KANDIDATSPECIALE

OVERFØRSEL AF PERSONOPLYSNINGER TIL USA OG EUROPA-KOMMISSIONENS STANDARDKON-TRAKTBESTEMMELSER I LYSET AF EU-RETTEN OG GRUNDLÆGGENDE RETTIGHEDER

TRANSFER OF PERSONAL DATA TO THE UNITED STATES AND THE EUROPEAN COMMISSION'S STANDARD CONTRACTUAL CLAUSES IN THE LIGHT OF EU LAW AND FUNDAMENTAL RIGHTS

NICOLAI KJÆRGAARD SØRENSEN
STUDIENR. 20164527

19. MAJ 2021

VEJLEDER: ULLA STEEN

AALBORG
UNIVERSITET

Abstract

This master's thesis examines the impact of fundamental rights and the "*Schrems II*" judgment delivered by the Court of Justice of the European Union, ECJ, when the Danish data controller transfers personal data to the United States pursuant to the European Commission's standard contractual clauses, cf. Article 46(2)(c) of the General Data Protection Regulation, GDPR.

A review of the Schrems II judgment and its background shows that the ECJ has invalidated the transfer tools *"Safe Harbor"* and "*Privacy Shield"*, which previously made it possible for the data controller to transfer personal data out of the EU to companies located in the United States. This happened with reference to the American security legislation that authorizes mass surveillance.

Against this background the thesis examines to what extent Europeans are afforded protection against the American surveillance under fundamental rights. Based on an analysis of the Schrems II judgment it is concluded that the American security legislation of FISA Section 702, E.O. 12333 and PPD-28 constitutes a disproportional violation of the Europeans' fundamental rights to privacy, data protection and effective remedies under Articles 7, 8, 47 and 52 of the Charter of Fundamental Rights of the EU. At the same time, an analysis of American Supreme Court case law shows that the Fourth Amendment to the Constitution of the United States, which otherwise authorizes a certain fundamental right to privacy, applies to American citizens only. Although Article 17 of the International Covenant on Civil and Political Rights provides protection against the American surveillance and the United States has ratified the covenant, the thesis finds that the international community is failing in creating a common data protection standard between the EU and the United States. However, according to the Schrems II judgment, the data controller may only use the Commission's standard contractual clauses as a legal basis for transferring personal data if the data subject whose personal data is transferred to a third country is afforded a level of protection "*essentially equivalent*" to that guaranteed by EU law. Therefore, the thesis concludes that the data controller transferring personal data to the United States is facing a legal barrier arising from fundamental rights.

Subsequently, the thesis examines the legal requirements associated with the data controller's use of the Commission's standard contractual clauses. The analysis shows that the data controller by

virtue of the ECJ's interpretation of Article 46 GDPR is required to verify, on a case-by-case basis, whether the law of the third country ensures adequate protection. Moreover, the data controller may provide supplementary safeguards to those offered by the standard contractual clauses.

In the light of these requirements, the thesis discusses the options available in practice when transferring personal data to the United States. With reference to the consultation version of the European Data Protection Board's Recommendations 01/2020, the thesis concludes that the data controller in the board's opinion must exclude the American authorities' access to the personal data transferred to the United States by using a technical supplementary safeguard like encryption. However, this safeguard may undermine the purpose of the transfer. Therefore, the thesis seeks to clarify whether the data controller, based on subjective assessments of the actual risk of American surveillance, in some circumstances may provide less radical supplementary safeguards. Based on an analysis of the accountability principle pursuant to Article 5(2) GDPR, the Commission's standard contractual clauses, Recommendations 01/2020 and considerations regarding fundamental rights, the thesis concludes that this question is marked by theoretical uncertainty. Nevertheless, the data controller may comply with Recommendations 01/2020 even though these are not legally binding.

Finally, possible solutions to the problems resulting from the Schrems II judgment are discussed. First, the thesis seeks to clarify whether the data controller may use data processors established in the EU with a view to avoiding the problems. However, with reference to Article 5(2) and 28 GDPR it is concluded that the data controller can only use data processors that are able to meet the requirements of the Schrems II-judgment. As the data controller is not able to overcome the fundamental problems on its own, it is relevant to consider what the legislator can do. The thesis concludes that amendments of the American security legislation may be a solution. However, the requirements of the Constitution may imply that such amendments to federal law are not sufficient to bring American legislating into line with the Charter.

Indholdsfortegnelse

1. Forkortelser 1

2. Introduktion, problemformulering og præcisering af afhandlingens fokus 5

2.1. Præcisering af afhandlingens fokus 7

3. Metodisk tilgang 8

3.1. Retsdogmatisk metode 8

3.2. Den retlige ramme 9

3.2.1. Samspil mellem den EU-retlige og danske regulering på persondatarettens område 9

3.2.2. Persondatarettens særlige begreber 11

3.3. Kommissionens forskellige sæt standardkontraktbestemmelser 13

3.4. Betydningen af det amerikanske reguleringssystem samt folkeretten 14

4. Schrems II-dommen og dens baggrund 16

5. Europæernes grundlæggende rettigheder og den amerikanske overvågning 20

5.1. De grundlæggende rettigheder efter Chartret 21

5.2. De grundlæggende rettigheder efter den amerikanske forfatning 26

5.3. De grundlæggende rettigheder efter CPR-Konventionen 29

5.4. Databeskyttelseskrigen 31

6. De retlige rammer for den dataansvarliges brug af Kommissionens standardkontraktbestemmelser 33

6.1. De fornødne garantier 34

6.2. Undersøgelsespligten 36

6.3. Den generelle gyldighed af Kommissionens standardkontraktbestemmelser 38

7. De praktiske muligheder for anvendelsen af Kommissionens standardkontraktbestemmelser 39

7.1. Supplerende foranstaltninger, der udelukker risikoen for amerikansk overvågning 40

7.2. Supplerende foranstaltninger, der ikke udelukker risikoen for amerikansk overvågning 43

7.2.1. Princippet om ansvarlighed og den risikobaserede tilgang 44

7.2.2. De grundlæggende rettigheder som fortolkningsmoment 48

7.2.3. Teoretisk usikkerhed og praktiske realiteter 51

8. Hvordan løses den grundlæggende problematik? 52

8.1. Den dataansvarliges brug af databehandlere etableret i EU 52

8.2. En ny Privacy Shield-ordning, lovændringer og teknologiens udvikling 55

9. Konklusion 58

10. Litteraturliste 62

11. Skærmprint med antal anslag 69

1. Forkortelser

Art.	Artikel.
Beslutning 2000/520	Kommissionens beslutning 2000/520/EF af 26. juli 2000 i henhold til direktiv 95/46 om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af Safe Harbor-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium.
Bl.a.	Blandt andet.
Chartret	Den Europæiske Unions charter om grundlæggende rettigheder (EU-Tidende nr. C 202/2 af 7. juni 2016, s. 389).
Clapper-sagen	Clapper v. Amnesty International USA, 568 U.S. 398 (2013).
CLOUD Act	Clarifying Lawful Overseas Use of Data Act.
CPR-Konventionen	FN's konvention om borgerlige og politiske rettigheder med tilhørende valgfri protokol (UNTS Vol. 999, No. 14668, p. 171; bekendtgørelse nr. 30 af 29. marts 1976).
CRS	Congressional Research Service.
Databeskyttelsesdirektivet	Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.
DBL	Databeskyttelsesloven (lov nr. 502 af 23. maj 2018).
DPC	Data Protection Commission.
EDPB	Det Europæiske Databeskyttelsesråd.
EDPS	Den Europæiske Tilsynsførende for Databeskyttelse.
EMRK	Den Europæiske Menneskerettighedskonvention (European Treaty Series - No. 5; bekendtgørelse nr. 20 af 11. juni 1953).
E.O. 12333	Executive Order 12333.
EU	Den Europæiske Union.
EU-Domstolen	Den Europæiske Unions Domstol.

