslået af EUD, at dette er uden betydning for DPRC's overensstemmelse med EUC artikel 47, hvorfor det ikke med sikkerhed kan udelukkes, at spørgsmålet vil kunne rejses i fremtiden.[247]

DPRC er endvidere oprettet under det amerikanske justitsministerium, som udgør en del af den udøvende magt, hvilket LIBE har fremhævet som væsentligt.[248] På den baggrund er det relevant at undersøge DPRC's praksis nærmere, eftersom organets uafhængighed afhænger af denne vurdering.[249] Baggrunden for denne vurdering findes i Schrems II-afgørelsen, hvor EUD lagde vægt på, at Ombudsmandens tilhørsforhold til udenrigsministeriet var uforeneligt med kravet om uafhængighed, jf. kapitel 7.7.[250] Denne bekymring er således i overensstemmelse med EUD's tidligere retspraksis. EDPB mener endvidere efter en grundig undersøgelse, at omstændighederne ikke argumenterer væsentligt imod DPRC's uafhængighed.[251] Dette anerkendes, eftersom der ved DPRC findes klare forbedringer i forhold til den tidligere ombudsmandsmekanisme. Dette inkluderer, at dommerne i DPRC ikke er underlagt indberetningspligt eller tilsyn af justitsministeren, og samtidig har dommerne omfattende beskyttelse mod uretmæssig afskedigelse, jf. kapitel 8.4. Disse forbedrede forhold var tidligere kritikpunkter for Ombudsmanden i forbindelse med Schrems II, jf. kapitel 7.7.[252]

[245] www.edpb.europa.eu/edpb-udtalelse5/2023-eu-us-dpf, betragtning 220
[246] Ibid., betragtning 221
[247] Ibid., betragtning 219
[248] www.europarl.europa.eu/LIBE-udkast-til-forslag-til-beslutning, betragtning 5
[249] www.edpb.europa.eu/edpb-udtalelse5/2023-eu-us-dpf, betragtning 223
[250] Schrems II, præmis 195
[251] www.edpb.europa.eu/edpb-udtalelse5/2023-eu-us-dpf, betragtning 224
[252] Schrems II, præmis 195

Derudover har DPRC beføjelse til at afsige bindende afgørelser i forbindelse med afhjælpende foranstaltninger, hvilket er endnu et forbedret forhold i relation til Ombudsmanden, som var en af de væsentligste mangler i Schrems II-afgørelsen, jf. kapitel 7.7 og 8.4.[253] EDPB kommer frem til samme vurdering i denne kontekst.[254]

EDPB udtrykker endvidere bekymring over, at DPRC i et bredt omfang anvender standardsvar, samt den manglende gennemsigtighed i afgørelserne og fraværet af appelmuligheder.[255] DPRC har også modtaget kritik fra NOYB, Max Schrems og andre aktører vedrørende anvendelse af standardsvar samt gennemsigtigheden af klageprocessen, eftersom EU-borgere ikke bliver informeret vedrørende de underliggende beslutninger i afgørelserne.[256] [257] LIBE udtrykker ligeledes bekymring vedrørende tilstedeværelsen af klassificerede afgørelser, klagerens begrænsede adgang til information samt den manglende appelmulighed. Derudover udtaler LIBE, at klageprocessen ikke indeholder et krav om at informere klager om behandling af personoplysninger, hvilket underminerer indsigtsretten og retten til berigtigelse, som følger af henholdsvis GDPR artikel 15 og 16.[258] [259]

Ovenstående bekymringer anerkendes, eftersom anvendelsen af standardsvar uden begrundelse til klageren på baggrund af en klassificeret klageprocess kan argumenteres for at være af væsentlig betydning efter EMD's retspraksis. I Big Brother Watch-sagen vurderede EMD, at en domstol eller uafhængigt organ ikke kan betegnes som et effektivt retsmiddel i overensstemmelse med EUC artikel 47, såfremt domstolen eller organet ikke begrunder deres afgørelser.[260] EDPB anerkender imidlertid, at DPRC's afgørelser er begrundede og nævner, at klageren vil blive informeret om potentielt fremtidige afklassificerede dokumenter og dermed begrundelsen.[261] Ud fra en formålsfortolkning, kan der argumenteres for, at EMD's retspraksis bør medføre, at klageren sikres modtagelse af begrundelsen for afgørelsen. Dette er begrundet i, at der kan argumenteres for, at formålet med præmis 359 i Big Brother Watch-sagen er at fremme gennemsigtighed og beskytte EU-borgere, eftersom de er stillet svagere ved amerikanske myndigheders indgreb. Efter denne optik kan DPRC ikke betegnes som et effektivt retsmiddel, såfremt organet undlader at videregive begrundelser for deres afgørelser til klager, hvilket var et væsentligt kritikpunkt for Ombudsmanden i Schrems II-

[253] Schrems II, præmis 196
[254] www.edpb.europa.eu/edpb-udtalelse5/2023-eu-us-dpf, betragtning 231
[255] Ibid., betragtning 239 og 241
[256] NG og Sakellariadis, *Inside Biden's secret surveillance court*
[257] www.noyb.eu/open-letter-future-eu-us-data-transfers
[258] www.europarl.europa.eu/LIBE-udkast-til-forslag-til-beslutning, betragtning 5
[259] Schrems II, præmis 194
[260] www.hudoc.echr.coe.int/big-brother-watch-and-others-v.-the-united-kingdom, præmis 359
[261] www.edpb.europa.eu/edpb-udtalelse5/2023-eu-us-dpf, betragtning 241

afgørelsen, jf. kapitel 7.7.[262] Det konstateres heller ikke, at dokumenterne med begrundelsen for DPRC's afgørelser med sikkerhed vil blive afklassificeret senere hen. I denne kontekst er der hermed tale om en uoverensstemmelse mellem kravet i EUC artikel 47 vedrørende effektive retsmidler og DPRC's funktionsmåde. EDPB kommer tilsyneladende ikke frem til samme konklusion på trods af deres fortolkning af Big Brother Watch-sagen.[263] EDPB anerkender imidlertid i denne sammenhæng, at "*Dette standardsvar tjener det generelt legitime formål at beskytte følsomme oplysninger om amerikanske efterretningsaktiviteter*.".[264] Der findes dermed et argument for, at EDPB ikke anvender eller lægger vægt på den korrekte fortolkning af præmis 359 i Big Brother Watch-sagen. LIBE konkluderer desuden i deres udtalelse, at DPRC ikke opfylder kravene fremsat i EUC artikel 47, eftersom domstolen ikke findes tilstrækkelig upartisk og uafhængig.[265] Dette kan potentielt anerkendes grundet det lovgivningsmæssige grundlag for oprettelsen af organet i form af et dekret. Dertil DPRC's manglende uafhængighed på baggrund omfattende anvendelse af standardsvar uden begrundelse for afgørelser til klager, hvilket kan argumenteres for ikke at være foreneligt med EUC artikel 47.

9.2 Delkonklusion

Ud fra ovenstående kan det konkluderes, at EDPB og EUK løbende vil være opmærksom på, hvordan organerne fungerer i praksis, men har en positiv tilgang til de forbedringer, som introduceres gennem EO 14086. LIBE og NOYB stiller sig derimod kritisk til EO 14086's indhold og funktionalitet i praksis. Det udledes, at der kan argumenteres for, at de garantier og begrænsninger, som EO 14086 indeholder, ikke findes klare, præcise eller forudsigelige i praksis, eftersom dekretet til enhver tid kan ændres eller ophæves af den amerikanske præsident. Der kan endvidere argumenteres for, at CLPO og DPRC's lovgivningsmæssige grundlag også kan kritiseres, eftersom disse organer er oprettet gennem dekretet, EO 14086. Dekretet kritiseres ydermere for ikke at forbyde masseindsamling af data ved signalefterretning og for den manglende forpligtelse til offentliggørelse af legitime nationale sikkerhedshensyn. USA's hensyn til nationale sikkerhedsmål anerkendes, men EU-borgeres grundlæggende rettigheder og friheder må ikke undermineres i denne kontekst. I denne sammenhæng kan det kritiseres, at PCLOB og CLPO under visse omstændigheder kan omgås i forbindelse med skjulte handlinger og valideret efterretningsprioriteter. Det konkluderes endvidere, at USA's

[262] Schrems II, præmis 197
[263] www.edpb.europa.eu/edpb-udtalelse5/2023-eu-us-dpf, betragtning 240 og 241
[264] Ibid., betragtning 239
[265] www.europarl.europa.eu/LIBE-udkast-til-forslag-til-beslutning, betragtning 5

fortolkning af nødvendighedsprincippet kan kritiseres, eftersom denne fortolkning ikke medfører samme beskyttelse som i EU-retten, og at der hermed ikke findes en overensstemmelse. Dertil opfattes proportionalitetsprincippet som overensstemmende med EU-rettens fortolkning.

Funktionaliteten vedrørende PCLOB kan kritiseres, eftersom organet på nuværende tidspunkt og potentielt fremadrettet ikke er beslutningsdygtigt. Disse omstændigheder kan argumenteres for ligeledes at påvirke CLPO og DPRC grundet PCLOB's heraf afledte utilstrækkelige forhold til at udføre tilsyn med disse organer. PCLOB kan endvidere kritiseres vedrørende organets manglende uafhængighed og gennemsigtighed, eftersom medlemmerne kan afsættes uden væsentlig og offentlig begrundelse. CLPO og DPRC anerkendes for deres afgørelsers bindende virkning, men kan imidlertid kritiseres for deres manglende uafhængighed grundet tilhørsforholdet til den udøvende magt, jf. Schrems II, præmis 195 og 196. Imidlertid anerkendes DPRC's forbedrede forhold, herunder fraværelsen af indberetningspligt og tilsyn af den udøvende magt samt uretmæssig afskedigelse af dommerne. DPRC kan endvidere kritiseres for deres omfattende anvendelse af standardsvar uden begrundelse samt manglende gennemsigtighed og appelmulighed. Afslutningsvis kan der argumenteres for, at disse forhold medfører, at DPRC ikke anses som et effektivt retsmiddel, hvilket er i uoverensstemmelse med EUC artikel 47.

10 Supplerende foranstaltninger ved SCC'er

For at kunne besvare specialets problemformulering findes det relevant at gennemgå væsentlige afgørelser fra diverse datatilsynsmyndigheder og nationale domstole i EU. Begrundelsen for udelukkende at undersøge SCC'er findes i, at dette overførselsgrundlag er det mest benyttede og relevante alternative overførselsgrundlag til en tilstrækkelighedsafgørelse, jf. kapitel 3. Formålet med denne analyse af retspraksis er at undersøge, hvornår tilstrækkelighed anses for at være opnået ved anvendelse af supplerende foranstaltninger ved SCC'er i praksis. Der fokuseres på dataoverførsler fra EU til USA ved anvendelse af SCC'er. Dertil vil EDPB's vejledning vedrørende supplerende foranstaltninger inddrages.

10.1 Retspraksis

Den 23. marts 2023 fremkom en af de første afgørelser vedrørende Google Analytics fra en national domstol, som erklærede en dataoverførsel til USA for ulovlig.[266] Sagen fra Tyskland omhandlede et forbrugercenter, som lagde sag an mod et telekommunikationsselskab. Sagsøger anførte, at sagsøgte ulovligt overførte kunders personoplysninger til Google LLC i USA. Domstolen fastslog, at der på daværende tidspunkt ikke var en gyldig tilstrækkelighedsafgørelse, som dermed kunne udgøre et overførselsgrundlag. Endvidere blev det fastlagt, at anvendelsen af SCC'er som overførselsgrundlag ikke kunne forekomme, eftersom SCC'er ikke medførte et tilstrækkeligt databeskyttelseniveau gennem fornødne garantier, jf. GDPR artikel 46, stk. 2, litra c. Dette var begrundet i, at SCC'er ikke kunne beskytte EU-/EØS-borgeres personoplysninger mod adgang og indgreb fra efterretningstjenesterne i USA, eftersom disse myndigheder ikke kunne bindes af SCC'er, jf. Schrems II, præmis 126. Dertil anførte domstolen, at eftersom tilstrækkelighedsafgørelsen var erklæret ugyldig grundet de lovgivningsmæssige omstændigheder i USA, kunne det ikke antages, at SCC'er kunne medføre en tilstrækkelig databeskyttelse uden supplerende foranstaltninger i henhold til GDPR artikel 44, jf. Schrems II, præmis 133. Derudover fremlagde sagsøgte ikke belæg for anvendelsen af supplerende foranstaltninger for at kompensere for den problematiske lovgivning i USA, eftersom der hverken var suppleret med tekniske, organisatoriske eller kontraktuelle foranstaltninger efter anbefalingerne af EDPB.[267] [268]

[266] www.gdprhub.eu/LG-Köln-33-O-376/22
[267] Ibid.
[268] www.edpb.europa.eu/henstilling-01/2020-om-foranstaltninger-der-supplerer-overførselsværktøjer

Den 12. maj 2023 blev det fastslået af en national domstol i Østrig, at en overførsel af personoplysninger til USA ved brug af Google Analytics var ulovlig.[269] Sagen udsprang af en tidligere afgørelse med samme kendelse fra datatilsynsmyndigheden i Østrig på baggrund af en klage fra NOYB baseret på udfaldet af Schrems II. Efter afgørelsen ved datatilsynsmyndigheden havde Google LLC anket til den nationale domstol. Google LLC anførte, at overførslerne var lovlige, eftersom der blev anvendt SCC'er som overførselsgrundlag, og at der samtidig var indført passende tekniske og organisatoriske foranstaltninger. Domstolen fandt, at de indførte foranstaltninger ikke var tilstrækkelige i et sådant omfang, at de forhindrede amerikanske efterretningstjenester fra at få adgang til personoplysningerne fra EU/EØS. Dette var understøttet af, at Googles rapportering viste, at mængden af anmodninger om adgang til personoplysninger fra efterretningstjenesterne var af væsentlig grad. Dertil fandt den østrigske domstol, at en organisatorisk foranstaltning i form af en kontraktuel forpligtelse til at underrette dataeksportøren om anmodninger fra efterretningstjenester i USA ikke ansås som en tilstrækkelig foranstaltning i henhold til beskyttelse af de registreredes rettigheder. Det følger af amerikansk lovgivning, at efterretningstjenester i nødstilfælde kan pålægge den dataansvarlige ikke at informere tredjeparter om disse anmodninger. Det blev endvidere vurderet, at et udslagsgivende element var, at EU-/EØS-borgere ikke havde mulighed for en effektiv klageadgang, såfremt der forekom en ulovlig videregivelse til efterretningstjenesterne. Domstolen vurderede ligeledes, at en teknisk foranstaltning i form af kryptering ikke var tilstrækkelig. Dette var begrundet i, at amerikansk lovgivning forpligter dataimportøren til at videregive personoplysninger såvel som de dekrypteringsnøgler, som er nødvendige for at kunne dekryptere dem. Grundet ovenstående konstaterede den østrigske domstol, at Google LLC's tekniske og organisatoriske foranstaltninger ikke var tilstrækkelige, hvilket medførte, at overførslen var ulovlig.[270]