EØS	Det Europæiske Økonomiske Samarbejdsområde.
FISA	Foreign Intelligence Surveillance Act.
FISC	Foreign Intelligence Surveillance Court.
FN	De Forenede Nationer.
FN's Børnekonvention	FN's børnekonvention (UNTS Vol. 1577, No. 27531, p. 3; bekendtgørelse nr. 6 af 16. januar 1992).
FN's Handicapkonvention.	FN's konvention om rettigheder for personer med handicap (UNTS Vol. 2515, No. 44910, p. 3; bekendtgørelse nr. 20 af. 15. november 2017).
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 og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).
Gennemførelsesafgørelse 2016/1250	Kommissionens gennemførelsesafgørelse (EU) 2016/1250 af 12. juli 2016 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred.
Henstilling 01/2020	Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, version til offentlig høring, 10. november 2020.
Højesteretten	Supreme Court of the United States.
Kap.	Kapitel.
Katz-sagen	Katz v. United States, 389 U.S. 347 (1967).
Kommentar 16	CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation.

Kommissionen	Europa-Kommissionen.
M.fl.	Med flere.
NSA	National Security Agency.
Olmstead-sagen	Olmstead v. United States, 277 U.S. 438 (1928).
PDL	Persondataloven (lov nr. 429 af 31. maj 2000).
PPD-28	Presidential Policy Directive 28.
Pkt.	Punktum.
Rakas-sagen	Rakas v. Illinois, 439 U.S. 128 (1978).
S.	Side.
Schrems I	EU-Domstolens dom af 6. oktober 2015, Sag C-362/14, *Schrems*.
Schrems II	EU-Domstolens dom af 16. juli 2020, Sag C-311/18, *Facebook Ireland og Schrems*.
Section 702	50 U.S.C. § 1881a (2018).
TEU	Konsolideret udgave af traktaten om Den Europæiske Union (EU-Tidende nr. C 202/1 af 7. juni 2016, s. 13).
TEUF	Konsolideret udgave af traktaten om Den Europæiske Unions funktionsmåde (EU-Tidende nr. C 202/1 af 7. juni 2016, s. 47).
Traktatkonventionen	Wienerkonventionen om traktatretten (UNTS Vol. 1155, No. 18232, p. 331; bekendtgørelse nr. 34 af 29. april 1980).
United States Dist. Ct.-sagen	United States v. United States Dist. Ct., 407 U.S. 297 (1972).
U.S.C.	United States Code.
Verdugo-Urquidez-sagen	United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).
2001-bestemmelserne	Kommissionens beslutning af 15. juni 2001 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til direktiv 95/46/EF, som ændret ved Kommissionens gennemførelsesafgørelse (EU) 2016/2297 af 16. december 2016 om ændring af beslutning

	2001/497/EF og afgørelse 2010/87/EU om standardkontraktbestemmelser for videregivelse af personoplysninger til tredjelande og registerførere etableret i tredjelande i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF.
2004-bestemmelserne	Kommissionens beslutning af 27. december 2004 om ændring af beslutning 2001/497/EF for at indføre en alternativ standardkontrakt om overførsel af personoplysninger til tredjelande.
2010-bestemmelserne	Kommissionens afgørelse af 5. februar 2010 om standardkontraktbestemmelser for videregivelse af personoplysninger til registerførere etableret i tredjelande i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF, som ændret ved Kommissionens gennemførelsesafgørelse (EU) 2016/2297 af 16. december 2016 om ændring af beslutning 2001/497/EF og afgørelse 2010/87/EU om standardkontraktbestemmelser for videregivelse af personoplysninger til tredjelande og registerførere etableret i tredjelande i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF.
2020-bestemmelserne	COMMISSION IMPLEMENTING DECISION (EU) …/… on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Document Ares(2020)6654686).

2. Introduktion, problemformulering og præcisering af afhandlingens fokus

USA er det vigtigste land i det internationale informationssamfund.[1] Samtidig er USA den største samhandelspartner for EU for både varer og services.[2] Den moderne digitale økonomi forudsætter imidlertid, at der kan ske overførsel af personoplysninger til USA.[3] I henhold til GDPR samt EU-Domstolens domme i Schrems I og den nylagt afsagte Schrems II kan der udelukkende overføres personoplysninger om en fysisk person til et tredjeland uden for EU og EØS, såfremt denne person sikres et databeskyttelsesniveau, der i det væsentlige svarer til beskyttelsesniveauet efter EU-retten. Dette beskyttelsesniveau kan efter omstændighederne opnås ved brug af ét af de såkaldte overførselsgrundlag, der reguleres nærmere i GDPR.

Særligt overførsler af personoplysninger til USA afføder dog væsentlige problematikker, som stikker langt dybere end GDPR og kravet om et overførselsgrundlag. Med Schrems I og Schrems II har EU-Domstolen således ad to omgange ugyldiggjort ordningerne Safe Harbor og Privacy Shield, der som overførselsgrundlag ellers muliggjorde overførsel af personoplysninger til amerikanske virksomheder, der ved at tilmelde sig ordningerne underlagde sig en række principper om databeskyttelse. I begge tilfælde skete dette med henvisning til, at den amerikanske sikkerhedslovgivning, der hjemler overvågning af ikke-amerikanere, gik forud for de pågældende ordninger. Derfor var ordningerne i strid med de grundlæggende rettigheder som fastsat i EU's charter om grundlæggende rettigheder (herefter betegnet Chartret). Når der gennemføres en overførsel af personoplysninger til USA, har grundrettigheder således en helt særlig og praktisk betydning, som det primære pligtsubjekt i henhold til GDPR, den dataansvarlige, nødvendigvis må forholde sig til.

Dette gælder, uanset hvilket overførselsgrundlag i GDPR den dataansvarlige måtte vælge. Dog er det særligt ét overførselsgrundlag, der nu påkalder sig særlig praktisk interesse. Med Schrems II-dommen fik EU-Domstolen anledning til at tage stilling til gyldigheden af Kommissionens standardkontraktbestemmelser efter GDPR art. 46, stk. 2, litra c. På trods af de grundlæggende rettigheders

[1] Blume, Peter, *Databeskyttelsesret*, 5. udgave, 1. oplag, 2018, s. 276.
[2] Kommissionen, *Trade, policy, Countries and regions, United States*, https://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/ (sidst besøgt: 4/5 2021).
[3] Blume, Peter, *Databeskyttelsesret*, 5. udgave, 1. oplag, 2018, s. 253.

afgørende betydning ved tilsidesættelsen af både Safe Harbor og Privacy Shield fandt EU-Domstolen ikke anledning til at tilsidesætte disse standardbestemmelser som ugyldige. Umiddelbart efterlader EU-Domstolen derfor dette overførselsgrundlag som et særdeles relevant alternativ ved overførsel af personoplysninger til USA. Dette leder til afhandlingens problemformulering:

> *Hvilken indvirkning har grundrettigheder samt EU-Domstolens dom i Schrems II på den danske dataansvarliges muligheder for at overføre personoplysninger til USA på baggrund af Kommissionens standardkontraktbestemmelser, jf. GDPR art. 46, stk. 2, litra c?*

Problemformuleringen giver anledning til en præcisering af afhandlingens fokus, som uddybes i kapitel 2.1. I kapitel 3 redegøres der herefter for de særlige metodiske overvejelser, der gør sig gældende i forbindelse med besvarelse af problemformuleringen.

Med henblik på at tilvejebringe en forståelse for Schrems II-dommen og de juridiske spørgsmål, den giver anledning til, redegøres der i kapitel 4 for dommens baggrund med fokus på den amerikanske overvågning og den sikkerhedslovgivning, der hjemler overvågningen. Med udgangspunkt i en antagelse om, at der gælder uoverensstemmelser mellem grundrettigheder i det EU-retlige, amerikanske samt folkeretlige reguleringssystem, vil europæernes grundrettighedsbeskyttelse mod den amerikanske overvågning herefter blive undersøgt i kapitel 5. På baggrund af disse undersøgelser vil kapitel 6 og 7 behandle den dataansvarliges aktuelle retsstilling i forbindelse med overførsel af personoplysninger til USA, når Kommissionens standardkontraktbestemmelser anvendes som overførselsgrundlag. I denne henseende vil der blive fokuseret på mulige værktøjer, som den dataansvarlige kan gøre brug af, ligesom eventuelle tvivlsspørgsmål vil blive fremhævet. De mulige løsningsmodeller, som den dataansvarlige ikke selv kan iværksætte, vil slutteligt blive behandlet i kapitel 8.

Med udgangspunkt i afhandlingens redegørelser og analyser konkluderes det, at den dataansvarlige i forbindelse med overførsel af personoplysninger til USA må overvinde en retlig barriere på grundrettighedsniveau. Mens den dataansvarlige udelukkende kan gennemføre overførslen, såfremt

personoplysningerne sikres et databeskyttelsesniveau, der i det væsentlige svarer til beskyttelsen efter EU-retten, er den amerikanske sikkerhedslovgivning i strid med de grundlæggende rettigheder i Chartret. Dette samtidig med, at den amerikanske forfatning ikke yder beskyttelse mod masseovervågning af ikke-amerikanere, og at det folkeretlige reguleringssystem fejler i at skabe en fælles databeskyttelsesstandard EU og USA imellem. Når den dataansvarlige anvender Kommissionens standardkontraktbestemmelser som overførselsgrundlag kan denne retlige barriere dog overvindes ved brug af beskyttelsesmekanismer, der supplerer standardbestemmelserne. Det står klart, at den dataansvarlige ved hjælp af eksempelvis kryptering af de overførte personoplysninger helt kan udelukke risikoen for amerikansk overvågning. Derimod er det mindre klart, om den dataansvarlige i visse tilfælde kan gøre brug af mindre radikale værktøjer, der ikke helt udelukker risikoen for overvågningen. Det er nærliggende, at lovgiver må adressere problematikkerne, og i denne henseende er ændringer af amerikansk sikkerhedslovgivning blot én af flere løsningsmodeller.

2.1. Præcisering af afhandlingens fokus

Overordnet set findes der to typer af dataansvarlige, nemlig dataansvarlige fra henholdsvis den private og offentlige sektor. Afhandlingen vil have fokus på de overførsler af personoplysninger, der finder sted i den private sektor. For det første skyldes dette, at Kommissionens standardkontraktbestemmelser efter GDPR art. 46, stk. 2, litra c, ikke er det foretrukne overførselsgrundlag ved overførsler mellem offentlige myndigheder. Her er det navnlig overførselsgrundlagene i GDPR art. 46, stk. 2, litra a, samt art. 46, stk. 3, litra b, der er praktisk relevante.[4] For det andet vil afhandlingen inddrage forretningsmæssige betragtninger, der navnlig gør sig gældende i den private sektor.

Afhandlingen vil ligeledes fokusere på grundlæggende rettigheder, der gælder for alle befolkningsgrupper. Det falder uden for afhandlingens rammer at vurdere eventuelle forskelle i grundrettighedsbeskyttelsen af specifikke befolkningsgrupper, og FN's Børnekonvention og FN's Handicapkonvention vil således ikke blive inddraget.

[4] EDPB, *Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies*, version 2.0, 15. december 2020, afsnit 1.

Problemformuleringen behandler et dynamisk emne, der er i løbende udvikling. Det bemærkes, at nærværende afhandling baseres på materiale, der var offentligt tilgængeligt d. 16. maj 2021. I afhandlingen henvises der til materiale, der kan blive ændret efter den nævnte skæringsdato. Dette materiale er vedhæftet som bilag.

3. Metodisk tilgang

3.1. Retsdogmatisk metode

Denne afhandling beskæftiger sig med et retsvidenskabeligt spørgsmål. Ved undersøgelsen af problemformuleringen vil den retsdogmatiske metode blive anvendt med henblik på at klarlægge gældende ret, *de lege lata*. I nærværende sammenhæng skal de lege lata forstås som den retstilstand, der skabes i samspillet mellem EU-Domstolens dom i Schrems II, grundlæggende rettigheder, GDPR samt Kommissionens standardkontraktbestemmelser, når den dataansvarlige gennemfører en overførsel af personoplysninger til USA. Som led i den retsdogmatiske analyse vil der blive inddraget en række retskilder og særlige persondataretlige begreber.[5]

Retskilder vil i nærværende sammenhæng blive opfattet som informationskilder vedrørende retssystemet, der kan være afgivet af en række forskellige aktører, der handler inden for en bestemt retlig kompetence. Der er identificeret flere af sådanne retskilder af relevans for besvarelsen af problemformuleringen. Ifølge retskildelæren vil retskilderne dog ikke have samme forpligtende virkning og politiske legitimation, og i lyset af deres retskildeværdi skal de derfor tillægges forskellig vægt.[6]

De væsentligste retskilder, der tilsammen udgør den retlige ramme for analyse og besvarelse af afhandlingens problemformulering, vil i det følgende blive beskrevet.

[5] Tvarnø, Christina D. og Nielsen, Ruth, *Retskilder og retsteorier*, 5. reviderede udgave, 1. oplag, 2017, s. 29 f.
[6] Tvarnø, Christina D. og Nielsen, Ruth, *Retskilder og retsteorier*, 5. reviderede udgave, 1. oplag, 2017, s. 29.

3.2. Den retlige ramme

3.2.1. Samspil mellem den EU-retlige og danske regulering på persondatarettens område

Når den danske dataansvarlige gennemfører en overførsel af personoplysninger fra Danmark til USA, vil retskilder fra potentielt fire forskellige reguleringssystemer kunne komme i spil: Det danske, EU-retlige, amerikanske samt folkeretlige reguleringssystem. Besvarelsen af problemformformuleringen forudsætter derfor en undersøgelse af samspillet de forskellige reguleringssystemer imellem.

Det danske reguleringssystem er relevant, da den dataansvarlige er etableret i Danmark og dermed er underlagt dansk ret. Med tiltrædelsesloven med senere ændringer har Danmark ratificeret EU's traktatgrundlag, herunder bl.a. TEU og TEUF. Disse traktater er en del af den primære EU-ret og indeholder bl.a. hjemmelsbestemmelser, der giver EU-institutionerne mulighed for at vedtage sekundær EU-lovgivning i form af eksempelvis forordninger og direktiver.[7]

I nærværende sammenhæng vil GDPR med tilhørende præambelbetragtninger blive inddraget. GDPR er en forordning og er dermed bindende EU-retlig sekundærregulering, der har fuld direkte virkning i EU-medlemsstaterne, herunder i Danmark, jf. TEUF art. 288, 2. pkt. Dette indebærer, at GDPR både har horisontal og direkte virkning i Danmark, hvorfor borgere i Danmark kan påberåbe sig GDPR overfor staten og en anden borger.[8] GDPR har til formål at regulere alle væsentlige spørgsmål om databeskyttelse og gøre dette på en måde, der medfører ensartethed i EU-medlemsstaternes persondataretlige regulering. Derfor kan GDPR karakteriseres som den centrale retskilde i dansk persondataret. Som led i fortolkningen af bestemmelserne i GDPR vil de tilhørende præambelbetragtninger blive inddraget. Betragtningerne er vedtaget sammen med GDPR, hvorfor GDPR og betragtninger skal læses som en helhed.[9]

[7] Christoffersen, Jonas m.fl., *EU's Charter om Grundlæggende Rettigheder med kommentarer*, 2. udgave, 1. oplag, 2018, s. 40.
[8] EUR-Lex, *EU-rettens direkte virkning*, https://eur-lex.europa.eu/legal-content/DA/ALL/?uri=uriserv%3Al14547 (sidst besøgt: 4/5 2021).
[9] Blume, Peter, *Databeskyttelsesret*, 5. udgave, 1. oplag, 2018, s. 60 f.