Tilsvarende forhold blev behandlet af DT i Danmark i Chromebook-sagen af den 14. juli 2022.[271] I denne sag anvendte adskillige danske kommuner Chromebooks og havde i denne henseende indgået en databehandleraftale med Google Irland vedrørende behandling af personoplysninger tilhørende skoleelever. Helsingør Kommune havde gennem instruks medført etablering af en underdatabehandler fra USA ved navn Google LLC. SCC'er blev anvendt mellem databehandleren og underdatabehandleren som overførselsgrundlag til USA. DT fandt, at sagens personoplysninger omhandlede *non-U.S persons*, hvilket medførte, at de registrerede var omfattet af FISA 702, og dermed muliggjorde indgreb ved krav om udlevering af personoplysninger til amerikanske

[269] www.gdprhub.eu/BVwG-W245-2252208-and-W245-2252221-1/30E
[270] Ibid.
[271] www.datatilsynet.dk/datatilsynet-fastholder-forbud-i-chromebook-sag-2020-431-0061

efterretningstjenester. I denne sammenhæng refererede DT til Schrems II, præmis 126 vedrørende SCC'ers tilstrækkelighed angående tredjelande, hvis lovgivning muliggør indgreb i EU-/EØS-registreredes grundlæggende rettigheder. Dertil fandt DT, at underdatabehandleren i sagen var omfattet af begrebet *electronic communications service provider* i amerikansk lovgivning, hvilket også var et krav for, at efterretningstjenester i USA kunne kræve udlevering af personoplysninger. DT fandt endvidere, at EO 12333 muliggjorde adgang til personoplysninger i transit, og dermed før de var ankommet til USA. DT henviste herefter til Schrems II-afgørelsen, hvor EUD konkluderede, at USA's omtalte lovgivning tilsidesatte de grundlæggende rettigheder i EUC artikel 47 og 52. DT konkluderede på baggrund af dette, at der skulle etableres supplerende foranstaltninger for at sikre et tilstrækkeligt databeskyttelsesniveau gennem SCC'er grundet USA's problematiske lovgivning, jf. Schrems II, præmis 132.[272] Angående anvendelse af supplerende foranstaltninger fandt DT, at Helsingør Kommune gjorde brug af kryptering både i hvile og i transit ved overførsel til USA. Dertil fastslog DT denne foranstaltning som værende effektiv i en generel forstand, jf. GDPR artikel 32, stk. 1, litra a. Det blev derimod anført, at krypteringen under sagens omstændigheder var ineffektiv, eftersom underdatabehandleren formentlig havde adgang til personoplysningernes *klartekst,*[273] og at dekrypteringsnøglen var i databehandlerens besiddelse. Der var således ikke tale om en effektiv supplerende foranstaltning, som forhindrede USA's efterretningstjenester i at få udleveret personoplysningerne. Dette var påkrævet grundet amerikansk lovgivning, samt fordi SCC'er kun er bindende for de indgåede parter og dermed ikke for tredjelandes myndigheder.[274]

En lignende sag af den 28. februar 2023 fra den norske datatilsynsmyndighed konkluderede, at der var sket en overtrædelse af GDPR artikel 44 ved anvendelsen af Google Analytics grundet en manglende tilstrækkelighed vedrørende supplerende foranstaltninger.[275] Datatilsynsmyndigheden udstedte en irettesættelse på baggrund af ovenstående. De etablerede foranstaltninger indebar procedurer, politikker samt et team af jurister med fokus på håndtering af anmodninger fra efterretningstjenester i henhold til personoplysninger. Dertil var der anvendt et *redigeringsscript*[276] og IP-anonymisering som supplerende foranstaltninger. Google argumenterede for, at det i denne sammenhæng ikke var muligt at videregive personoplysninger til efterretningstjenester efter anmodning. Den norske datatilsynsmyndighed vurderede imidlertid, at Google stadig havde adgang til personoplysningernes *klartekst,* og at de behandlede personoplysninger involverede yderligere

[272] www.datatilsynet.dk/datatilsynet-fastholder-forbud-i-chromebook-sag-2020-431-0061
[273] *Ukrypteret og læsbar data*
[274] www.datatilsynet.dk/datatilsynet-fastholder-forbud-i-chromebook-sag-2020-431-0061
[275] www.gdprhub.eu/Datatilsynet-(Norway)-20/03771
[276] *Program, som kan redigere personoplysninger inden en tredjelandsoverførsel*

data end blot IP-adresser. Det blev fastslået, at personoplysningerne kunne omfattes af FISA 702 i praksis, og i denne sammenhæng var der ikke tale om tilstrækkelige supplerende foranstaltninger.[277]

Datatilsynsmyndigheden i Østrig fremlagde tilsvarende afgørelse i en sag af den 22. december 2021, hvor tilstrækkeligheden af en pseudonymiseringsforanstaltning ikke fandtes ækvivalent, eftersom de registrerede fortsat var identificerbare ved diverse identifikatorer.[278] Ligeledes af den 20. august 2024 blev det vurderet, at en anden supplerende foranstaltning i form af en *proxyserver*[279] ikke opfyldte kravet om tilstrækkelighed i en afgørelse fra Holland. Den hollandske datatilsynsmyndighed udstedte i denne afgørelse en irettesættelse, eftersom de registrerede fortsat var identificerbare grundet mængden af data tilgængelig for efterretningstjenester og dataimportør.[280]

10.2 EDPB's vejledning om supplerende foranstaltninger

Henstilling nr. 01/2020 - Version 2, som er vedtaget den 18. juni 2021, omhandlende foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, er en vejledning til EU-/EØS-dataeksportører. Denne vejledning hjælper dataeksportører med at vurdere, hvorvidt et tredjelands lovgivning samt praksis står i kontrast til de fornødne garantier, som er sikret i GDPR artikel 46. Dertil beskrives retningslinjer for, hvordan og hvornår effektive supplerende foranstaltninger skal implementeres, såfremt dette kræves grundet et tredjelands lovgivning og praksis. Denne henstilling findes relevant at sammenholde med den tidligere fremlagte retspraksis ved EUD samt nationale datatilsynsmyndigheder og domstole for at kunne besvare problemformuleringen fyldestgørende.[281]

EDPB henviser indledningsvis til diverse betragtninger udledt i Schrems II-afgørelsen. EDPB lægger vægt på Schrems II, præmis 93-94 vedrørende ækvivalent databeskyttelse ved overførsel til tredjelande, som skal sikres ved at sammenholde præmisserne med EUC og kapitel V i GDPR. Dertil nævnes, at såfremt der ikke eksisterer en tilstrækkelighedsafgørelse, skal de fornødne garantier ved overførsel til tredjelande sikres på anden vis gennem GDPR artikel 46, stk. 2. Derudover kan SCC'er ikke binde offentlige myndigheder i tredjelande, og det kan således findes nødvendigt at implementere supplerende foranstaltninger for at sikre SCC'er som et tilstrækkeligt

[277] www.gdprhub.eu/Datatilsynet-(Norway)-20/03771
[278] www.gdprhub.eu/DSB-(Austria)-2021-0.586.257
[279] *Proxyservere skjuler IP-adresser*
[280] www.gdprhub.eu/AP-(The-Netherlands)-Takeaway-B.V.-z2022-04011
[281] www.edpb.europa.eu/henstilling-01/2020-om-foranstaltninger-der-supplerer-overførselsværktøjer, s. 1-5

overførselsgrundlag, jf. Schrems II, præmis 132-133. Dataeksportøren pålægges at vurdere lovgivning og praksis i tredjelandet med henblik på tilstrækkelig databeskyttelse, som kan ske i samarbejde med dataimportøren hvis relevant, jf. Schrems II, præmis 134. Såfremt nødvendige supplerende foranstaltninger ikke kan sikres af dataeksportøren, skal overførslen afbrydes af dataeksportøren eller datatilsynsmyndigheden, jf. Schrems II, præmis 135. På trods af disse betragtninger findes der ikke en klar definition gennem EUD's retspraksis eller i GDPR for overførselsgrundlaget i artikel 46, stk. 2. EDPB forklarer, at formålet med denne henstilling er at give retningslinjer for, hvornår supplerende foranstaltninger skal implementeres samt hvilke supplerende foranstaltninger, der bør være til stede under forskellige omstændigheder.[282]

Fremgangsmåde ved indførelse af supplerende foranstaltninger

EDPB opstiller i deres henstilling seks trin, som en dataeksportør med fordel kan anvende til at vurdere, om der ved en overførsel af personoplysninger til tredjelande skal indføres supplerende foranstaltninger. I denne sammenhæng skal dataeksportøren kunne påvise gennem dokumentation, hvordan vurderingen af overførslen samt de supplerende foranstaltninger er foretaget. Derudover skal denne dokumentation udleveres til en datatilsynsmyndighed, såfremt dette påkræves.[283]

Trin et indebærer en oversigt og grundig viden vedrørende de pågældende overførsler, som foretages. Der skal i denne sammenhæng være kendskab til alle overførsler og deres type. Denne oversigt kan sammenholdes med fortegnelser over behandlingsaktiviteter. Der skal samtidig foretages løbende opdatering og revidering af dette.[284] Trin to omhandler, hvilket overførselsgrundlag eller værktøj, som benyttes, hvilket i denne kontekst er SCC'er, jf. GDPR artikel 46, stk. 2, litra c. Ved anvendelse af SCC'er kan supplerende foranstaltninger være nødvendigt for at sikre tilstrækkelig databeskyttelse.[285]

Trin tre vedrører en vurdering af, hvorvidt det valgte overførselsgrundlag findes effektivt i forbindelse med sikring af databeskyttelsesniveauet i praksis. I situationer hvor garantierne ved overførselsgrundlaget tilsidesættes grundet lovgivning og praksis i tredjelandet, vil der ikke være tale om en tilstrækkelig databeskyttelse. Dette gælder også for personoplysningernes transit til tredjelandet. I denne situation skal dataeksportøren og dataimportøren i samarbejde med hinanden

[282] www.edpb.europa.eu/henstilling-01/2020-om-foranstaltninger-der-supplerer-overførselsværktøjer, s. 3 og 7-8
[283] Ibid., s. 10
[284] Ibid., s. 10-11
[285] Ibid., s. 12-14

foretage en vurdering af, hvorvidt lovgivning og praksis i tredjelandet kan tilsidesætte garantierne i overførselsgrundlaget, og om overførslen kan blive omfattet af disse regler. I denne vurdering skal det undersøges, hvorvidt en offentlig myndighed, herunder efterretningstjenester, kan tilgå de pågældende personoplysninger uden en dataimportørens kendskab til dette. Dertil også om myndighederne kan tilgå personoplysninger gennem dataimportøren eller andre organisationer som telekommunikationsudbydere. Alle relevante omstændigheder vedrørende personoplysninger og involverede aktører bør undersøges for at kunne foretage en vurdering af tredjelandets lovgivning og praksis. EDPB henviser specifikt til offentlige myndigheders adgang til personoplysninger i forbindelse med national sikkerhed og lignende hensyn. I denne kontekst tilsidesætter tredjelandets lovgivning og praksis ikke nødvendigvis de registreredes rettigheder, såfremt der findes overensstemmelse med nødvendigheds- og proportionalitetsprincipperne. Der skal også mere specifikt foretages en vurdering af de registreredes mulighed for klageindgivelse og retshåndhævelse af krænkelser ved domstole eller datatilsynsmyndigheder. Et tredjelands lovgivning og praksis anses som værende i uoverensstemmelse med de sikrede garantier i eksempelvis SCC'er, såfremt rettighederne og frihederne i EUC ikke anerkendes, eller principperne om nødvendighed eller proportionalitet ikke overholdes.[286]

Trin fire omfatter indførelsen af supplerende foranstaltninger, såfremt dette findes nødvendigt efter vurderingen af et tredjelands lovgivning og praksis i trin tre. Disse foranstaltninger kan være af teknisk, organisatorisk eller kontraktlig karakter. Dertil kan en kombination af de tre typer være fordelagtig. Dog findes det væsentligt at nævne, at kun supplerende foranstaltninger af den tekniske type anses som effektive mod indgreb af offentlige myndigheder i tredjelande. Dette finder eksempelvis sted, når der foretages indgreb i forbindelse med overvågning, som medfører tilsidesættelse af kravene i EUC artikel 47 og 52. EDPB anbefaler i sådanne scenarier, at en dataeksportør blandt andet vurderer følgende omstændigheder i forbindelse med valg af foranstaltning: personoplysningers format og type, antal af aktører og mulighed for videreoverførsel. Valg af supplerende foranstaltninger afhænger endvidere altid af overførslens kontekst. Ved overførsel til tredjelande, hvor lovgivning og praksis medfører, at eksempelvis kryptering er ineffektivt, skal der indføres andre mere effektive supplerende foranstaltninger for at opretholde de standarder, som sikres i EU/EØS.[287]

[286] www.edpb.europa.eu/henstilling-01/2020-om-foranstaltninger-der-supplerer-overførselsværktøjer, s. 15-21
[287] Ibid., s. 23-25

I trin fem beskrives de proceduremæssige valg, som en dataeksportør bør overveje i forbindelse med valg af supplerende foranstaltninger. Ændringer eller tilføjelser af standardbestemmelser skal ikke godkendes af datatilsynsmyndigheder, såfremt de ikke er uforenelige eller underminerer love og principper i GDPR. Ændringer skal beskrives klart og præcist, så der ikke kan forekomme tvivl i fortolkningen af disse. Datatilsynsmyndigheder har desuden kompetence til at vurdere disse supplerende foranstaltninger. EDPB understreger endvidere, at overførselsgrundlag som SCC'er er af kontraktlig art og kan dermed ikke forpligte tredjelandes myndigheder. Trin seks forklarer, at dataeksportøren kontinuerligt skal revidere og evaluere tredjelandets forandringer i lovgivning og praksis. Dette kan enten være i forbindelse med en vurdering af, om supplerende foranstaltninger overhovedet er nødvendigt, eller om valget af disse ikke længere findes effektivt i praksis.[288]

Supplerende foranstaltninger og opstillede scenarier

Foruden ovenstående forholder EDPB sig også til adskillige specifikke supplerende foranstaltninger af alle typer og opstiller scenarier, hvor de supplerende foranstaltninger henholdsvis findes effektive eller ineffektive. Her medtages de relevante supplerende foranstaltninger og scenarier, som der findes i denne henstilling.[289]

EDPB opstiller et scenarie, hvor der eksporteres data til et tredjeland med lovgivning eller praksis, som muliggør, at myndighederne i landet kan tilgå den eksporterede data i transit. I denne situation vurderer EDPB, at der anvendes *transportkryptering*,[290] som er effektiv mod myndighedernes metoder til at tilgå data. Derudover skal personoplysningerne også krypteres *ende-til-ende*[291] for at sikre databeskyttelse, såfremt transportkryptering ikke er nok i sig selv grundet omstændighederne. Endvidere varetages krypteringsnøglerne af en dataeksportør eller af en anden aktør, som kan sikre tilsvarende databeskyttelse. Såfremt disse omstændigheder opnås i dette scenarie på en sikret, teknisk aktuel og korrekt måde, vurderes det af EDPB, at der er tale om en effektiv supplerende foranstaltning.[292]

Et andet scenarie, som EDPB opstiller, omhandler dataeksport til en cloud-udbyder i et tredjeland, hvor det er muligt for myndigheder at tilgå data grundet lovgivning og praksis. I dette tilfælde er der grundet databehandlingens omstændigheder ikke anvendt effektiv pseudonymisering eller kryptering.