Ligeledes vil Chartret indgå i afhandlingen. I medfør af TEU art. 6, stk. 1, gælder Chartret på traktatniveau, og er ligesom TEU og TEUF derfor en del af den primære EU-ret.[10] Chartret kodificerer en række grundlæggende rettigheder og almindelige retsprincipper, der oprindeligt er blevet udviklet af EU-Domstolen.[11] Chartrets nærmere betydning for dansk persondataret fastslås i præambelbetragtning 4 i GDPR, hvorefter GDPR overholder Chartret. Chartret skal derfor inddrages ved fortolkningen af GDPR.[12]

EU-Domstolen tillægger Chartret styrende betydning, når den i sine domme tager stilling til persondataretlige spørgsmål.[13] Dette illustreres af EU-Domstolens domme i henholdsvis Schrems I og Schrems II, som vil blive inddraget i afhandlingen. Begge domme er præjudicielle afgørelser, og efter TEUF art. 267, 1. pkt., fremgår det, at EU-Domstolen i sådanne afgørelser har kompetence til at afgøre præjudicielle spørgsmål om fortolkningen af EU's traktater samt om gyldigheden og fortolkningen af retsakter udstedt af EU's institutioner m.fl. Afgørelserne kan ikke appelleres. Det er således EU-Domstolen, der med bindende virkning endeligt fastlægger EU-rettens indhold, herunder reglerne og rettighederne som fastsat i GDPR og Chartret. EU-Domstolens afgørelser kan derfor anses som den øverste retskilde i en EU-retlig sammenhæng.[14] For så vidt angår EU-dommes præjudikatvirkning i forhold til nationale domstole, fremgår det ifølge EU-Domstolen af loyalitetsforpligtelsen efter TEU art. 4, stk. 3, samt EU-Domstolens praksis, at nationale domstole har pligt til at rette sig efter EU-Domstolens fortolkninger.[15]

I Danmark er DBL generelt set en central retskilde i dansk persondataret. DBL udfylder og supplerer GDPR, som i et vist omfang åbner op for et nationalt råderum.[16] I relation til standardkontraktbestemmelser efter GDPR art. 46, stk. 2, litra c, indeholder DBL dog ingen bestemmelser, der har praktisk betydning. Den retlige regulering af den dataansvarliges muligheder for at anvende Kommissionens standardkontraktbestemmelser er således fastlagt på EU-retligt niveau. Retskilder, der

[10] Christoffersen, Jonas m.fl., *EU's Charter om Grundlæggende Rettigheder med kommentarer*, 2. udgave, 1. oplag, 2018, s. 40.
[11] Tvarnø, Christina D. og Nielsen, Ruth, *Retskilder og retsteorier*, 5. reviderede udgave, 1. oplag, 2017, s. 102.
[12] Blume, Peter, *Persondatarettens kilder og metode*, 1. udgave, 1. oplag, 2020, s. 58.
[13] Blume, Peter, *Databeskyttelsesret*, 5. udgave, 1. oplag, 2018, s. 60.
[14] Blume, Peter, *Databeskyttelsesret*, 5. udgave, 1. oplag, 2018, s. 63.
[15] Tvarnø, Christina D. og Nielsen, Ruth, *Retskilder og retsteorier*, 5. reviderede udgave, 1. oplag, 2017, s. 156.
[16] Blume, Peter, *Databeskyttelsesret*, 5. udgave, 1. oplag, 2018, s. 53.

udelukkende udspringer fra det danske reguleringssystem, vil derfor kun blive inddraget i begrænset omfang.

GDPR indeholder en række særlige persondataretlige begreber. Som led i forståelsen af den retlige ramme vil udvalgte begreber i det følgende blive beskrevet.

3.2.2. Persondatarettens særlige begreber

Behandling af personoplysninger

I medfør af legaldefinitionen i GDPR art. 4, nr. 1, skal personoplysninger forstås som enhver form for information om en identificeret eller identificerbar fysisk person, der kan karakteriseres som "*den registrerede*". Ifølge GDPR art. 4, nr. 2, vil en behandling bestå i enhver aktivitet eller række aktiviteter, som de nævnte personoplysninger gøres til genstand for.

Dataansvarlig og databehandler

Den dataansvarlige er persondatarettens primære pligtsubjekt. I medfør af GDPR art. 4, nr. 7, er den dataansvarlige den, som udøver bestemmelsen over persondatabehandlingens formål, og på hvilken måde behandlingen foregår. Omvendt er databehandleren ifølge GDPR art. 4, nr. 8, enhver, som på vegne af den dataansvarlige varetager den faktiske persondatabehandling.[17]

Tredjelandsoverførsel

En tredjelandsoverførsel er ikke defineret direkte i GDPR art. 4, men skal karakteriseres som en overførsel af personoplysninger til et land, der både står uden for EU og EØS. Overførselsbegrebet dækker i praksis over mange konkrete situationer og omfatter også den såkaldte se-adgang, hvor en aktør i et tredjeland udelukkende kan se og ikke lagre eller printe de personoplysninger, der befinder sig på vedkommendes skærm. Det faktum, at personoplysninger lægges ud på en internetside, kan dog ikke i sig selv udgøre en tredjelandsoverførsel.[18]

[17] Blume, Peter, *Den nye persondataret*, 2. udgave, 1. oplag, 2018, s. 73 ff.
[18] Nielsen, Kristian Korfits og Lotterup, Anders, *Databeskyttelsesforordningen og databeskyttelsesloven*, 1. udgave, 1. oplag, 2020, s. 771 ff.

Når den dataansvarlige eller databehandleren gennemfører en tredjelandsoverførsel, kan vedkommende benævnes dataeksportør, ligesom den aktør i tredjelandet, der modtager de pågældende personoplysninger, kan karakteriseres som en dataimportør.[19] Henset til afhandlingens fokus på dataansvarlige, vil dataeksportøren i nærværende sammenhæng blive benævnt dataansvarlig. Aktøren i tredjelandet, som den dataansvarlige overfører personoplysninger til, vil blive benævnt dataimportør.

Overførselsgrundlag

Når den dataansvarlige ønsker at gennemføre en tredjelandsoverførsel, er vedkommende efter det generelle princip for tredjelandsoverførsler, jf. GDPR art. 44, forpligtet til at anvende ét af de overførselsgrundlag, der fremgår af GDPR kap. V. Overførselsgrundlaget udgør den dataansvarliges hjemmel til at foretage overførslen. GDPR art. 45 indeholder hjemmel til at overføre personoplysninger til et tredjeland, der i medfør af en afgørelse fra Kommissionen yder et "*tilstrækkeligt beskyttelsesniveau*", også kaldet et sikkert tredjeland. USA kan ikke karakteriseres som et sikkert tredjeland, og ved tredjelandsoverførsler til dette land kan GDPR art. 45 derfor ikke anvendes som overførselsgrundlag. GDPR art. 46 rummer imidlertid en række yderligere overførselsgrundlag, der kan anvendes, når der overføres personoplysninger til et usikkert tredjeland som USA. I medfør af art. 46, stk. 1, kan en overførsel efter art. 46 som udgangspunkt kun finde sted, såfremt den dataansvarlige udsteder de *"fornødne garantier*". I art. 46, stk. 2, opregnes en række instrumenter, der efter omstændighederne kan sikre de fornødne garantier. Ét af disse instrumenter er Kommissionens standardkontraktbestemmelser, jf. GDPR art. 46, stk. 2, litra c. I en retlig kontekst er standardkontraktbestemmelserne et bilag til en afgørelse vedtaget af Kommissionen. Standardkontraktbestemmelserne pålægger såvel den dataansvarlige som dataimportøren en række forpligtelser, der overordnet svarer til dem, der gælder for dataansvarlige og databehandlere efter GDPR.[20]

I situationer, hvor hverken GDPR art. 45 og 46 kan anvendes som overførselsgrundlag, kan der ligeledes gennemføres en tredjelandsoverførsel på grundlag af de i GDPR art. 49 nævnte undtagelser.