[288] www.edpb.europa.eu/henstilling-01/2020-om-foranstaltninger-der-supplerer-overførselsværktøjer, s. 26-28
[289] www.edpb.europa.eu/henstilling-01/2020-om-foranstaltninger-der-supplerer-overførselsværktøjer, s. 30-32
[290] *Beskytter data under transmission*
[291] *Kryptering ved afsender og dekryptering ved modtager*
[292] www.edpb.europa.eu/henstilling-01/2020-om-foranstaltninger-der-supplerer-overførselsværktøjer, s. 34-35

Derudover er det gennem tredjelandets lovgivning eller praksis muligt for myndigheder at tilgå de eksporterede data på en måde, som er i uoverensstemmelse med principperne om proportionalitet og nødvendighed. Her vurderer EDPB, at der ikke er anvendt en effektiv supplerende foranstaltning, som beskytter de registreredes rettigheder. EDPB uddyber yderligere, at der ikke er tale om en effektiv supplerende foranstaltning i situationer, hvor dataimportøren skal kunne tilgå personoplysningerne, selvom der er anvendt kryptering både i transit og i hvile. Dette er begrundet i, at dataimportøren i disse scenarier råder over krypteringsnøglerne, hvilket kan kræves udleveret til myndighederne i tredjelandet.[293]

Foruden de tekniske foranstaltninger kan der indføres yderligere kontraktmæssige foranstaltninger. Kontraktmæssige supplerende foranstaltninger vil som oftest indebære unilaterale, bilaterale eller multilaterale forpligtelser. Ved anvendelse af eksempelvis SCC'er som overførselsgrundlag er der tale om multilaterale forpligtelser i kontraktlig forstand. Det kan dog være hensigtsmæssigt eller nødvendigt at introducere yderligere kontraktmæssige foranstaltninger på trods af anvendelsen af SCC'er for yderligere at sikre de garantier, som SCC'er skal medføre for de registrerede. Eftersom SCC'er ikke kan forpligte myndigheder i tredjelande, kan indførelse af tekniske, organisatoriske og kontraktmæssige foranstaltninger medføre større sikkerhed. EDPB forklarer imidlertid, at foranstaltningerne skal baseres på den individuelle overførsel og kan dermed ikke nødvendigvis sikre overensstemmelse med EU-/EØS-standarder.[294]

Kontraktlige foranstaltninger kan indebære en forpligtelse til at indføre tekniske foranstaltninger, før en overførsel foretages. Dertil kan der være krav om gennemsigtighed mellem dataimportøren og dataeksportøren. Dette kan indebære væsentlig information vedrørende tredjelandets lovgivning og retspraksis samt udviklingen inden for dette. Det kan også indebære, hvorvidt forretningspraksis ændres, eller om dataimportøren ved krav skal overlevere krypteringsnøgler. Derudover kan dataeksportøren eksempelvis introducere strengere krav vedrørende mulighed for inspektioner ved dataimportøren. Såfremt en inspektion skulle medføre opdagelse af uoverenstemmelser med EU-/EØS-standarder, kan der også indføres strengere krav for suspendering eller ophævelse i forbindelse med tidsgrænser. Mere specifikt kan der også indføres en kanariefuglsgaranti fra dataimportørens side, hvor denne regelmæssigt oplyser dataeksportøren vedrørende modtagne krav om overgivelse af personoplysninger til myndighederne i tredjelandet. Dataimportøren kan også forpligtes i denne

[293] www.edpb.europa.eu/henstilling-01/2020-om-foranstaltninger-der-supplerer-overførselsværktøjer, s. 37
[294] Ibid., s. 39

sammenhæng til at anfægte modtagne krav om overgivelse, såfremt omstændighederne taler for denne mulighed.[295]

Organisatoriske foranstaltninger, som kan medføre styrket sikkerhed af de garantier, som overførselsgrundlaget indebærer, kan bestå af forretningsmæssige standarder og politikker. Der kan introduceres en procedure, som beskriver, hvordan en dataimportør skal reagere i forbindelse med anmodninger om videregivelse af personoplysninger og risici herved. Disse foranstaltninger kan eksempelvis sætte fokus på rapportering, ansvarsfordeling og juridiske anliggender.[296]

10.3 Delkonklusion

Der kan på baggrund af ovenstående konkluderes ud fra retspraksis og EDPB's retningslinjer, hvordan og hvornår supplerende foranstaltninger skal anvendes ved benyttelse af SCC'er som overførselsgrundlag. Dette inkluderer at lave en oversigt over alle overførsler og overførselsgrundlag, som foretages og anvendes. Dertil skal der foretages en vurdering af det pågældende tredjelands lovgivning og praksis, hvilket inkluderer den registreredes mulighed for klageindgivelse samt retshåndhævelse. Herefter skal der indføres supplerende foranstaltninger, såfremt det er nødvendigt grundet tredjelandets lovgivning og praksis, hvilket kan være af teknisk, organisatorisk eller kontraktlig karakter. Effektive tekniske supplerende foranstaltninger kan eksempelvis omfatte kryptering og pseudonymisering, men dette er betinget af omstændighederne for overførslen, lovgivning og praksis samt detaljerne for de supplerende foranstaltninger. Dertil kan der indføres kontraktlige foranstaltninger i form af krav om gennemsigtighed eller organisatoriske som standarder og politikker.

Det kan endvidere fastslås gennem retspraksis, at SCC'er som overførselsgrundlag kun retmæssigt kan anvendes, såfremt de medfører et tilstrækkeligt databeskyttelseniveau gennem fornødne garantier, jf. GDPR artikel 46, stk. 2, litra c. Dertil kan SCC'er i modsætning til tilstrækkelighedsafgørelsers potentielle lovgivningsmæssige følger ikke beskytte registrerede mod indgreb fra efterretningstjenester i USA på samme vis, eftersom myndighederne ikke kan bindes af SCC'er, jf. Schrems II, præmis 126. Tilstrækkeligheden af SCC'er skal derimod sikres gennem de fornødne garantier i forbindelse med overførselsgrundlaget, herunder tekniske, organisatoriske eller

[295] www.edpb.europa.eu/henstilling-01/2020-om-foranstaltninger-der-supplerer-overførselsværktøjer, s. 39-46
[296] Ibid., s. 48-51

kontraktlige foranstaltninger. Det kan endvidere udledes af retspraksis, at anvendelse af kryptering ved udlevering af dekrypteringsnøgle og underrettelse af dataimportør vedrørende myndighedsanmodninger ikke medfører en tilstrækkelig databeskyttelse under visse omstændigheder i relation til amerikansk lovgivning. Dertil at anvendelse af IP-anonymisering, *redigeringsscript*, pseudonymisering og *proxyserver* også kan ifalde samme problematikker.

11 CLOUD Act

CLOUD Act blev i 2018 indført i amerikansk lovgivning med det formål at sikre hurtig adgang til data, som opbevares hos udbydere af onlinetjenester, forudsat at adgangen er begrundet i en strafferetlig efterforskning.[297] På trods af lovgivningens manglende medtagelse i Schrems I- og II-afgørelserne findes den stadig relevant i relation til udfordringer forbundet med dataoverførsel til USA. Udfordringen beror på, at CLOUD Act kan pålægge amerikanske databehandlere, som er etableret i EU, at udlevere personoplysninger på baggrund af myndighedsanmodninger uden et relevant behandlings- eller overførselsgrundlag, som anerkendes af EU-retten.[298] Denne type af databehandlere kan således befinde sig i en jurisdiktionskonflikt mellem USA og EU's lovgivning. Databehandleraftaler findes relevant at inddrage i denne sammenhæng, eftersom indholdet i en databehandleraftale kan have betydning på dette område. Dette vil herefter belyses nærmere ved inddragelse af KOMBIT-sagen, hvor DT tager stilling til konkrete komplikationer forbundet med dette.

11.1 Databehandleraftaler

Databehandleraftaler regulerer, hvordan en databehandler, typisk en cloud-udbyder, må behandle personoplysninger på vegne af en dataansvarlig, såsom en virksomhed i EU.[299] Databehandleraftaler skal således udarbejdes, såfremt der foreligger en databehandlerkontruktion mellem en dataansvarlig og en databehandler, og sådanne skal leve op til kravene i GDPR.[300]

Kravene i GDPR

GDPR fastsætter i artikel 28, stk. 3, litra a-h, specifikke minimumskrav til en databehandleraftales indhold, herunder oplysninger om, hvad en behandling omfatter og dens varighed, karakter og formål. En databehandleraftale skal ydermere angive type af personoplysninger og en dataansvarligs rettigheder og forpligtelser, herunder en databehandlers pligter i henhold til en behandlings udførelse.[301] En databehandler må i henhold til en tredjelandsoverførsel kun behandle personoplysninger efter instruks fra en dataansvarlig, og før en behandling igangsættes, skal en dataansvarlig sikre sig, at en databehandler vil være i stand til at overholde de i GDPR nævnte krav.

[297] www.justice.gov/criminal/cloud-act-resources
[298] www.edps.europa.eu/19-07-10-edpb-edps-cloud-act-annex, s. 1
[299] www.datatilsynet.dk/Vejledning-om-cloud
[300] www.datatilsynet.dk/Vejledning-om-dataansvarlige-og-databehandlere
[301] Ibid.

En dataansvarlig, såsom en virksomhed i EU, forpligtes således til at bruge en databehandler, såsom en cloud-udbyder i USA, som overholder GDPR, jf. artikel 28, stk. 1.[302] Denne situation vil gennemgås nærmere i kapitel 11.2 og 11.3 omhandlende CLOUD Act, MLAT og KOMBIT.

Følgende vil indeholde en gennemgang af udvalgte og relevante minimumskrav, som en databehandleraftale skal indeholde ved en databehandlerkontruktion mellem en dataansvarlig og en databehandler.

Instruks, jf. GDPR artikel 28, stk. 3, litra a

En databehandler er pligtig i henhold til at iagttage instrukser fra en dataansvarlig ved behandling af personoplysninger, herunder dataoverførsler til tredjelande.[303] En dataansvarligs dokumenterede anvisninger udgør således rammerne for, hvordan en databehandler kan og må behandle personoplysninger.[304] Instrukskrav er imidlertid ikke gældende, hvis retlige forpligtelser eller lovkrav, herunder EU-lovgivning eller national lovgivning, som en databehandler underlægges, går forud for en dataansvarligs dokumenterede instrukser. I denne situation skal en databehandler underrette en dataansvarlig om de retlige krav, før en behandling igangsættes, medmindre en sådan underretning forbydes af hensyn til en vigtig samfundsmæssig interesse, jf. artikel 28, stk. 3, litra a.[305]

Denne forpligtelse om instruks følger ligeledes af GDPR artikel 29, hvorefter en databehandler og enhver, som udfører arbejde for en dataansvarlig eller en databehandler, og som har adgang til personoplysninger, kun må behandle sådanne oplysninger efter instruks fra en dataansvarlig.[306] Såfremt en databehandler med overlæg ikke følger en dataansvarligs instrukser, vil en sådan kunne blive en selvstændig dataansvarlig for de pågældende behandlinger, hvorfor kravene til en dataansvarlig i GDPR skal overholdes.[307]

Behandlingssikkerhed, jf. GDPR artikel 28, stk. 3, litra c

En databehandler skal iværksætte alle de sikkerhedsforanstaltninger, som kræves i artikel 32.[308] I medfør af stk. 1, skal en dataansvarlig såvel som en databehandler implementere passende tekniske og organisatoriske foranstaltninger, såsom pseudonymisering og kryptering, som afspejler de aktuelle

[302] Udsen, *Databeskyttelsesret*, s. 105
[303] www.datatilsynet.dk/Artikel-29-gruppen-vedrørende-databeskyttelse
[304] Udsen, *Databeskyttelsesret*, s. 109
[305] GDPR artikel 28
[306] GDPR artikel 29
[307] Udsen, *Databeskyttelsesret*, s. 102 ff.
[308] GDPR artikel 28

tekniske niveauer og risici for de registreredes rettigheder.[309] En dataansvarligs forpligtelser i henhold til behandlingssikkerhed fremgår ligeledes af GDPR artikel 24 og artikel 5, stk. 2, omhandlende ansvarlighedsprincippet, som pålægger en dataansvarlig at dokumentere overholdelse af GDPR.[310] [311]

Underdatabehandlere, jf. GDPR artikel 28, stk. 3, litra d

En databehandler skal opfylde de i artikel 28, stk. 2 og 4, nævnte betingelser, før en underdatabehandler anvendes.[312] En underdatabehandler må udelukkende anvendes med tilladelse fra en dataansvarlig, og i en sådan situation bindes en underdatabehandler af de samme forpligtelser, som aftales mellem en dataansvarlig og en databehandler.[313] Kravene i en underdatabehandleraftale er identiske med de krav til en databehandleraftale, som følger af artikel 28, stk. 3.[314] Såfremt en underdatabehandler ikke opfylder dens forpligtelser, forbliver den oprindelige databehandler ansvarlig over for den dataansvarlige for opfyldelse af underdatabehandlerens forpligtelser, jf. GDPR artikel 28, stk. 4.[315]

Revisioner og inspektioner, jf. GDPR artikel 28, stk. 3, litra h

En databehandler skal stille alle de nødvendige oplysninger til rådighed for en dataansvarlig for at kunne påvise overholdelse af de i artikel 28 nævnte krav.[316] En dataansvarlig skal i medfør af ansvarlighedsprincippet løbende vurdere og kontrollere, at en behandling af personoplysninger opfylder kravene i GDPR.[317] En dataansvarlig skal således sikre ved valg af en databehandler, at denne er i stand til at overholde de i GDPR nævnte krav og løbende kontrollere, at denne overholdelse faktisk sker, og til hjælp for dette forpligtes en databehandler til at muliggøre en revision og inspektion.[318]

Sammenfatning

Det udledes, at der ved en databehandlerkontruktion skal udarbejdes en databehandleraftale, som er bindende for en databehandler. I forbindelse hermed skal en dataansvarlig vurdere, om en

[309] GDPR artikel 32
[310] GDPR artikel 24
[311] GDPR artikel 5
[312] GDPR artikel 28
[313] Udsen, *Databeskyttelsesret*, s. 114
[314] GDPR artikel 28
[315] GDPR artikel 28
[316] GDPR artikel 28
[317] GDPR artikel 5
[318] Udsen, *Databeskyttelsesret*, s. 115

databehandler kan og vil overholde kravene i GDPR. En sådan vurdering har særlig relevans, hvis en virksomhed i EU (dataansvarlig) anvender en cloud-udbyder i USA (databehandler), eftersom udenlandske udbydere kan underlægges nationale lovgivninger som CLOUD Act, som kan give de amerikanske myndigheder, herunder efterretningstjenester, adgang til personoplysninger.[319] Denne udfordring vil gennemgås nedenfor.

11.2 CLOUD Act's indhold og problematikker

CLOUD Act blev til som følge af den langvarige retssag mellem den amerikanske regering og Microsoft. Sagen omhandlede en uafhængig domstols udstedelse af en ransagningskendelse til Department Of Justice i henhold til US Stored Communications Act. I første og anden instans fik Microsoft ikke medhold i, at data opbevaret i Irland lå uden for amerikansk jurisdiktion. Ved en appelsag fik Microsoft dog medhold, eftersom virksomheden argumenterede for, at en amerikansk ransagningskendelse ikke har forrang over irsk lovgivning, og at adgang til data, der er lagret uden for USA, bør indhentes gennem internationale aftaler.[320] Domstolens afgørelse fastslog, at retten til privatliv skal sikres online på samme måde, som den respekteres i den virkelige verden. Den amerikanske regering havde dermed ikke hjemmel til at kræve udlevering af personlige e-mails lagret uden for USA på baggrund af den daværende US Stored Communications Act.[321]

I modsætning til Stored Communications Act indebærer CLOUD Act, at telekommunikationsudbyderne kan pålægges at udlevere personoplysninger på anmodning fra amerikanske myndigheder, selv når disse oplysninger er underlagt bestemmelserne i GDPR.[322] Denne udvidelse af Stored Communications Act kan betragtes som en omgåelse af MLAT, som har til formål at sikre, at dataindsamlingen sker i overensstemmelse med de indgåede aftaler mellem de to lande. Formålet med MLAT er at fremme globalisering og internationalt samarbejde ved at sikre, at efterretningstjenester og politimyndigheder kan håndtere udviklingen af kriminalitet, som i stigende grad udnytter landegrænserne.[323]

CLOUD Act pålægger amerikansk-ejede virksomheder en forpligtelse til at opbevare, føre backup af samt udlevere data om individer, som benytter deres platforme. Derudover fastsætter CLOUD Act

[319] www.justice.gov/criminal/cloud-act-resources
[320] Giles, *Why the Microsoft Ireland Case is Important?*
[321] Ibid.
[322] www.edps.europa.eu/19-07-10-edpb-edps-cloud-act-annex, s. 1
[323] www.commission.europa.eu/mutual-legal-assistance-and-extradition

også, at amerikansk-ejede virksomheder, der er etableret uden for USA, omfattes af dens anvendelsesområde.[324] CLOUD Act indeholder forhold, som kan sikre, at udlevering af personoplysninger sker under hensyn til national lovgivning, hvilket indebærer, at både GDPR og EMRK kan sætte en mulig begrænsning for en sådan overførsel. CLOUD Act giver desuden mulighed for indgåelse af såkaldte Executive Agreements, som har til formål at fremme effektiv efterforskning. Disse aftaler indgås mellem lande og skal danne grundlag for en fælles forståelse og fortolkning af de respektive landes lovgivninger. Ydermere skal der indføres vilkår og krav, som sikrer, at udleveringen kan ske på en mere effektiv måde, særligt hvor de nationale lovgivninger ikke er forenelige.[325]

Anvendelsesområdet for CLOUD Act er beskrevet i artikel 103 (a)(1), hvor det fastslås, at udbydere " *(...) shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.*". Denne artikel udvider USA's ekstraterritorial jurisdiktion, hvorfor vedtagelsen af CLOUD Act er en direkte udvidelse af den forhenværende US Stored Communication Act, som ikke gav hjemmel til indhentelse af personoplysninger i ovennævnte Microsoft-sag. Der blev ydermere indført visse begrænsninger, som kan modvirke udlevering af personoplysninger efter anmodning, såfremt en telekommunikationsudbyder har mistanke om, at den registrerede ikke er amerikansk statsborger.[326] Udleveringen kan desuden begrænses, såfremt den vil skabe en reel konflikt med lovgivningen i den kontraherende stat, hvor udbyderen har sine servere.[327] Denne begrænsning er dog kun relevant, hvis den kvalificerede stat har indgået en Executive Agreement med USA. Det er domstolene, som skal vurdere, om en begrænsning eller afvisning er passende begrundet. Følgende krav skal indgå i en sådan vurdering: Anmodningen må ikke være i strid med lovgivningen i den kvalificerede stat, og den registrerede må hverken være amerikansk statsborger eller have bopæl i USA.[328]

Der er ingen mulighed for at gøre indsigelser efter CLOUD Act, såfremt der ikke foreligger en Executive Agreement med den stat, hvor dataen er lagret, hvorfor amerikanske virksomheder

[324] www.edps.europa.eu/19-07-10-edpb-edps-cloud-act-annex
[325] Wernblad, *Ny lov bremser sagen om Microsofts udlevering af data fra EU*
[326] www.justice.gov/2201-division-v-cloud-act, s. 5
[327] Ibid., s. 5
[328] Ibid., s. 5

etableret i EU ikke kan begrænse eller afvise en sådan anmodning.[329] Ifølge CLOUD Act må amerikanske efterretningstjenesterne kun anmode om personoplysninger, som har direkte forbindelse til en efterforskning af en straffesag, hvis anmodningen har en dommerkendelse. Dommerkendelsen skal være konkret begrundet i faktiske omstændigheder, som skal være specificeret og præciseret i forhold til alvoren. Principperne om nødvendighed og proportionalitet skal ligeledes være opfyldt, hvorfor en dataopbevaring ikke må vare længere end nødvendigt for at fuldende en efterforskning. Endelig må en dommerkendelse ikke udstedes, såfremt der findes andre og mindre indgribende metoder, som kan opnå samme resultat.[330]

GDPR artikel 48 omhandler internationale aftaler som overførselsgrundlag og har følgende ordlyd: "*Enhver dom afsagt af en domstol eller ret og enhver afgørelse truffet af en administrativ myndighed i et tredjeland, der kræver, at en dataansvarlig eller en databehandler overfører eller videregiver personoplysninger, kan kun anerkendes eller håndhæves på nogen måde, hvis den bygger på en international aftale.*". Det kan derfor konstateres, at en overførsel af personoplysninger med henvisning til CLOUD Act ikke kan ske på baggrund af en international aftale i henhold til GDPR, eftersom EU ikke har indgået en Executive Agreement med USA. En sådan overførsel kan derfor ikke anses for at være lovlig i henhold til GDPR artikel 48. Derimod udgør MLAT, som tidligere nævnt, en international aftale og et lovligt overførselsgrundlag, hvorfor USA derigennem kan tilgå data på samme måde som med CLOUD Act. EDPB og EDPS har udtalt, at når der foreligger en international aftale som MLAT, skal virksomheder etableret i EU afvise anmodninger om direkte adgang til personoplysninger, såfremt disse ikke beror på den nævnte aftale og i stedet henvise til MLAT.[331]

Der kan dog forekomme visse situationer, hvor det vil være muligt at overføre data til USA lovligt under henvisning til CLOUD Act. Dette kan forekomme, hvis der foreligger et lovligt behandlingsgrundlag i medfør af GDPR artikel 6 og artikel 49. Eftersom artikel 49, stk. 1, litra a-c og g, ikke er relevante for denne type overførsel, medtages de ikke i vurderingen. GDPR artikel 49, stk. 1, litra d, fastsætter, at en overførsel kun kan finde sted, såfremt den er nødvendig af hensyn til vigtige samfundsinteresser, som imidlertid skal være anerkendt enten i EU-retten eller i en medlemsstats nationale ret, jf. artikel 49, stk. 4.[332] Eftersom overførsler til USA med henvisning til CLOUD Act

[329] www.edps.europa.eu/19-07-10-edpb-edps-cloud-act-annex, s. 3
[330] www.eurojust.europa.eu/the-cloud-act, s. 4
[331] www.edps.europa.eu/19-07-10-edpb-edps-cloud-act-annex, s. 6
[332] Ibid., s. 6-7

ikke hviler på sådanne anerkendte samfundsinteresser, kan de ikke anses for at være i overensstemmelse med artikel 49, stk. 4. GDPR artikel 49, stk. 1, litra e, fastsætter, at en overførsel kan finde sted, såfremt "*overførslen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares.*". EDPB og EDPS har udtalt, at denne nødvendighed kan bero på efterforskning af kriminalitet, men at der kræves en meget tæt sammenhæng mellem dataoverførslen og den konkrete efterforskning. Det er ikke tilstrækkeligt, at oplysningerne muligvis kan medvirke til en efterforskning eller understøtte et retskrav. Dertil må oplysninger heller ikke indsamles til potentielt fremtidigt brug, eftersom dette ville stride mod kravene om formålsbegrænsning og nødvendighed, jf. GDPR artikel 5, stk. 1, litra b.[333] GDPR artikel 49, stk. 1, litra f, kræver, at "*overførslen er nødvendig for at beskytte den registreredes eller andre personers vitale interesser, hvis den registrerede ikke fysisk eller juridisk er i stand til at give samtykke.*". EDPB og EDPS vurderer, at denne bestemmelse i visse ekstraordinære, specifikke og nødvendige situationer kan anvendes til at imødekomme anmodninger under CLOUD Act. Desuden vil bestemmelsen kunne anvendes, såfremt den registrerede ikke er i stand til at give samtykke, og samtidig udgør en fare for andre personers liv.[334] GDPR artikel 49, stk. 1, andet afsnit, oplister en række omfattende kumulative betingelser, som skal være opfyldt, forinden bestemmelsen kan benyttes som et gyldigt overførselsgrundlag. CLOUD Act tilsigter hemmeligholdelse af indsamling, hvorfor den registrerede ikke bliver underrettet om indsamlingen, hvilket strider mod underretningskravet i bestemmelsen. Efter EDPB og EDPS' opfattelse vil det ikke være muligt at anvende GDPR artikel 49, stk. 1, andet afsnit, eftersom der ikke kan indføres passende foranstaltninger som underretning i praksis. EDPB og EDPS understreger dog, at såfremt der allerede foreligger andre overførselsgrundlag såsom MLAT, bør sådanne anvendes som overførselsgrundlag frem for undtagelsesbestemmelserne i GDPR artikel 49.[335]

MLAT i relation til CLOUD Act

Såfremt CLOUD Act ikke har nogen bindende retsvirkning over for amerikanske virksomheder etableret i EU, kan personoplysninger med henblik på strafferetlig efterforskning i stedet udveksles gennem MLAT. MLAT er en international aftale, der skal fremme et retligt samarbejde mellem USA og EU-medlemsstaterne, og som sikrer en vis harmonisering mellem de respektive retssystemer. De bruges til at håndtere grænseoverskridende anmodninger om udlevering af bevismaterialer og hjælper med at opretholde de nødvendige retsgarantier, selvom de oftest kritiseres for at være langsomme og

[333] www.edps.europa.eu/19-07-10-edpb-edps-cloud-act-annex, s. 6
[334] Ibid., s. 7
[335] Ibid., s. 3

bureaukratiske.[336] I dette afsnit vil det bliver undersøgt, om MLAT fortsat udgør et tilstrækkeligt grundlag for udvekslingen af beviser i strafferetlig efterforskninger eller om deres begrænsninger og bureaukratiske karakter burde have været adresseret i højere grad, især i forhold til de mere direkte mekanismer, som CLOUD Act tilbyder.

Som tidligere nævnt er MLAT en international aftale konciperet mellem EU og USA, som danner grundlag for overførsel af data i forbindelse med efterforskningsmateriale vedrørende kriminalitet. USA's vedtagelse af CLOUD Act giver imidlertid amerikanske myndigheder adgang til at kræve udlevering af data, der opbevares af amerikansk-ejede virksomheder beliggende uden for USA. Denne adgang tilsidesætter MLAT, som ellers skulle udgøre det retlige overførselsgrundlag. Gennem CLOUD Act bliver det muligt at omgå de krav, som følger af MLAT, herunder begrænsninger vedrørende opbevaring og anvendelse af data, jf. MLAT artikel 9.[337] Ydermere omgås kravet i MLAT artikel 5, som forudsætter, at der foretages en samlet vurdering af nødvendigheden i overensstemmelse med retsreglerne i den stat, hvorfra oplysningerne kræves udleveret.[338]

Problemet ved CLOUD Act knytter sig grundlæggende til opbevaringen og brugen af data samt flere centrale databeskyttelsesprincipper. Som tidligere nævnt er amerikansk lovgivning og EU-retten ikke samhørig, eftersom metode, fortolkning, generelle forpligtelser og rettigheder ikke tildeles samme betydning. Brugen af data og dertilhørende begrænsninger er ikke ækvivalente med de databeskyttelsesprincipper, som gælder i EU, hvorfor omgåelse gennem CLOUD Act udgør et direkte brud på den aftale, som EU og USA har indgået. Selvom USA stadig anerkender MLAT som gældende mellem EU og USA, understøtter USA samtidig, at CLOUD Act fremmer amerikanske interesser og reducerer de processuelle byrder, som følger af MLAT.[339]

CLOUD Act er endvidere udformet for også at støtte udenlandske myndigheder, som vælger at indgå en Executive Agreement med USA, hvilket kan styrke opfattelsen af, at USA's tidligere anerkendelse af MLAT indirekte er ved at blive trukket tilbage. USA opfatter ikke implementeringen af CLOUD Act som en tilsidesættelse af MLAT, men derimod som et supplement, der har til formål at fremme en mere effektiv og optimeret adgang til elektroniske beviser på tværs af jurisdiktioner.[340] Denne tilgang følger EU's egen ambition og ønske om en mere effektiv bekæmpelse af kriminelles brug af

[336] Mignon, *The CLOUD Act: Unveiling European Powerlessness*
[337] www.eur-lex.europa.eu/agreement-on-mutual-legal-assistence-between-eu-and-usa, artikel 9
[338] Ibid., artikel 5
[339] www.justice.gov/frequently-asked-questions-cloud-act, s. 1
[340] Wood m.fl., *The CLOUD Act and Transatlantic Trust*

digitale platforme.[341] Selvom EU og USA deler samme ønske om hurtigere og mere effektiv dataudveksling, må implementeringen af CLOUD Act stadig betragtes som en omgåelse, eftersom udleveringen af data beror på en amerikansk dommerkendelse, som ikke anerkendes i EU, jf. GDPR artikel 48. MLAT artikel 17 fastsætter muligheden for revidering af aftalen, hvorfor aftalen skal genoptages til forhandling for at følge med den teknologiske og retlige udvikling, navnlig hvad angår overførsel af elektroniske beviser.[342] Artikel 17 indeholder yderligere krav til aftalens praktiske gennemførsel, som tidligere blev gennemgået af EU og USA i perioden 2015-2016. I denne gennemgang blev følgende elementer nævnt, som skulle optimeres for at følge med den teknologiske udvikling: "*The review process also resulted in recommendations to improve the practical functioning of the EU-US mutual legal assistance relationship, including on better sharing of knowledge among practitioners about each others' laws and processes and to make better use of technology to speed up the transmission of requests and evidence and general communications.*".[343] På baggrund af ovenstående anbefalinger rejses spørgsmålet om, hvorfor CLOUD Act blev vedtaget frem for at revidere MLAT, eftersom de to instrumenter tilsyneladende har samme formål.