[19] Nielsen, Kristian Korfits og Lotterup, Anders, *Databeskyttelsesforordningen og databeskyttelsesloven*, 1. udgave, 1. oplag, 2020, s. 773.
[20] Udsen, Henrik, *IT-ret*, 4. udgave, 1. oplag, 2019, s. 439 ff.

Undtagelserne skal fortolkes restriktivt og vedrører hovedsagligt behandlingsaktiviteter, der er lejlighedsvise og ikke præget af gentagelser.[21]

3.3. Kommissionens forskellige sæt standardkontraktbestemmelser

Kommissionen har vedtaget flere forskellige sæt standardkontraktbestemmelser, der kan anvendes i forbindelse med tredjelandsoverførsler, og som derfor vil blive inddraget i nærværende afhandling. For det første kan nævnes 2001-bestemmelserne, der suppleres af 2004-bestemmelserne. For det andet 2010-bestemmelserne, der skal anvendes ved overførsler til databehandlere etableret i tredjelandet.[22]

I nærværende sammenhæng kan også et fjerde sæt standardkontraktbestemmelser nævnes, nemlig 2020-bestemmelserne. I skrivende stund er 2020-bestemmelserne endnu ikke endeligt vedtaget af Kommissionen. Bestemmelserne er udelukkende et udkast, og som Kommissionen selv påpeger, udtrykker de derfor ikke Kommissionens endelige opfattelse.[23] Uanset dette er 2020-bestemmelserne publiceret efter EU-Domstolen dom i Schrems II, og der henvises da også til Schrems II i bestemmelsernes fodnoter.[24] Derfor kan 2020-bestemmelserne anvendes til at illustrere, hvilken indvirkning den pågældende dom har på Kommissionens umiddelbare forståelse af, hvordan den dataansvarlige bør anvende standardbestemmelserne. Desuden lægges der i 2020-bestemmelserne op til, at de efter deres vedtagelse skal ophæve de øvrige standardbestemmelser efter en overgangsperiode på et år regnet fra ikrafttrædelsesdatoen.[25] På baggrund af disse bemærkninger vil 2020-bestemmelserne blive inddraget i afhandlingen.

[21] Udsen, Henrik, *IT-ret*, 4. udgave, 1. oplag, 2019, s. 448; EDPB, *Retningslinjer 2/2018 vedrørende undtagelser i artikel 49 i forordning 2016/679*, 25. maj 2018, s. 4 f.
[22] 2001-bestemmelserne, betragtning 8; 2010-bestemmelserne, betragtning 8 og 9.
[23] BILAG B, s. 1.
[24] BILAG B, s. 2, fodnote 2 og 3; BILAG B, s. 4, fodnote 9; BILAG B, s. 6, fodnote 10.
[25] BILAG B, s. 8 f., article 6.

3.4. Betydningen af det amerikanske reguleringssystem samt folkeretten

Da nærværende afhandling har tredjelandsoverførsler til USA i fokus, vil kilder fra det amerikanske reguleringssystem ligeledes blive inddraget. Amerikansk ret kan ikke karakteriseres som gældende dansk ret. Det er dog karakteristisk for mange persondataretlige problemstillinger, at de ikke er autonome eller rene, men opstår i sammenhæng med anden retlig regulering, der fungerer som baggrundsret.[26] Den dataansvarlige kan udelukkende anvende Kommissionens standardkontraktbestemmelser i forbindelse med tredjelandsoverførsler til USA, såfremt den registrerede, hvis personoplysninger overføres til USA, sikres et databeskyttelsesniveau, der i det væsentlige svarer til beskyttelsen efter EU-retten.[27] Det amerikanske beskyttelsesniveau som fastsat i den amerikanske lovgivning har derfor betydning ved besvarelsen af problemformuleringen.

Fra det amerikanske reguleringssystem vil den amerikanske forfatning samt tilknyttet praksis fra den amerikanske højesteret blive inddraget. Derudover vil amerikansk sikkerhedslovgivning indgå, navnlig FISA Section 702, E.O. 12333 samt PPD-28. FISA Section 702 er føderal lovgivning, der gælder på tværs af de enkelte amerikanske delstater. E.O. 12333 samt PPD-28 kan karakteriseres som henholdsvis et præsidentielt dekret og et præsidentielt direktiv udstedt af den amerikanske præsident. Disse retlige instrumenter kan sidestilles med føderal lovgivning.[28] I medfør af forfatningens art. VI, stk. 2, er forfatningen den højest rangerede retskilde i amerikansk ret, og øvrig lovgivning, herunder føderal lovgivning og de enkelte amerikanske delstaters forfatninger, må derfor ikke være i strid med denne. Føderal lovgivning går forud for lovgivning på delstatsniveau.[29]

Da en tredjelandsoverførsel fra et EU-medlemsland som Danmark til USA involverer flere stater i det internationale verdenssamfund, vil kilder fra det folkeretlige reguleringssystem ligeledes blive inddraget. For så vidt angår det generelle forhold mellem folkeret og dansk ret hviler dansk forfatningsret på en dualistisk opfattelse. Grundlæggende skal folkeretten og dansk ret således anskues

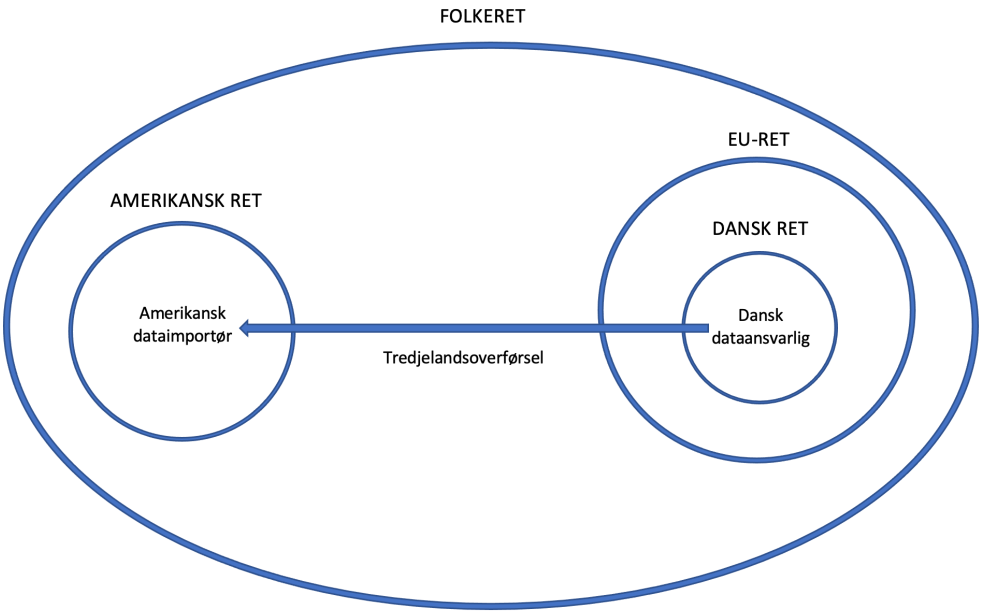
[26] Blume, Peter, *Persondatarettens kilder og metode*, 1. udgave, 1. oplag, 2020, s. 24.
[27] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 105.
[28] Patel, Oliver og Lea, Nathan, *EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows*, 2020, s. 23; USA.gov, *How Laws Are Made and How to Research Them,* https://www.usa.gov/how-laws-are-made (sidst besøgt: 4/5 2021); CRS, *Presidential Directives: An Introduction*, 2019.
[29] National Constitution Center, *The Supremacy Clause*, https://constitutioncenter.org/interactive-constitution/interpretation/article-vi/clauses/31 (sidst besøgt: 4/5 2021).

som separate retssystemer, hvor folkeretten som udgangspunkt kun regulerer staters indbyrdes forhold.[30] Med henblik på at undersøge EU-medlemslandenes og USA's indbyrdes forhold på persondatarettens område vil navnlig CPR-Konventionen blive inddraget. Denne konvention er en multilateral traktat vedtaget af FN's Generalforsamling i 1966. Konventionen er væsentlig, dels fordi den er ratificeret af samtlige EU-medlemslande og USA, dels fordi den i art. 17 bl.a. fastslår en grundlæggende ret til ikke at være genstand for vilkårlig eller ulovlig indblanding i privatliv.[31] Da bestemmelsen også indebærer en ret til beskyttelse af personoplysninger, kan konventionen siges at udgøre den folkeretlige ramme om den dataansvarliges tredjelandsoverførsler til USA.[32]

I kraft af Danmarks medlemskab af EU er Danmark ikke kun medlem af folkeretssamfundet direkte som nationalstat, men også indirekte via EU, der også er folkeretssubjekt.[33] EMRK er således ratificeret og inkorporeret i dansk lov, mens EU har underskrevet den pågældende konvention. Med henvisning til EU-rettens særlige karakteristika og autonomi har EU-Domstolen imidlertid slået fast, at tiltrædelsen på nuværende tidspunkt er i strid med EU's traktatgrundlag.[34] EMRK er derfor ikke en formel del af EU-retten. Ifølge EU-Domstolen skal vurderingen af EU-retsakter, herunder GDPR, derfor udelukkende vurderes i lyset af Chartret og ikke EMRK.[35] Da EMRK ydermere ikke er tiltrådt af USA, vil EMRK ikke ligesom CPR-Konventionen være en del af den folkeretlige ramme om den dataansvarliges tredjelandsoverførsler til USA. EMRK vil derfor ikke blive inddraget i afhandlingen.

Det overordnede samspil mellem reguleringssystemerne ved tredjelandsoverførsler fra den dataansvarlige i Danmark til dataimportøren i USA kan illustreres med nedenstående figur:

[30] Rytter, Jens Elo, *Individets grundlæggende rettigheder*, 3. udgave, 1. oplag, 2019, s. 62.
[31] United Nations Treaty Collection, *4. International Covenant on Civil and Political Rights*, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en#EndDec (sidst besøgt: 6/5 2021).
[32] Taylor, Paul M., *A Commentary on the International Covenant on Civil and Political Rights*, 2020, s. 471 ff.
[33] Tvarnø, Christina D. og Nielsen, Ruth, *Retskilder og retsteorier*, 5. reviderede udgave, 1. oplag, 2017, s. 125.
[34] EU-Domstolen, *Udtalelse 2/13 af 18. december 2014*, præmis 258.
[35] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 98 og 99.



Figur 1. Samspil mellem reguleringssystemer

4. Schrems II-dommen og dens baggrund

Databeskyttelsesdirektivet, der i dag er erstattet af GDPR, blev vedtaget i 1995. Da USA ikke havde en generel lovgivning om beskyttelse af personoplysninger, stod det allerede på dette tidspunkt klart, at USA ikke sikrede et tilstrækkeligt beskyttelsesniveau i direktivets forstand. Danske dataansvarlige havde således ikke umiddelbart mulighed for at overføre personoplysninger til USA i medfør af PDL § 27, stk. 1, der ligesom den nugældende GDPR art. 45 ellers muliggjorde persondataoverførsler til tredjelande, som ifølge en afgørelse fra Kommissionen kunne karakteriseres som et sikkert tredjeland. Med henvisning til den fremtrædende rolle, som USA spiller i den digitale økonomi og på det digitale marked og dermed vigtigheden af dataudveksling europæiske og amerikanske virksomheder imellem, måtte der imidlertid findes en løsning. Denne løsning blev den såkaldte "*Safe Harbor*"-ordning, som amerikanske virksomheder frivilligt kunne tilmelde sig. De tilmeldte amerikanske virksomheder var forpligtede til at iagttage en række principper om behandling af personoplysninger, der fulgte af ordningen. I medfør af Kommissionens Beslutning 2000/520, som Kommissionen i juli 2000 vedtog med hjemmel i databeskyttelsesdirektivets art. 25, stk. 6, havde de tilmeldte amerikanske virksomheder herefter et tilstrækkeligt beskyttelsesniveau. Efter

Kommissionens opfattelse var de amerikanske virksomheder dermed en sikker havn for europæiske borgeres personoplysninger.[36]

Med Edward Snowdens afsløringer i 2013 blev der imidlertid lækket oplysninger om to højteknologiske overvågningsprogrammer drevet af de amerikanske efterretningstjenester, navnlig NSA: "*Prism*" og "*Upstream*". Begge programmer har til formål at indsamle kommunikation fra personer, men gør det på forskellige måder. Hvor Prism har til formål at indsamle kommunikationen direkte fra amerikanske virksomheder, indsamler Upstream oplysningerne fra internettets infrastruktur som eksempelvis internetkabler, mens oplysningerne er i transit til USA.[37]

På denne baggrund indgav internetaktivisten Max Schrems i juni 2013 en klage over Kommissionens Beslutning 2000/520 til det irske datatilsyn, DPC. Baggrunden for klagen var, at irske Facebook Ireland overførte personoplysninger om europæiske borgere til amerikanske Facebook Inc., der var tilmeldt Safe Harbor-ordningen. Schrems mente ikke, at den amerikanske lovgivning og praksis sikrede en tilstrækkelig beskyttelse af de personoplysninger, der blev opbevaret i USA, mod de amerikanske efterretningstjenesters overvågningsvirksomhed. DPC afviste klagen med henvisning til, at vurderingen af tilstrækkeligheden af databeskyttelsen i USA skulle afgøres i overensstemmelse med Beslutning 2000/520, og at Kommissionen i denne beslutning havde fastslået, at USA sikrede et tilstrækkeligt beskyttelsesniveau. På denne baggrund anlagde Schrems sag ved den øverste retsinstans i Irland, High Court, som i 2014 indgav EU-Domstolen to præjudicielle spørgsmål. Begge spørgsmål relaterede sig til de nationale tilsynsmyndigheders kompetence til at vurdere tredjelandes beskyttelsesniveau.[38]

I Schrems I-dommen afsagt d. 6. oktober 2015 fastlog EU-Domstolen, at en afgørelse som Kommissionens Beslutning 2000/520 ikke er til hinder for, at de nationale tilsynsmyndigheder kan foretage en selvstændig vurdering af, om et tredjeland rent faktisk sikrer et tilstrækkeligt beskyttelsesniveau.

[36] Beslutning 2000/520, art. 1; Blume, Peter, *Den nye persondataret*, 2. udgave, 1. oplag, 2018, s. 186 ff.; Udsen, Henrik, *IT-ret*, 4. udgave, 1. oplag, 2019, s. 440.
[37] Gregory, Anthony, *American Surveillance*, 2016, s. 107 ff.; Fieldfisher, *US surveillance: s702 FISA, EO 12333, PRISM and UPSTREAM,* https://www.fieldfisher.com/en/insights/us-surveillance-s702-fisa-eo-12333-prism-and-ups (sidst besøgt: 5/5 2021).
[38] EU-Domstolen, Sag C-362/14, *Schrems,* præmis 27-30 og 36.