I medfør af MLAT artikel 14 er det muligt for USA og et EU-medlemsland at indgå bilaterale aftaler, forudsat at disse er i overensstemmelse med bestemmelserne i MLAT.[344] Efter artikel 14 kan det potentielt være muligt at anvende CLOUD Act gennem Executive Agreements, såfremt aftalerne er i overensstemmelse med MLAT. Problematikken er imidlertid, at CLOUD Act ikke indeholder databeskyttelsesbestemmelser, som er forenelige eller tilstrækkelige i forhold til EU-retten. Dette forhold har imidlertid potentiale for at blive afhjulpet, eftersom CLOUD Act forudsætter, at amerikanske myndigheder respekterer lovgivningen i de lande, som har indgået en Executive Agreement med USA. Formålet med en sådan aftale er at fjerne begrænsninger og restriktioner i den kontraherende stat for at sikre en flydende dataudveksling, og denne afskaffelse skal aftales indbyrdes mellem USA og den kontraherende stat.[345] Endvidere tager Executive Agreements udelukkende afsæt i national lovgivning, men det forbliver stadig uklart, om MLAT artikel 14 mellem EU og USA også skal anerkendes i denne sammenhæng, eftersom MLAT ikke udgør en national lovgivning. Artikel 14 fastsætter, at en bilateral aftale mellem et medlemsland og USA kun kan indgås, såfremt aftalen er forenelig med MLAT. Spørgsmålet er derfor, om det efter MLAT's betingelser er muligt eller tilstrækkeligt at indgå en aftale gennem en Executive Agreement, såfremt der ikke tages stilling til

[341] www.eur-lex.europa.eu/com-(2022)-230-18-5-2022
[342] www.eur-lex.europa.eu/agreement-on-mutual-legal-assistence-between-eu-and-usa, artikel 17
[343] www.eur-lex.europa.eu/summary-agreement-with-the-united-states-on-mutual-legal-assistance
[344] www.eur-lex.europa.eu/agreement-on-mutual-legal-assistence-between-eu-and-usa, artikel 14
[345] www.justice.gov/frequently-asked-questions-cloud-act, s. 2

allerede eksisterende aftaler som MLAT. Indgåelsen af Executive Agreement mellem et EU-medlemsland og USA indebærer yderligere komplikationer, og formålet med CLOUD Act er som udgangspunkt at fjerne begrænsninger og restriktioner. Dette kan således medføre, at MLAT-aftalen, som det pågældende medlemsland er part i, reelt tilsidesættes for at muliggøre en Executive Agreement.

På baggrund af ovenstående kan det konkluderes, at CLOUD Act ikke kan anses som forenelig med EU-retten, eftersom den tilsidesætter flere bestemmelser i MLAT. Derudover anvender CLOUD Act en ekstraterritorial rækkevidde uden nogen form for international anerkendelse eller et EU-retligt supplement, der kunne legitimere en sådan anvendelse. Den nuværende udformning af CLOUD Act bygger ikke på en international aftale mellem USA og EU. Dermed må CLOUD Act anses som ensidigt vedtaget amerikansk national lovgivning. Som følge heraf har den ingen direkte retsvirkning i EU-retten, hvorfor den ikke uden videre kan pålægge virksomheder i EU forpligtelser.[346] Selvom CLOUD Act ikke har en direkte retsvirkning i EU, kan en gennemgang og udvikling af den udgøre en vigtig rolle i bekæmpelsen af international kriminalitet. CLOUD Act vil med stor sandsynlighed få fremtidig relevans, eftersom der siden juni 2019 har været forhandlinger om en harmonisering med EU-retten.[347] Dette harmoniserer med EU's overordnede målsætning om at fremme effektiv grænseoverskridende adgang til elektroniske beviser i forbindelse med kriminalitetsbekæmpelse, som tidligere beskrevet.

11.3 KOMBIT

Faktum og spørgsmål

DT svarede den 29. marts 2022 på en forespørgsel fra KOMBIT vedrørende, hvorvidt en tredjelandsoverførsel skulle anses som utilsigtet, såfremt databehandleraftalen medførte, at databehandleren ville overgive personoplysninger til tredjelandes offentlige myndigheder på baggrund af afgørelser. AWS, som var en af KOMBIT's databehandlere, var omfattet af CLOUD Act og ville derfor kunne modtage anmodninger fra myndighederne i USA vedrørende udlevering af personoplysninger. I databehandleraftalen var ordlyden af det omtalte som følgende: "*Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except […] as necessary to comply with the law or binding order of a governmental body.*". Dermed

[346] www.justice.gov/frequently-asked-questions-cloud-act, s. 7-8
[347] Mignon, *The CLOUD Act: Unveiling European Powerlessness*

indeholder databehandleraftalen en instruks, som muliggør overførsel baseret på myndighedsanmodninger som ved CLOUD Act.[348]

KOMBIT's forespørgsel var på baggrund af den 3. udgave af vejledningen fra DT vedrørende overførsel til tredjelande fra juli 2021. I denne udgave blev det konstateret gennem eksempel 10 om myndighedsanmodninger fra tredjelande, at utilsigtede tredjelandsoverførsler ikke var omfattet af GDPR kapitel V. I dette eksempel blev det fastlagt, at imødekommelsen af en myndighedsanmodning fra tredjelande, såfremt det var i strid med databehandleraftalen, udgjorde en utilsigtet overførsel.[349] Dette eksempel kan ligeledes findes i DT's 4. udgave om overførsel til tredjelande fra april 2024.[350] Derudover kom forespørgslen også på baggrund af DT's vejledning om anvendelsen af cloud fra marts 2022. I afsnit 3.6 i eksempel 14 beskriver DT, at den dataansvarlige i denne kontekst skal fokusere på en tilstrækkelig behandlingssikkerhed efter GDPR artikel 32, som medfører, at de pågældende personoplysninger ikke utilsigtet kan komme i andres besiddelse. Såfremt databehandleren i strid med databehandleraftalen udleverer personoplysninger på baggrund af en myndighedsanmodning fra et tredjeland, anses det som et brud på persondatasikkerheden.[351] KOMBIT's endelige spørgsmål var dermed som følgende: "*Kan Datatilsynet be- eller afkræfte, om der vil være tale om en utilsigtet overførsel, hvis muligheden for overførsel af personoplysninger til myndigheder, herunder myndigheder i tredjelande, fremgår af databehandlerens standarddatabehandleraftale, og om situationen skal behandles efter reglerne om passende behandlingssikkerhed, jf. afsnit 3.6 i Datatilsynets vejledning om cloud?*".[352]

DT nævner endvidere i vejledningen om tredjelandsoverførsel, at GDPR finder anvendelse, såfremt det er en tilsigtet tredjelandsoverførsel. Dette betyder, at såfremt en databehandler handler i overensstemmelse med databehandleraftalen ved overførsel af personoplysninger til tredjelandsmyndigheder på baggrund af anmodning, vil overførslen omfattes af GDPR. Under disse omstændigheder kræves der en behandlingshjemmel og et overførselsgrundlag i henholdsvis GDPR artikel 6 og kapitel V. DT understreger i vejledningen, at en myndighedsanmodning ikke i sig selv kan konstituere et overførselsgrundlag.[353]

[348] www.datatilsynet.dk/vedrørende-tilsigtede-eller-utilsigtede-overførsler-til-tredjelande
[349] Ibid.
[350] www.datatilsynet.dk/Vejledning-om-overførsel-til-tredjelande, s. 12
[351] www.datatilsynet.dk/Vejledning-om-cloud, s. 30
[352] www.datatilsynet.dk/vedrørende-tilsigtede-eller-utilsigtede-overførsler-til-tredjelande
[353] www.datatilsynet.dk/Vejledning-om-overførsel-til-tredjelande, s. 26

Datatilsynets besvarelse

DT fastlagde indledningsvis, at en databehandlers behandling af personoplysninger kun tillades, såfremt det sker på baggrund af den dataansvarliges instruks. Dette inkluderer tredjelandsoverførsler, medmindre databehandleren er omfattet af national lovgivning eller EU-ret, hvor dette kræves, jf. GDPR artikel 28, stk. 3, litra a. En potentiel videregivelse af behandlede personoplysningerne fra AWS ville være i overensstemmelse med den tidligere nævnte ordlyd i databehandleraftalen. DT vurderede derfor, at der var tale om en tilsigtet tredjelandsoverførsel. Eftersom de tidligere eksempler i DT's vejledninger omhandlede databehandling i strid med databehandleraftaler, var de ikke tilsvarende de pågældende omstændigheder for KOMBIT. Ud fra DT's tidligere nævnte vejledninger, blev det konstateret, at GDPR dermed fandt anvendelse. De dataansvarlige skulle derfor sikre overholdelse af GDPR, såfremt AWS ville modtage en myndighedsanmodning.[354]

DT forklarede endvidere, at disse myndighedsanmodninger fra tredjelande kun håndhæves eller anerkendes, såfremt afgørelsen er baseret på en international aftale mellem EU eller EU-/EØS-lande og det pågældende tredjeland. Som i DT's vejledning blev der ligeledes lagt vægt på, at disse afgørelser ikke konstituerer et overførselsgrundlag. DT anbefalede derudover, at en uddybelse af lovmæssige forhold vedrørende tredjelandsoverførsel på baggrund af CLOUD Act kunne findes i EDPS og EDPB's fælles udtalelse af den 10. juli 2019, jf. kapitel 11.2.[355]

DT nævner afslutningsvis, at såfremt en dataansvarlig vælger at anvende databehandlere, som kan omfattes af CLOUD Act-anmodninger, skal den dataansvarlige fokusere på tre forhold: Som det første anbefaler DT, at den dataansvarlige sikrer sig, at databehandleren kan stille fornødne garantier for overholdelse af tilstrækkelig databeskyttelse og behandling, jf. GDPR artikel 28, stk. 1. Det andet forhold omhandler, at tilstrækkelig behandlingssikkerhed overholdes af den dataansvarlige. Dette inkluderer, at personoplysninger ikke utilsigtet overføres til andre uautoriserede parter. Den dataansvarlige skal dermed foretage en risikovurdering af muligheden for databehandlerens efterlevelse af en myndighedsanmodning på trods af, at denne imødekommelse er i strid med databehandleraftalen, jf. GDPR artikel 28, stk. 3, litra c, og artikel 32, stk. 1. Det tredje og sidste forhold indebærer indførelsen af regelmæssige tilsyn af den dataansvarlige over for databehandleren, jf. GDPR artikel 5, stk. 2. Dette kan udføres gennem revisioner og inspektioner, jf. GDPR artikel 28,

[354] www.datatilsynet.dk/vedrørende-tilsigtede-eller-utilsigtede-overførsler-til-tredjelande
[355] Ibid.

stk. 3, litra h. Såfremt myndighedsanmodninger imødekommes i strid med databehandleraftalen, er den dataansvarlige forpligtet til at standse dette.[356]

Praktiske anbefalinger

Såfremt der forekommer en situation, hvor der kan opstå tvivl med hensyn til, hvorvidt en databehandler skal imødekomme en myndighedsanmodning, bør den dataansvarlige formentligt afklare dette på forhånd. Henrik Udsen mener, at GDPR artikel 28, stk. 1, formentligt medfører, at den dataansvarlige forpligtes til at afklare databehandlerens hensigt i forbindelse med modtagelsen af en potentiel myndighedsanmodning baseret på CLOUD Act. Dette gælder især, såfremt databehandlerens vilkår er med til at skabe tvivl vedrørende imødekommelse af myndighedsanmodninger.[357] Grundet ovenstående antages det, at databehandleraftaler bør være klare og præcise i deres indhold, således der ikke forekommer tvivl vedrørende en databehandlers ageren under omstændigheder omhandlende CLOUD Act-anmodninger. En præcis ordlyd i databehandleraftalen findes væsentlig, eftersom databehandleren kun vil ifalde erstatningsansvar, såfremt databehandleren har handlet i strid med instrukser eller ikke opfyldt forpligtelser i GDPR, jf. GDPR artikel 82, stk. 2. Dermed kan en præcis ordlyd i databehandleraftalen være af væsentlig betydning, eftersom dette kan have indflydelse på erstatningsansvaret. Det antages i denne sammenhæng, at databehandlere potentielt kan undgå erstatningsansvar, såfremt der eksisterer fortolkningstvivl vedrørende imødekommelse af CLOUD Act-anmodninger.

11.4 Delkonklusion

Ud fra ovenstående kan det konkluderes, at CLOUD Act muliggør udlevering af personoplysninger til amerikanske myndigheder fra virksomheder i EU, såfremt virksomhederne er amerikansk-ejede. CLOUD Act indeholder imidlertid forhold, som sikrer, at der samtidig skal tages hensyn til udenlandsk national lovgivning, hvoraf dette muliggør introducering af begrænsninger fra GDPR og EMRK. På trods af dette kan EU-databehandlere ufrivilligt ende i en jurisdiktionskonflikt mellem EU og USA's lovgivningen, eftersom modstridende krav i denne sammenhæng kan fremkomme. Det konkluderes yderligere, at amerikanske myndighedsanmodninger skal bero på MLAT for lovligt at kunne anvende overførselsgrundlaget i GDPR artikel 48. Endvidere findes der komplikationer vedrørende anvendelsen af undtagelsesbestemmelserne i GDPR artikel 49. I henhold til GDPR artikel

[356] www.datatilsynet.dk/vedrørende-tilsigtede-eller-utilsigtede-overførsler-til-tredjelande
[357] Udsen, *Databeskyttelsesret*, s. 106

49, litra d, konkluderes det, at overførselsgrundlaget i undtagelsen ikke kan anvendes i relation til CLOUD Act, eftersom USA's væsentlige samfundsinteresser ikke anerkendes af EU-retten, jf GDPR artikel 49, stk. 4. I henhold til GDPR artikel 49, litra e, konkluderes det, at der kræves en væsentlig sammenhæng mellem dataoverførslen og efterforskningen, hvilket dermed medfører strenge krav for anvendelse. I henhold til GDPR artikel 49, litra f, konkluderes det, at dette overførselsgrundlag udelukkende bør anvendes i ekstraordinære nødstilfælde. I henhold til GDPR artikel 49, stk. 1, andet afsnit, konkluderes det, at denne undtagelse ikke kan anvendes, eftersom underretningskravet ikke kan opfyldes i praksis. Afslutningsvis konkluderes det i henhold til undtagelsesbestemmelserne i GDPR artikel 49, at andre overførselsgrundlag bør prioriteres før anvendelse af bestemmelserne, herunder MLAT.

Ud fra ovenstående konkluderes det yderligere, at CLOUD Act ikke er forenelig med EU-retten grundet tilsidesættelsen af MLAT's bestemmelser. CLOUD Act har således ingen retsvirkning i EU og kan dermed ikke kræve udlevering af personoplysninger fra virksomheder i medlemsstaterne uden videre. CLOUD Act muliggør omgåelse af en række bestemmelser i MLAT, hvilket udgør et direkte brud på den aftale, som EU og USA har indgået. USA anser imidlertid CLOUD Act som et effektivt instrument, men der kan argumenteres for, at det er en indirekte omgåelse af MLAT. De igangværende forhandlinger om en harmonisering med EU-retten i henhold til EU's ambitioner om at fremme grænseoverskridende kriminalitetsbekæmpelse indikerer imidlertid, at CLOUD Act kan blive relevant i fremtiden i et EU-retligt perspektiv.

Ud fra retspraksis gennem KOMBIT-sagen kan det konkluderes, at GDPR finder anvendelse, såfremt imødekommelse af CLOUD Act-anmodninger er i overensstemmelse med databehandleraftalen. Dertil blev det fastlagt, at anmodningerne kun skal imødekommes, såfremt de har grundlag i internationale aftaler mellem parternes lande eller tredjelandet og EU. Derudover blev det konstateret, at en dataansvarlig skal forsikre sig, at databehandleren kan sikre tilstrækkelig databeskyttelse. Dertil at den dataansvarlige sikrer tilstrækkelig behandlingssikkerhed, herunder udarbejdelse af relevante risikovurderinger. Endvidere skal den dataansvarlige foretage regelmæssigt tilsyn i forbindelse med databehandleren. Såfremt der forekommer en imødekommelse af CLOUD Act-anmodninger på trods af, at dette er i strid med databehandleraftalen, skal den dataansvarlige standse dette. Afslutningsvis udledes det gennem juridisk litteratur og GDPR, at dataansvarlige bør afklare fortolkningstvivl i databehandleraftalen på forhånd. Dertil at databehandleraftalen bør være præcis og klar i ordlyden af indholdet, eftersom dette kan have betydning for fordelingen af erstatningsansvar mellem dataansvarlig og databehandler, jf. GDPR artikel 28, stk. 1, og 82, stk. 2.

12 Fremtidige forhold i relation til tredjelandsoverførsel til USA

Afslutningsvis findes det relevant på baggrund af analysen at vurdere og diskutere de forventninger, som eksisterer ved en potentiel Schrems III. I dette kapitel vil der inddrages udtalelser fra diverse aktører med henblik på at diskutere fremtiden for dataoverførsel til USA fra EU. Derudover vil omstændighederne belyses i et praktisk perspektiv med henblik på at fremlægge anbefalinger i relation til udarbejdelse af en strategi, såfremt DPF ugyldiggøres. Dertil vil de pågældende konsekvenser for virksomheder klarlægges under samme forhold.

12.1 Forventninger og fremtidige forhold i relation til en mulig Schrems III

Alisa Vekeman, som på daværende tidspunkt var policy officer i EUK og forhandler i forbindelse med DPF, udtalte i maj 2022 ved en konference, at dataoverførselsaftalen med overvældende sandsynlighed ville blive bragt for EUD. Dertil forklarede Vekeman, at det ikke kan vides, hvorvidt aftalen bliver ugyldiggjort eller ej.[358] På daværende tidspunkt var DPF ikke trådt i kraft, og dermed var indholdet af aftalen endnu ukendt, men usikkerhederne vedrørende aftalens tilstrækkelighed var allerede tilstedeværende. Selve forhandlerne for aftalen er dermed tvivlende på DPF's gyldighed på længere sigt, hvilket kun bestyrker den generelle usikkerhed forbundet med aftalen og tredjelandsoverførsel til USA. Det skal bemærkes i denne kontekst, at det kun er EUK eller EUD, som kan ophæve eller suspendere aftalen, jf. GDPR artikel 45, stk. 5, samt Schrems I og II. Dette medfører, at DPF's gyldighed kan være vanskelig at forudse, særligt grundet USA's lovgivning, praksis og regeringsskifte, eftersom DPF blev dannet under Biden-administrationen. Imidlertid kan der argumenteres for, at regeringsskiftet er af mindre betydning, eftersom myndighederne i USA omgående prioriterede dannelse af en ny dataoverførselsaftale under den forrige Trump-administration på baggrund af ugyldiggørelsen ved Schrems II. Dertil mener flere aktører, at den økonomiske og politiske betydning for både USA og EU er for væsentlig til, at DPF's funktionalitet afhænger af et regeringsskifte.[359]

Til samme konference forholdte Max Schrems sig kritisk til aftalen i sin helhed og beskrev databehandlingen i USA som *unødvendig og ikke-proportionel*.[360] Schrems vurderer her, at principperne om nødvendighed og proportionalitet ikke sikres ved DPF på trods af deres medtagelse

[358] Olifent, *Skepsis over data-aftale vokser: Topforhandler vil ikke lægge hovedet på Schrems III-blokken*
[359] LaCasse, *European Commission report reviews progress of EU-US DPF*
[360] Olifent, *Skepsis over data-aftale vokser: Topforhandler vil ikke lægge hovedet på Schrems III-blokken*

i EO 14086 og hovedfokus på disse i forhandlingerne.[361] Der kan argumenteres for, at Schrems ikke er overbevist om, at principperne vil blive anvendt på en tilstrækkelig og overensstemmende måde i henhold til EU-retten, jf. kapitel 8.1 og 9.1.1. Henrik Udsen deler flere af de samme bekymringer som Schrems med hensyn til en generel skepticisme i forbindelse med DPF. Udsens skepticisme er begrundet i den manglende forandring af USA's lovgivning, hvilket en udstedelse af et afhjælpende dekret dermed ikke konstituerer.[362] Der bliver i denne henseende argumenteret for, at fundamentet for DPF potentielt ikke er tilstrækkeligt i en lovgivningsmæssig sammenhæng. Der kan argumenteres for, at en dataoverførselsaftale mellem USA og EU kræver en ændring af den egentlige lovgivning som FISA 702. Begrænsninger og garantier bør efter denne optik ikke oprettes gennem dekreter, men derimod gennem en lovgivningsmæssig vedtagelse af Kongressen. Dermed vil fundamentet for en dataoverførselsaftale være mere solidt, eftersom dekreter kan afskaffes eller ændres uden Kongressens involvering, jf. kapitel 8.

Vekeman er uenig i ovenstående kritik vedrørende anvendelsen af dekret som fundament for DPF. Her mener Vekeman, at fokus skal være på resultatet af aftalen og ikke midlet, som anvendes til at opnå dette. Ifølge Vekeman findes begrundelsen for dette i, at en betydelig mængde af sikkerhedslovgivningen i USA er dannet af dekreter, og deres bindende effekt kan derfor ikke bestrides. Dertil at den amerikanske præsident besidder en omfattende mængde af beføjelser, herunder udstedelse af dekreter.[363] Der kan dog i denne sammenhæng argumenteres for, at en fremtidig eventuel ændring eller ophævelse af altafgørende dekreter også uden videre kan forekomme grundet den amerikanske præsidents beføjelser. Udgangspunktet på nuværende tidspunkt er imidlertid, at dette ikke er realiseret, og dekreters lovgivningsmæssige soliditet kan være af større betydning, end kritikere mener. Trumps tidligere udtalelser fra 2025 vedrørende potentielle fremtidige ophævelser af sikkerhedsdekreter, herunder EO 14086, skaber dog usikkerhed for dekretets fremtid, jf. kapitel 9.1. Såfremt dekretet ophæves, vil fundamentet for DPF forsvinde, og dermed vil aftalen med al sandsynlighed ugyldiggøres i fremtiden.

Såfremt den nuværende dataoverførselsaftale mellem USA og EU ugyldiggøres, kan dette have væsentlige konsekvenser for fremtidige aftaler ifølge Udsen og Vekeman. I denne sammenhæng udtaler begge aktører, at det er svært at forestille sig, at en ny aftale kan etableres efterfølgende. Dette begrundes i, at ugyldiggørelsen vil medføre, at EUD vil fremsætte endnu strengere og omfattende

[361] Olifent, *Skepsis over data-aftale vokser: Topforhandler vil ikke lægge hovedet på Schrems III-blokken*
[362] Ibid.
[363] Ibid.

krav til en ny dataoverførselsaftale, herunder specifikke krav til USA's retssystem.[364] Det skal bemærkes, at sagen endnu ikke er fremlagt for EUD, hvilket dermed på nuværende tidspunkt argumenterer mod denne potentielle situations tilstedeværelse inden for en nær fremtid. Baseret på de omtalte aktørers udtalelser, den generelle usikkerhed forbundet med DPF samt USA's nuværende regerings handlinger, findes denne fremtid dog ikke usandsynlig. En Schrems III-sag vil med al sandsynlighed før eller senere blive fremlagt for EUD, hvorefter der skal tages stilling til DPF. Grundet tidligere udledte problematikker og uoverensstemmelser i forbindelse med implementeringen af EO 14086 i praksis, vurderes det ligeledes, at en ugyldiggørelse af DPF kan være aktuel, jf. kapitel 9.2. Såfremt dette forekommer, vil fremtiden for dataoverførsel mellem USA og EU muligvis ikke involvere et overførselsgrundlag i form af en tilstrækkelighedsafgørelse, eftersom dette anses som værende usandsynligt. Fremtiden for dataoverførsel mellem USA og EU vil dermed ændre sig væsentligt, og der må i denne kontekst anvendes alternative overførselsgrundlag fra GDPR artikel 46.

12.2 Praktiske anbefalinger og konsekvenser for virksomheder

På baggrund af specialets analyse og vurdering af de foreliggende omstændigheder, kan det antages, at kritikpunkterne, som blev fremført i Schrems II, ikke er blevet udbedret tilstrækkeligt, jf. kapitel 9.2. I fremtiden kan det dermed være aktuelt at anvende SCC'er som et alternativt overførselsgrundlag frem for en tilstrækkelighedsafgørelse, jf. kapitel 10 og 12.1. Såfremt det antages, at DPF ugyldiggøres, vil SCC'er udgøre det primære overførselsgrundlag af personoplysninger til USA. Selvom en potentiel ugyldiggørelse af DPF ikke direkte vil påvirke brugen af SCC'er, vil ugyldiggørelsen stadig besværliggøre processen, hvorpå SCC'erne bliver udarbejdet. Processen besværliggøres, eftersom de tidligere eksisterende garantier og begrænsninger dermed vurderes til ikke opfylde kravene fremsat i eksempelvis EUC artikel 47, hvilket medfører strengere krav til supplerende foranstaltninger, jf. 10.3. USA vil i denne sammenhæng kategoriseres som et usikkert tredjeland, hvorfor lovgivningen og praksis skal vurderes for hver individuel overførsel. Virksomheder, som er afhængige af den frie datastrøm mellem USA og EU, vil blive tvunget til at allokere ressourcer til henholdsvis forbedring af tekniske foranstaltninger samt vurdering af den amerikanske lovgivning, eftersom SCC'er løbende skal revideres og holdes ajourførte.[365] Eftersom SCC'er skal specificeres for hver af virksomhedens individuelle overførsler, skal der udarbejdes en

[364] Olifent, *Skepsis over data-aftale vokser: Topforhandler vil ikke lægge hovedet på Schrems III-blokken*
[365] Navarro, *The legal uncertainty facing EU-US Data Transfers*

separat SCC til hver overførsel, hvorfor det kan argumenteres for at denne proces vil blive omfattende og omkostningstung for virksomheder etableret i EU.

Som det blev fastslået tidligere, er tilstrækkelighedsafgørelsen stadig gældende, hvorfor den fortsat kan anvendes som det primære overførselsgrundlag. På baggrund af usikkerhederne vedrørende DPF, anbefales det, at virksomheder allerede inden en potentiel ugyldiggørelse af DPF udarbejder en strategi for at få kendskab til organisationens overførsler, tilføjer supplerende foranstaltninger og tager processuelle forbehold. En eventuel foranstaltning er at initiere brugen af europæiske databehandlere eller cloud-udbydere, men problematikken er, om der i realiteten stadig sker en overførsel af personoplysninger til USA. De fleste programmer, som benyttes af den offentlige sektor og europæiske selskaber til at drive virksomhed, er forbundet til store amerikanske tech-virksomheder, hvor der automatisk vil ske en overførsel til USA. Det vil derfor være svært at løsrive sig fra anvendelsen af deres online tjenesteydelser, såfremt det overhovedet er muligt rent logistisk.[366] Selvom det kan blive byrdefuldt for europæiske virksomheder og myndigheder, anbefales det at påbegynde en undersøgelse af alternative løsninger, som kan opfylde de samme behov som dem, de amerikanske tech-giganter tilbyder.

Udarbejdelsen af en exitstrategi findes relevant, eftersom der ved Schrems II-afgørelsen ingen overgangsfase var. På trods af dette udviste de forskellige datatilsynsmyndigheder imidlertid en vis tidsmæssig tolerance for omstruktureringen.[367] Tolerancen efter Schrems II-afgørelsen beror sandsynligvis på, at der efter Schrems I-afgørelsen var en overgangsfase, hvorfor virksomheder havde forventet, at tilsvarende ville ske.[368] Den norske datatilsynsmyndighed mener desuden heller ikke, at der vil forekomme en overgangsfase, såfremt DPF skulle ugyldiggøres.[369] På baggrund af den sidste ugyldiggørelse kan det antages, at datatilsynsmyndighederne vil udvise mindre tolerance, eftersom EDPB udgav en vejledning om supplerende foranstaltninger kort tid efter Schrems II, jf. kapitel 10.2. Denne antagelse beror på, at der på nuværende tidspunkt foreligger vejledninger om, hvordan en overførsel til USA gennem SCC'er kan medføre tilstrækkelig databeskyttelse.

Det vil afslutningsvist anbefales, at virksomheder påbegynder sin brug af SCC'er, klarlægger ens datastrømme, udarbejder en Transfer Impact Assessment (TIA)[370] og på baggrund af den fastsætter

[366] Ravn-Højgaard m.fl., *Tænketank: Big tech styrer vores digitale infrastruktur. Det truer vores sikkerhed og demokrati*
[367] www.datatilsynet.dk/anbefalinger-efter-schrems-ii
[368] www.morganlewis.com/no-grace-period-after-invalidation-of-eu-us-privacy-shield-in-schrems-ii
[369] www.datatilsynet.no/informasjon-om-overføringer-til-usa
[370] *Risiko- og konsekvensvurdering*

supplerende foranstaltninger, som kan sikre et tilstrækkeligt databeskyttelsesniveau. Desuden findes det relevant at undersøge alternativer til de amerikanske cloud- og telekommunikationsudbyderne, men der hersker fortsat tvivl om, hvorvidt dette overhovedet er muligt på nuværende tidspunkt.

13 Konklusion

Første del af konklusionen vil besvare, hvorledes begrænsningerne og garantierne i EO 14086 sikrer en tilstrækkelig databeskyttelse i forbindelse med lovlig tredjelandsoverførsel til USA. Ud fra ovenstående kan det konkluderes, at der kan argumenteres for, at begrænsningerne og garantierne i EO 14086 hverken kan anses som forudsigelige, klare eller præcise i praksis grundet det lovgivningsmæssige grundlag, som EO 14086 er stiftet gennem. Dette skyldes, at USA's præsident har beføjelse til at ophæve eller ændre dekretet til enhver tid. Endvidere kan CLPO og DPRC's stiftelse gennem dekretet kritiseres ud fra samme betragtning. EO 14086 kan yderligere kritiseres for ikke at forbyde masseindsamling af personoplysninger samt det manglende krav vedrørende offentliggørelse af legitime nationale sikkerhedshensyn. Dertil konkluderes det, at disse hensyn anerkendes, men at de registreredes grundlæggende rettigheder og friheder i relation til dette ikke må krænkes. Det kan ydermere kritiseres, at PCLOB og CLPO kan omgås under bestemte omstændigheder, hvilket henvender sig til valideret efterretningsprioriteter og skjulte handlinger. Derudover anerkendes USA's fortolkning af proportionalitetsprincippet som overensstemmende med EU-rettens fortolkning. Imidlertid findes USA's fortolkning af nødvendighedsprincippet kritisabel grundet en uoverensstemmende karakter ved sammenholdelse af EU-rettens fortolkning, eftersom de ikke indebærer samme beskyttelse.