Derudover indeholdt dommen et vigtigt obiter dictum: På trods af, at den irske High Court ikke direkte havde forelagt EU-Domstolen spørgsmålet, fastslog EU-Domstolen, at Beslutning 2000/520 var ugyldig.[39]

EU-Domstolen fastslog indledningsvist, at kravet om et tilstrækkeligt beskyttelsesniveau i databeskyttelsesdirektivets art. 25, stk. 6, skulle forstås således, at tredjelandets lovgivning skulle sikre et databeskyttelsesniveau, der "*i det væsentlige*" svarer til det niveau, der er sikret inden for EU efter databeskyttelsesdirektivet sammenholdt med Chartret.[40] EU-Domstolen konstaterede herefter, at principperne i Safe Harbor-ordningen ikke kunne forhindre amerikanske offentlige myndigheders indsamling af personoplysninger som led i overvågning, da den amerikanske sikkerhedslovgivning gik forud for ordningen. De amerikanske virksomheder tilmeldt ordningen kunne derfor tilpligtes at se bort fra ordningen, såfremt denne var i modstrid med den amerikanske lovgivning.[41] EU-Domstolen henviste herefter til det sikrede beskyttelsesniveau inden for EU som fastsat i Chartret samt den tilknyttede praksis og fastslog, at en lovgivning, der på generel vis tillader masseindsamling af samtlige personoplysninger, der overføres fra EU til USA, uden at der bliver foretaget nogen form for differentiering, begrænsning eller undtagelse, vil være i strid med Chartrets art. 7 om retten til respekt for privatliv og familieliv samt art. 8 om retten til beskyttelse af personoplysninger. Derudover slog EU-Domstolen fast, at en manglende adgang for europæiske borgere til en effektiv domstolsbeskyttelse mod en uberettiget brug af personoplysninger vil være i strid med Chartrets art. 47 om adgang til effektive retsmidler.[42] Allerede fordi, at Kommissionen i forbindelse med vedtagelsen af Beslutning 2000/520 ikke havde foretaget en tilstrækkelig analyse af, om USA faktisk sikrede et beskyttelsesniveau, der i det væsentligste svarede til beskyttelsen efter EU-retten, fandt EU-Domstolen herefter ikke, at beslutningen var i overensstemmelse med databeskyttelsesdirektivets art. 25, stk. 6, sammenholdt med Chartret.[43] EU-Domstolen fandt det således unødvendigt at foretage en nærmere vurdering af den konkrete amerikanske sikkerhedslovgivning.

[39] EU-Domstolen, Sag C-362/14, *Schrems,* præmis 107.
[40] EU-Domstolen, Sag C-362/14, *Schrems,* præmis 73.
[41] EU-Domstolen, Sag C-362/14, *Schrems,* præmis 82-87.
[42] EU-Domstolen, Sag C-362/14, *Schrems,* præmis 91-95.
[43] EU-Domstolen, Sag C-362/14, *Schrems,* præmis 96-98.

Med EU-Domstolens tilsidesættelse af Beslutning 2000/520 kunne Safe Harbor-ordningen ikke længere anvendes som et gyldigt overførselsgrundlag. På denne baggrund udarbejdede Kommissionen og den amerikanske regering herefter en ny rammeaftale, der skulle afløse Safe Harbor-ordningen: "*Privacy Shield*". Denne nye ordning havde til hensigt at håndtere manglerne i Safe Harbor-ordningen. Med ordningen blev der bl.a. indført en ny ombudsmandsmekanisme for nationale sikkerhedsforanstaltninger, der skulle sikre, at kravene efter Chartrets art. 47 ville blive efterlevet. Desuden indeholdt ordningen beskrivelser af begrænsningerne i de amerikanske myndigheders adgang til de overførte personoplysninger.[44] Ved Gennemførelsesafgørelse 2016/1250 traf Kommissionen i juli 2016 beslutning om, at Privacy Shield sikrede et tilstrækkeligt beskyttelsesniveau.[45] Dermed kunne ordningen ifølge Kommissionen anvendes som overførselsgrundlag i forbindelse med tredjelandsoverførsler til de amerikanske virksomheder, der tilmeldte sig ordningen og dermed underlagde sig de indeholdte databeskyttelsesprincipper.

Efter Schrems I-dommen valgte Facebook Ireland imidlertid at overføre en stor del af de personoplysninger, der blev overført til Facebook Inc., på grundlag af Kommissionens standardkontraktbestemmelser, nærmere bestemt 2010-bestemmelserne. På denne baggrund formulerede Max Schrems en ny klage til DPC, som han indgav d. 1. december 2015. Schrems gjorde atter gældende, at Facebook Inc. efter amerikansk sikkerhedslovgivning skal stille de personoplysninger, der overføres til Facebook Inc., til rådighed for de amerikanske efterretningstjenester, og at disse myndigheder anvendte oplysningerne i strid med Chartrets art. 7, 8 og 47. Schrems gjorde følgelig gældende, at 2010-bestemmelserne ikke kunne begrunde overførslen af disse personoplysninger til USA, og han anmodede derfor DPC om at forbyde eller suspendere overførslen af hans personoplysninger til Facebook Inc.[46]

DPC gav i et udkast til afgørelse udtryk for, at Schrems' nye klage rejste spørgsmål om gyldigheden af 2010-bestemmelserne. DPC indbragte derfor sagen for High Court, og i maj 2018 indgav High Court elleve præjudicielle spørgsmål til EU-Domstolen, som alle relaterede sig til gyldigheden af

[44] Udsen, Henrik, *IT-ret*, 4. udgave, 1. oplag, 2019, s. 442; EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 43.
[45] Gennemførelsesafgørelse 2016/1250, art. 1, stk. 1.
[46] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 54-55.

2010-bestemmelserne.[47] Det var disse spørgsmål, der dannede grundlag for Schrems II-dommen, og d. 16. juli 2020 afsagde EU-Domstolen dom.

EU-Domstolen lod historien gentage sig en-til-en. På trods af den kendsgerning, at High Court ikke direkte havde forelagt EU-Domstolen spørgsmålet om gyldigheden af Privacy Shield, fastslog Domstolen, at Kommissionens Gennemførelsesafgørelse 2016/1250 var ugyldig og i strid med GDPR art. 45, stk. 1, sammenholdt med Chartrets art. 7, 8 og 47.[48] EU-Domstolen henviste i denne forbindelse til sin første dom i Schrems I og understregede den grundlæggende problematik forbundet med Privacy Shield-ordningen: Amerikansk sikkerhedslovgivning havde forrang.[49]

Således kunne heller ikke Privacy Shield-ordningen anvendes som gyldigt overførselsgrundlag. Fra den ene dag til den anden blev tæppet derfor trukket væk under de ca. 5.300 amerikanske virksomheder, der havde tilsluttet sig ordningen, samt de europæiske virksomheder, der anvendte ordningen som overførselsgrundlag.[50] Schrems II-dommen indeholdt dog også et væsentligt lyspunkt: EU-Domstolen fandt det ikke nødvendigt at tilsidesætte 2010-bestemmelserne som ugyldige.[51] I denne henseende fulgte EU-Domstolen således generaladvokaten, der i sit forslag til afgørelse afgivet året forinden var nået til samme konklusion.[52] Umiddelbart efterlod Schrems II-dommen således Kommissionens standardkontraktbestemmelser som et særdeles relevant overførselsgrundlag at tage i betragtning, når den dataansvarlige ønsker at gennemføre en tredjelandsoverførsel til USA.