Vedrørende PCLOB konkluderes det, at organet kan kritiseres grundet den nuværende og længerevarende mangel på beslutningsdygtighed. I denne sammenhæng kan der argumenteres for, at dette også har betydning for CLPO og DPRC, eftersom PCLOB har til opgave at udføre tilsyn i forbindelse med disse organer. Endvidere kan PCLOB kritiseres for organets manglende gennemsigtighed og uafhængighed grundet afskedigelser med medlemmer uden offentlig og relevant begrundelse. Imidlertid anerkendes CLPO og DPRC's beføjelse til at afsige afgørelser med bindende virkning, men organerne kan derimod kritiseres for en utilstrækkelig uafhængighed, eftersom de har et tilhørsforhold til den udøvende magt, jf. Schrems II, præmis 195 og 196. Det konkluderes yderligere, at DPRC's manglende indberetningspligt samt tilsyn i forbindelse med den udøvende magt anerkendes. Dertil at organets dommere sikres mod uretmæssig afskedigelse. Imidlertid kritiseres DPRC's for manglende begrundelse for afgørelser til den pågældende klager. Dertil kritiseres DPRC's manglende appelmulighed, gennemsigtighed samt omfattende anvendelse af standardsvar. Derudover kan der argumenteres for, at DPRC ikke opfylder kravet om adgang til et effektivt retsmiddel grundet ovenstående kritikpunkter, jf. EUC artikel 47.

Denne del af konklusionen vil besvare, hvornår og hvordan SCC'er gennem supplerende foranstaltninger kan anvendes som overførselsgrundlag på trods af USA's lovgivning og praksis. I forbindelse hermed kan det konkluderes ud fra EDPB's retningslinjer, at det anbefales, at der udformes en oversigt, som vedrører alle relevante overførsler. Derudover anbefales det, at det relevante tredjelands lovgivning og praksis vurderes, herunder muligheden for retshåndhævelse og klageindgivelse. På baggrund af denne vurdering skal der indføres supplerende foranstaltninger, såfremt dette findes nødvendigt grundet ovenstående forhold. Supplerende foranstaltninger omfatter databeskyttelse gennem tekniske, organisatoriske og kontraktlige foranstaltninger. Effektiviteten af disse foranstaltninger afhænger af omstændighederne forbundet med den individuelle overførsel. Forhold, som kan påvirke effektiviteten, indebærer et tredjelands lovgivning, praksis samt de supplerende foranstaltningers detaljer. Tekniske supplerende foranstaltninger kan eksempelvis bestå af pseudonymisering og kryptering. Derudover kan organisatoriske foranstaltninger bestå af henholdsvis standarder og politikker, mens kontraktlige kan indebære krav om gennemsigtighed.

Yderligere kan det konkluderes gennem retspraksis, at SCC'er kun kan anvendes som overførselsgrundlag, såfremt et tilstrækkeligt databeskyttelseniveau sikres gennem fornødne garantier, jf. GDPR artikel 46, stk. 2, litra c. Derudover fastlægges det, at SCC'er ikke er bindende over for myndigheder i tredjeland, jf. Schrems II, præmis 126. Dermed findes det udelukkende muligt for SCC'er at beskytte registrerede mod efterretningstjenesters indgreb i USA gennem supplerende foranstaltninger, som kan bestå af teknisk, organisatorisk eller kontraktlig karakter for at sikre en tilstrækkelig databeskyttelse. Gennem retspraksis konkluderes det endvidere, at supplerende foranstaltninger som underrettelse af dataimportør i henhold til myndighedsanmodninger samt kryptering, hvor dekrypteringsnøglen er i dataimportørs besiddelse, ikke nødvendigvis sikrer en tilstrækkelig databeskyttelse. Disse supplerende foranstaltninger er betinget af overførslens omstændigheder, herunder USA's lovgivning og praksis. Derudover udledes det, at samme forhold gælder for anvendelse pseudonymisering, IP-anonymisering, *redigeringsscript* og *proxyserver*.

Afsluttende del af konklusionen vil besvare, hvordan CLOUD Act komplicerer tredjelandsoverførsel til USA, og hvordan dataansvarlige bør agere, såfremt vedkommendes databehandlere omfattes af CLOUD Act. I relation hertil konkluderes det, at amerikansk-ejede virksomheder i EU kan befinde sig i en jurisdiktionskonflikt mellem USA og EU's lovgivning. Dette begrundes i, at disse virksomheder kan modtage CLOUD Act-anmodninger, hvoraf modstridende krav i forbindelse med USA og EU's lovgivning kan forekomme. Imidlertid skal USA's myndigheder basere deres anmodninger på MLAT, såfremt et lovligt overførselsgrundlag skal anvendes, jf. GDPR artikel 48.

En imødekommelse af en CLOUD Act-anmodning med GDPR artikel 49, litra d, som overførselsgrundlag kan ikke realiseres i praksis, eftersom USA og EU's fortolkning af væsentlige samfundsinteresser ikke findes forenelig. En imødekommelse af en CLOUD Act-anmodning med GDPR artikel 49, litra e, som overførselsgrundlag findes vanskelig, eftersom dette medfører strenge krav i forbindelse med sammenhængen mellem efterforskningen og dataoverførslen. En imødekommelse af en CLOUD Act-anmodning med GDPR artikel 49, litra f, som overførselsgrundlag findes ligeledes besværlig, eftersom bestemmelsen kun bør anvendes i ekstraordinære nødstilfælde. En imødekommelse af en CLOUD Act-anmodning med GDPR artikel 49, stk. 1, andet afsnit, som overførselsgrundlag kan ikke realiseres, eftersom underretningskravet ikke kan opfyldes i praksis. Derudover bør internationale aftaler, herunder MLAT, anvendes som overførselsgrundlag, før undtagelsesbestemmelserne i GDPR artikel 49 overvejes. Endvidere konkluderes det, at CLOUD Act ikke findes forenelig med EU-retten, hvilket begrundes i fravigelsen samt omgåelsen af bestemmelserne i MLAT. Dette medfører, at CLOUD Act-anmodninger ikke skal imødekommes af omfattede virksomheder uden videre. Grundet igangværende forhandlinger vedrørende harmonisering kan CLOUD Act imidlertid potentielt medføre færre komplikationer i fremtiden i et EU-retligt perspektiv

Afslutningsvis konkluderes det ud fra retspraksis gennem KOMBIT-sagen, at imødekommelse af CLOUD Act-anmodninger i overensstemmelse med databehandleraftaler medfører, at databehandlere omfattes af GDPR. Derudover fastlægges det, at imødekommelse af myndighedsanmodninger kun skal forekomme, såfremt grundlaget findes i internationale aftaler. Det konkluderes yderligere, at dataansvarlige skal afklare på forhånd, om vedkommendes databehandlere sikrer en tilstrækkelig databeskyttelse. Dertil skal den dataansvarlige sikre en tilstrækkelig behandlingssikkerhed, hvilket kan indebære relevante risikovurderinger. Endvidere skal der foretages regelmæssige tilsyn med vedkommendes databehandler. Ydermere skal den dataansvarlige standse imødekommelse af CLOUD Act-anmodninger, såfremt dette er i strid med databehandleraftalen. Det kan endvidere konkluderes gennem GDPR og juridisk litteratur, at fortolkningstvivl bør afklares af den dataansvarlige på forhånd. Derudover bør ordlyden i databehandleraftalen være præcis og klar, hvilket begrundes i, at dette kan være betydningsfuldt for erstatningsansvarets fordeling mellem den dataansvarlige og databehandleren, jf. GDPR artikel 28, stk. 1 og 82, stk. 2.

14 Litteraturliste

Administration of Joseph R. Biden, Jr. "Executive Order 14086—Enhancing Safeguards for United States Signals Intelligence Activities." *govinfo.gov*, 7. oktober 2022, https://www.govinfo.gov/content/pkg/DCPD-202200894/pdf/DCPD-202200894.pdf. Adgang 18. marts 2025.

American Bar Association. "What Is an Executive Order?" *americanbar.org*, 25. januar 2021, https://www.americanbar.org/groups/public_education/publications/teaching-legal-docs/what-is-an-executive-order-/. Adgang 5. marts 2025.

Blume, Peter. *Persondatarettens kilder og metode: med en guide til den persondataretlige sag*. 1. udgave, Djøf Forlag, 2020.

Blume, Peter. *Retssystemet og juridisk metode*. 3. udgave, Jurist- og Økonomforbundets Forlag, 2016.

Center for Democracy and Technology. "Section 702: What It Is & How It Works." https://cdt.org/wp-content/uploads/2017/02/Section-702.pdf. Adgang 10. marts 2025.

Criminal Division. "CLOUD Act Resources." *Department of Justice*, https://www.justice.gov/criminal/cloud-act-resources. Adgang 2. maj 2025.

CURIA. "Sag C-311/18." https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=20266186.

CURIA. "Sag C-362/14." https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=20266244.

Data Privacy Framework Program. "Data Privacy Framework." *Data Privacy Framework*, https://www.dataprivacyframework.gov/Program-Overview. Adgang 15. marts 2025.

Datatilsynet. “Anbefalinger efter Schrems II.” *Datatilsynet*, 11. november 2020, https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/nov/anbefalinger-efter-schrems-ii. Adgang 8. maj 2025.

Datatilsynet. “Artikel 29-gruppe vedrørende databeskyttelse.” *Datatilsynet*, 6. februar 2018, https://www.datatilsynet.dk/media/7859/arbejdsdokument-om-elementer-og-principper-der-skal-vaere-indeholdt-i-et-saet-bindende-virksomhedsregler-bcr-for-databehandlere.pdf. Adgang 10. marts 2025.

Datatilsynet. “Behandling af personoplysninger om hjemmesidebesøgende.” *Datatilsynet*, Februar 2020, https://www.datatilsynet.dk/Media/F/8/Behandling%20af%20personoplysninger%20om%20hjemmesidebes%C3%B8gende.pdf. Adgang 10. marts 2025.

Datatilsynet. “EDPB.” https://www.datatilsynet.dk/internationalt/det-europaeiske-databeskyttelsesraad-edpb. Adgang 10. marts 2025.

Datatilsynet. “Sager ved EUD.” *Datatilsynet*, https://www.datatilsynet.dk/internationalt/sager-ved-eu-domstolen. Accessed 10. marts 2025.

Datatilsynet. “Svar på forespørgsel: Vedrørende tilsigtede eller utilsigtede overførsler til tredjelande.” 29. marts 2022, https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/vedroerende-tilsigtede-eller-utilsigtede-overfoersler-til-tredjelande. Adgang 5. maj 2025.

Datatilsynet. “Tredjelandsoverførsler.” https://www.datatilsynet.dk/internationalt/tredjelandsoverfoersler. Adgang 5. marts 2025.

Datatilsynet. “Vejledning om cloud.” *Datatilsynet*, marts 2022, https://www.datatilsynet.dk/Media/637824109172292652/Vejledning%20om%20cloud.pdf. Adgang 10. april 2025.

Datatilsynet. “Vejledning om dataansvarlige og databehandlere.” *Datatilsynet*, november 2017, https://www.datatilsynet.dk/Media/7/6/Dataansvarlige%20og%20databehandlere.pdf. Adgang 10. marts 2025.

Datatilsynet. “Vejledning om overførsel til tredjelande.”, april 2024, https://www.datatilsynet.dk/Media/638478180234447566/Vejledning%20om%20overf%C3%B8rsel%20til%20tredjelande.pdf. Adgang 5. marts 2025.

“Datatilsynet fastholder forbud i Chromebook-sag: 2020-431-0061.” 18. august 2022, https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/aug/datatilsynet-fastholder-forbud-i-chromebook-sag. Adgang 5. april 2025.

Datatilsynet NO. “Informasjon om overføringer til USA.” 26. februar 2025, https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2025/informasjon-om-overforinger-til-usa/. Adgang 2. maj 2025.

Den Europæiske Unions Tidende. “Den Europæiske Unions Charter om Grundlæggende Rettigheder.” https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:12012P/TXT.

Den Europæiske Unions Tidende. “Forklaringer til EU's Charter om Grundlæggende Rettigheder.” *EUR-Lex.europa.eu.*, https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32007X1214(01). Adgang 7. maj 2025.

Den Europæiske Unions Tidende. “Traktat om Den Europæiske Union.” https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:12016ME/TXT. Adgang 5. februar 2025.

EDPB. “ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data.” *European Data Protection Board*, 10. juli 2019, https://www.edps.europa.eu/sites/default/files/publication/19-07-10_edpb_edps_cloudact_annex_en.pdf. Adgang 2. maj 2025.

EDPB. “EDPB Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework.” 4. november 2024, https://www.edpb.europa.eu/system/files/2024-11/edpb_report_20241104_reportonfirstreviewofeu-u.s.dpf_en.pdf. Adgang 1. maj 2025.

EDPB. “Guidelines 02/2024 on Article 48 GDPR.” 2024, https://www.edpb.europa.eu/system/files/2024-12/edpb_guidelines_202402_article48_en.pdf. Adgang 5. marts 2025.

EDPB. “Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveau for beskyttelse af personoplysninger.” 18. juni 2021, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_da.pdf. Adgang 2. maj.

EDPB. “Retningslinjer 05/2021 om samspil mellem anvendelse af artikel 3 og bestemmelserne om internationale overførsler i henhold til kapitel V i GDPR.” https://www.edpb.europa.eu/system/files/2023-09/edpb_guidelines_05-2021_interplay_between_the_application_da.pdf.

EDPB. “Retningslinjer 2/2018 vedrørende undtagelser i artikel 49 i forordning 2016/679.” 2018. Adgang 5. marts 2025.

EDPB. “Udtalelse 5/2023 om Kommissionens udkast til gennemførelsesafgørelse om tilstrækkelig beskyttelse af personoplysninger i henhold til databeskyttelsesramme mellem EU og USA.” 28. februar 2023, https://www.edpb.europa.eu/system/files/2023-09/edpb_opinion52023_eu-us_dpf_da.pdf. Adgang 5. maj 2025.

EMD. “CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM.” *HUDOC*, 25. maj 2021,

https://hudoc.echr.coe.int/fre#%7B%22itemid%22:[%22001-210077%22]%7D. Adgang 8. maj 2025.

EMD. "CASE OF SZABÓ AND VISSY v. HUNGARY." *HUDOC*, 2016, https://hudoc.echr.coe.int/fre#%7B%22itemid%22:[%22001-160020%22]%7D. Adgang 8. maj 2025.

Europa-Kommissionen. "Agreement with the United States on mutual legal assistance." 16. april 2019, https://eur-lex.europa.eu/EN/legal-content/summary/agreement-with-the-united-states-on-mutual-legal-assistance.html?fromSummary=23. Adgang 5. maj 2025.

Europa-Kommissionen. "Kommissionens beslutning af 26. juli 2000 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkelighed af den beskyttelse, der opnås ved hjælp af safe harbor-principperne til beskyttelse af privatlivets fred." 2000, https://eur-lex.europa.eu/legal-content/da/ALL/?uri=CELEX%3A32000D0520. Adgang 10. marts 2025.

Europa-Kommissionen. "Kommissionens gennemførelsesafgørelse (EU) 2016/1250 af 12. juli 2016 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkelighed af den beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred." 2016, https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016D1250&from=NL. Adgang 5. marts 2025.

Europa-Kommissionen. "Kommissionens gennemførelsesafgørelse (EU) 2023/1795 af 10. juli 2023 i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679 om et tilstrækkeligt beskyttelsesniveau for personoplysninger inden for EU-USA-databeskyttelsesrammen." 2023, https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj/dan.

Europa-Kommissionen. "MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, DET EUROPÆISKE RÅD, RÅDET, DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET." 18. maj 2022,

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&from=EN. Adgang 2. maj 2025.

Europa-Kommissionen. "RAPPORT FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET om den første regelmæssige revision af, hvordan afgørelsen om tilstrækkeligheden af beskyttelsesniveauet i forbindelse med EU-USA-databeskyttelsesrammen fungerer." 9. Oktober 2024, https://eur-lex.europa.eu/legal-content/DA/ALL/?uri=CELEX:52024DC0451. Adgang 5. april 2025.

"Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger." *EUR-Lex.europa.eu.*, 23. november 1995, https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:31995L0046. Adgang 5. april 2025.

"Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF." *EUR-Lex.europa.eu.*, https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679. Adgang 5. maj 2025.

Europa-Parlamentets Udvalg om Borgernes Rettigheder og Retlige og Indre Anliggender (LIBE). "UDKAST TIL FORSLAG TIL BESLUTNING 2023/2501." 14. februar 2023, https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_DA.pdf. Adgang 5. maj 2025.

European Commission. "Mutual legal assistance and extradition." *European Commission*, https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en. Adgang 2. maj 2025.

European Court of Human Rights. “Factsheet – Mass surveillance.” *ECHR*, Juni 2024, https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng. Adgang 15. april 2025.

European Parliament. “A Comparison between US and EU Data Protection Legislation for Law Enforcement.” 2015, https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU%282015%29536459_EN.pdf. Adgang 5. maj 2025.

European Union Agency for Criminal Justice Cooperation. “THE CLOUD ACT.” 22. december 2022, https://www.eurojust.europa.eu/sites/default/files/assets/the-cloud-act.pdf. Adgang 2. maj 2025.

The European Union and the United States of America. “AGREEMENT on mutual legal assistance between the European Union and the United States of America.” 19. Juli 2003, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22003A0719(02). Adgang 2. maj 2025.

Folketinget. “§ 20.” *Folketinget*, https://www.ft.dk/da/dokumenter/bestil-publikationer/publikationer/mingrundlov/min-grundlov/kapitel-3/paragraf-20. Adgang 10. marts 2025.

Folketingets EU-Oplysning. “Suverænitet.” *Folketingets EU-Oplysning*, https://www.eu.dk/danmark-i-eu/eu-ret-i-danmark/suveraenitet. Adgang 10. marts 2025.

GDPRhub. “AP (The Netherlands) - Takeaway B.V. - z2022-04011.” *GDPRhub*, 26. november 2024, https://gdprhub.eu/index.php?title=AP_(The_Netherlands)_-_Takeaway_B.V._-_z2022-04011. Adgang 5. maj 2025.

GDPRhub. “Article 46 GDPR.” Adgang 5. marts 2025.

GDPRhub. “Article 48 GDPR.” https://www.gdprhub.eu/Article_48_GDPR. Adgang 5. marts 2025.

GDPRhub. “Article 49 GDPR.” https://gdprhub.eu/Article_49_GDPR. Adgang 5. marts 2025.

GDPRhub. “BVwG - W245 2252208-1/36E and W245 2252221-1/30E.” 12. maj 2023, https://gdprhub.eu/index.php?title=BVwG_-_W245_2252208-1/36E_and_W245_2252221-1/30E. Adgang 2. maj 2025.

GDPRhub. “CJEU - C-311/18 - Facebook Ireland and Schrems.” https://gdprhub.eu/index.php?title=CJEU_-_C-311/18_-_Facebook_Ireland_and_Schrems. Adgang 10. marts 2025.

GDPRhub. “Datatilsynet (Norway) - 20/03771.” 1. marts 2023, https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_20/03771. Adgang 2. maj 2025.

GDPRhub. “DSB (Austria) - 2021-0.586.257.” *GDPRhub*, 22. december 2021, https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2021-0.586.257. Adgang 5. maj 2025.

GDPRhub. “LG Köln - 33 O 376/22.” 10. maj 2023, https://gdprhub.eu/index.php?title=LG_Köln_-_33_O_376/22. Adgang 20. april 2025.

GDPRhub. “LG Traunstein - 9 O 173/24.” *GDPRhub*, https://gdprhub.eu/index.php?title=LG_Traunstein_-_9_O_173/24. Adgang 5. maj 2025.

Giles, John. “Why the Microsoft Ireland Case is Important?” *Michalsons*, 28. juni 2019, https://www.michalsons.com/blog/why-the-microsoft-ireland-case-is-important/18566. Adgang 2. maj 2025.

Hamer, Carina Risvig, et al. *Juraens verden: metoder, retskilder og discipliner*. Djøf Forlag, 2020.

Harmon, Rachel A. “When Is Police Violence Justified?” 2008, https://download.ssrn.com/08/07/21/ssrn_id1157348_code1003843.pdf?response-content-disposition=inline&X-Amz-Security-

Token=IQoJb3JpZ2luX2VjENH%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJIMEYCIQD8lYzxEXfBCQuCaWWStxQdZdKWUq31%2BRjNCtnE8TmI%2BAIhAIue%2BQZ. Adgang april 2025.

Haslund, Alexander. "Trump ryster EU-aftale: Cloud-løsninger risikerer at blive ulovlige." *Finansforbundet*, 29. januar 2025, https://finansforbundet.dk/dk/nyheder/2025/trump-ryster-eu-aftale-cloud-loesninger-risikerer-at-blive-ulovlige/. Adgang 5. maj 2025.

Institut for Menneskerettigheder. "REFORM AF DEN EUROPÆISKE MENNESKERETTIGHEDSKONVENTION?" September 2016, https://menneskeret.dk/files/media/dokumenter/udgivelser/faktaark_qa/faktaark_reform_af_den_europaeiske_menneskerettighedskonvention.pdf. Adgang 20. april 2025.

intel.gov. "FISA Section 702 A One Page Overview." *Foreign Intelligence Surveillance Act*, https://www.intelligence.gov/foreign-intelligence-surveillance-act/1237-fisa-section-702. Adgang 5. marts 2025.

intelligence.gov. "FACT SHEET: Implementation of the USA FREEDOM Act of 2015." *Intel-god*, https://www.intelligence.gov/ic-on-the-record-database/results/787-fact-sheet-implementation-of-the-usa-freedom-act-of-2015. Adgang 4. marts 2025.

Joel, Alex. "Necessity, Proportionality, and Executive Order 14086." Maj 2023, https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?params=/context/research/article/1101/&path_info=Necessity_Proportionality_and_Executive_Order_14086.pdf. Adgang 15. april 2025.

Joel, Alex. "Protecting Privacy and Promoting Transparency: The Perspective of a Civil Liberties Protection Officer." 13. marts 2023, https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/protecting-privacy-and-promoting-transparency/. Adgang 25. april 2025.

LaCasse, Alex. “European Commission report reviews progress of EU-US DPF.” *IAPP*, 9. oktober 2024, https://iapp.org/news/a/european-commission-report-reviews-progress-of-eu-us-dpf. Adgang 2. maj 2025.

Lando, Ole. “Præambel.” *Lex*, 13. februar 2025, https://lex.dk/pr%C3%A6ambel. Adgang 10. marts 2025.

“Lov om Den Europæiske Menneskerettighedskonvention.” *Retsinformation*, https://www.retsinformation.dk/eli/lta/1992/285. Adgang 15. marts 2025.

“Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (DBL).” *Retsinformation*, https://www.retsinformation.dk/eli/lta/2018/502. Adgang 5. april 2025.

Mantel, Lauren. “The Civil Liberties Protection Officers: The Gateway to Redress.” 23. april 2024, https://privacyacrossborders.org/2024/04/23/the-civil-liberties-protection-officers-the-gateway-to-redress/. Adgang 25. april 2025.

Mignon, Emmanuelle. “The CLOUD Act: Unveiling European Powerlessness.” https://geopolitique.eu/articles/the-cloud-act-unveiling-european-powerlessness/. Adgang 2. maj 2025.

Mignon, Emmanuelle. “The CLOUD Act: Unveiling European Powerlessness - Groupe d'Etudes Géopolitiques.” *Groupe d'études géopolitiques*, https://geopolitique.eu/articles/the-cloud-act-unveiling-european-powerlessness/. Adgang 12. maj 2025.

Mildebrath, Hendrik. “Reaching the EU-US Data Privacy Framework: First reactions to Executive Order 14086.” *europarl.europa.eu*, December 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739261/EPRS_BRI(2022)739261_EN.pdf. Adgang 18. marts 2025.

Morgan Lewis. “NO GRACE PERIOD AFTER INVALIDATION OF EU-US PRIVACY SHIELD IN SCHREMS II.” *Morgan Lewis*, 27. juli 2020, https://www.morganlewis.com/pubs/2020/07/no-grace-period-after-invalidation-of-eu-us-privacy-shield-in-schrems-ii. Adgang 8. maj 2025.

Munk-Hansen, Carsten. *Retsvidenskabsteori*. 3. udgave, Djøf, 2022.

Navarro, Patrice. “The legal uncertainty facing EU–US Data Transfers – Storm over the Atlantic.” 2. maj 2025, https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2025/05/the-legal-uncertainty-facing-eu-us-data-transfers-storm-over-the-atlantic.html. Adgang 5. maj 2025.

“New Standard Contractual Clauses - Questions and Answers overview.” *European Commission*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en. Adgang 1. maj 2025.

NG, Alfred, and John Sakellariadis. “Inside Biden’s secret surveillance court.” 17. januar 2024, https://www.politico.com/news/2024/01/17/inside-bidens-secret-surveillance-court-00136175. Adgang 5. maj 2025.

Noori, Kave. “Det blåser kring datadelningsavtalet med USA.” *Forum för Dataskydd*, 14. marts 2025, https://dpforum.se/det-blaser-kring-datadelningsavtalet-med-usa/. Adgang 2. maj 2025.

NOYB. “EU-US Data Transfers.” https://noyb.eu/en/eu-us-data-transfers-0. Adgang 10. marts 2025.

NOYB. “Open Letter on the Future of EU-US Data Transfers.” *NOYB*, 23. maj 2022, https://noyb.eu/en/open-letter-future-eu-us-data-transfers. Adgang 5. maj 2025.

NOYB. “US Cloud soon illegal? Trump punches first hole in EU-US Data Deal.” *NOYB*, 23. januar 2025, https://noyb.eu/en/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal. Adgang 5. maj 2025.

Office of the Director of National Intelligence. “National Intelligence Priorities Framework.” *dni.gov*, 2021, https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf. Adgang 18. marts 2025.

Olifent, Louise. “Danmark er 100 procent afhængig af Microsoft: Nu truer Trump den aftale, der gør det lovligt at bruge.” *Version2*, 24. januar 2025, https://www.version2.dk/artikel/danmark-er-100-procent-afhaengig-af-microsoft-nu-truer-trump-den-aftale-der-goer-det-lovligt-bruge. Adgang 5. maj 2025.

Olifent, Louise. “Skepsis over data-aftale vokser: Topforhandler vil ikke lægge hovedet på Schrems III-blokken.” 10. maj 2022, https://www.version2.dk/artikel/skepsis-over-data-aftale-vokser-topforhandler-vil-ikke-laegge-hovedet-paa-schrems-iii-blokken. Adgang 2. maj 2025.

PCLOB. “Advisory Function Policy and Procedure.” Oktober 2015, https://documents.pclob.gov/prod/DynamicImages/Generic/dd216c11-67e2-440b-9944-675f389b289f/Policy-Advisory_Function_Policy_Procedure%20-508%20-%20Jan%2023%202023.pdf. Adgang marts 2025.

Peters, Gerhard, and John T. Woolley. “National Security Memorandum on Partial Revocation of Presidential Policy Directive 28.” *The American Presidency Project*, 7. oktober 2022, https://www.presidency.ucsb.edu/documents/national-security-memorandum-partial-revocation-presidential-policy-directive-28. Adgang 1. maj 2025.

Ravn-Højgaard, Signe, et al. “Tænketank: Big tech styrer vores digitale infrastruktur. Det truer vores sikkerhed og demokrati.” *Altinget*, 6. maj 2025,

https://www.altinget.dk/embedsvaerk/artikel/forskere-det-offentlige-rum-er-kommet-paa-private-haender-det-truer-vores-sikkerhed-og-demokrati. Adgang 8. maj 2025.

Reimann, Johan. "EU-traktaternes hovedprincipper." *Lex*, 25. maj 2021, https://lex.dk/EU-traktaternes_hovedprincipper. Adgang 10. marts 2025.

Stanley, Jay. "What Powers Does the Civil Liberties Oversight Board Have?" *ACLU*, 4. november 2013, https://www.aclu.org/news/national-security/what-powers-does-civil-liberties-oversight-board. Adgang 20. marts 2025.

Toh, Amos, et al. "Overseas Surveillance in an Interconnected World." *Brennan Center for Justice*, 2016, https://www.brennancenter.org/sites/default/files/publications/Overseas_Surveillance_in_an_Interconnected_World.pdf. Adgang 5. marts 2025.

Tvarnø, Christina D., og Ruth Nielsen. *Retskilder og retsteorier*. Jurist- og Økonomforbundets Forlag, 2017.

Udsen, Henrik. *Databeskyttelsesret*. 1. udgave, www.databeskyttelsesret.dk, 2022, www.databeskyttelsesret.dk.

U.S. Department of Justice. "Frequently Asked Questions - CLOUD Act." https://www.justice.gov/criminal/media/999616/dl?inline. Adgang 2. maj 2025.

U.S. Department of Justice. "Rules and Regulations 62303." 14. oktober 2022, https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22234.pdf?utm_source=federalregister.gov&utm_medium=email&utm_campaign=subscription+mailing+list. Adgang 15. april 2025.

U.S. Department of Justice. "2201 DIVISION V—CLOUD ACT." *CLOUD Act*, 9. april 2019, https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf. Adgang 2. maj 2025.

U.S. Privacy and Civil Liberties Oversight Board. “History and Mission.” *pclob.gov*, https://www.pclob.gov/About/HistoryMission. Adgang 21. marts 2025.

Wernblad, Thomas. “Ny lov bremser sagen om Microsofts udlevering af data fra EU.” *Kromann Reumert*, 14. maj 2018, https://kromannreumert.com/nyheder/ny-lov-bremser-sagen-om-microsofts-udlevering-data-fra-eu. Adgang 2. maj 2025.

Wood, Georgia, and Andrew Lewis. “The CLOUD Act and Transatlantic Trust.” *CSIS*, 29. marts 2023, https://www.csis.org/analysis/cloud-act-and-transatlantic-trust. Adgang 2. maj 2025.