5. Europæernes grundlæggende rettigheder og den amerikanske overvågning

Som EU-Domstolens domme i henholdsvis Schrems I og II illustrerer, var det den amerikanske sikkerhedslovgivning og dennes forrang for principperne i både Safe Harbor- og Privacy Shield-ordningen, der fik EU-Domstolen til at tilsidesætte de pågældende ordninger. Det kan derfor konstateres, at det netop er den amerikanske sikkerhedslovgivning, der har særlig vigtig betydning for den

[47] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 56, 57 og 68.
[48] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 199-201 og 203.
[49] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 164 og 165.
[50] Patel, Oliver, og Nathan, Lea, *EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows*, 2020, s. 3.
[51] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 122 og 203.
[52] Generaladvokat H. Saugmandsgaard Øe, *Forslag til afgørelse*, 19. december 2019, afsnit 121 og 160.

dataansvarliges muligheder for at gennemføre en tredjelandsoverførsel til USA. På denne baggrund skal det undersøges, i hvilket omfang grundlæggende rettigheder efter henholdsvis det EU-retlige, amerikanske og folkeretlige reguleringssystem hjemler en beskyttelse mod den databehandling af europæiske personoplysninger, som de amerikanske myndigheder foretager som led i overvågning af hensyn til den nationale sikkerhed. Dette vil ske med henblik på at afdække de retlige barrierer på grundrettighedsniveau, der måtte gøre sig gældende, når den dataansvarlige anvender Kommissionens standardkontraktbestemmelser som overførselsgrundlag ved tredjelandoverførsler til USA.

5.1. De grundlæggende rettigheder efter Chartret

Ved undersøgelsen af, i hvilket omfang europæerne efter EU-retten ydes en beskyttelse mod den databehandling, som nationale myndigheder foretager af hensyn til den nationale sikkerhed, er TEU art. 4 omhandlende bl.a. forholdet mellem EU og medlemsstaterne central. Efter TEU art. 4, stk. 2, 2. pkt., fremgår det, at EU respekterer medlemsstaternes "*centrale statslige funktioner, herunder sikring af statens territoriale integritet, opretholdelse af lov og orden samt beskyttelse af den nationale sikkerhed.*" I bestemmelsens sidste pkt. fastslås det udtrykkeligt, at navnlig den nationale sikkerhed forbliver den enkelte medlemsstats eneansvar. Sammenholdes dette med TEU art. 6, stk. 1, 2. pkt., hvoraf det fremgår, at Chartrets bestemmelser ikke på nogen måde udvider EU's beføjelser som fastsat i traktaterne, finder Chartrets bestemmelser således ej heller anvendelse på tilfælde, der kan henføres til medlemsstaternes sikkerhedsanliggender. At dette også gælder i relation til behandling af personoplysninger, tydeliggøres af GDPR art. 2, stk. 2, litra a, hvorefter GDPR ikke gælder for behandling af personoplysninger, som finder sted under udøvelse af aktiviteter, der falder uden for EU-retten. I præambelbetragtning 16 nævnes udtrykkeligt aktiviteter vedrørende statens sikkerhed som et eksempel.

Det står således klart, at europæerne ikke på EU-retligt niveau hjemles rettigheder til beskyttelse mod den persondatabehandling, som de enkelte EU-medlemsstater gennemfører af hensyn til den nationale sikkerhed, eksempelvis i forbindelse med overvågningsforanstaltninger. Det skal imidlertid bemærkes, at denne væsentlige undtagelse udelukkende vedrører EU-medlemsstater, der er omfattet af TEU og derfor ikke tredjelande uden for EU. Denne kendsgerning skal sammenholdes med behandlingsbegrebet i GDPR. Efter GDPR art. 2, stk. 1, finder forordningen anvendelse på

"*behandling af personoplysninger*", og efter legaldefinitionen i art. 4, nr. 2, vil en "*behandling*" bl.a. kunne bestå i "*videregivelse ved transmission, formidling eller enhver anden form for overladelse*". I præmis 82 i Schrems II-dommen bemærker EU-Domstolen, at der i denne definition ikke sondres mellem, om aktiviteterne foretages inden for EU eller har forbindelse til et tredjeland. Videre fastslår EU-Domstolen i præmis 83, at den transaktion, der består i at overføre personoplysninger fra en EU-medlemsstat til et tredjeland, vil udgøre en behandling af personoplysninger foretaget på en medlemsstats område omfattet af anvendelsesområdet i GDPR.

Samlet følger det af ovenstående, at EU-medlemsstaters behandling af personoplysninger som led i overvågning foretaget af hensyn til nationens sikkerhed ikke er omfattet af EU-retten. I det øjeblik, at den dataansvarlige foretager en tredjelandsoverførsel, vil EU-retten, herunder GDPR og de grundlæggende rettigheder Chartret, imidlertid finde anvendelse. Dette uanset, om myndighederne i tredjelandet behandler de overførte oplysninger til formål, der ellers ikke er omfattet af EU-retten. I denne sammenhæng kan EU-retten følgelig siges at pålægge tredjelande, herunder USA, større krav end den gør i relation til EU's egne medlemsstater.

Schrems I og II illustrerer, at det i EU-retten er Chartret, som EU-Domstolen tillægger styrende betydning i forbindelse med vurderingen af tredjelandsoverførsler til USA. På denne baggrund skal det afsøges, hvilken konkret beskyttelse Chartret yder mod den amerikanske overvågning af europæere, der gennemføres på baggrund af den amerikanske sikkerhedslovgivning. Central i denne forbindelse er Schrems II-dommens præmis 168-202. I modsætning til sin tidligere dom i Schrems I tager EU-Domstolen her udtrykkeligt stilling til konkret amerikansk sikkerhedslovgivning i forbindelse med sin vurdering af Gennemførelsesafgørelse 2016/1250 og denne afgørelses forenelighed med GDPR art. 45, stk. 1, sammenholdt med Chartrets 7, 8 og 47. I de pågældende præmisser er det FISA Section 702, E.O. 12333 og PPD-28, som EU-Domstolen finder relevant at tage i betragtning.

Med henvisning til EU-Domstolens øvrige praksis slår EU-Domstolen indledningsvist fast, at selve adgangen til personoplysninger om en fysisk person med henblik på opbevaring og brug udgør et indgreb i både retten til privatliv efter art. 7 samt retten til beskyttelse af personoplysninger efter art. 8. Dette med henvisning til, at en sådan adgang indebærer en behandling af personoplysninger,

der omfattes af beskyttelsesområdet i art. 8, og at retten til privatliv efter art. 7 vedrører enhver form for information om en identificeret eller identificerbar fysisk person.[53] EU-Domstolen indfortolker således et særdeles bredt materielt beskyttelsesområde i både art. 7 og 8, der svarer til det tilsvarende brede beskyttelsesområde i GDPR, der finder anvendelse ved behandling af personoplysninger.

EU-Domstolen konstaterer imidlertid, at rettighederne i art. 7 og 8 ikke er absolutte. I denne forbindelse henviser EU-Domstolen til proportionalitetsprincippet i Chartrets art. 52, stk. 1, 2. pkt., hvorefter ethvert indgreb i rettighederne efter Chartret skal begrænses til det nødvendige.[54] Hvilke krav national lovgivning, der hjemler indgreb i Chartrets rettigheder, konkret skal overholde for at være i overensstemmelse med proportionalitetsprincippet, fremgår af Schrems II-dommens præmis 175 og 176. Her fastslår EU-Domstolen, at lovgivningen skal indeholde klare og præcise regler, der selv definerer rækkevidden af begrænsningen i rettighederne som fastsat i Chartret. Derudover skal lovgivningen opstille en række mindstekrav, således at de personer, hvis personoplysninger er blevet overført, råder over tilstrækkelige garantier, der gør det muligt at beskytte deres personoplysninger mod misbrug. Ifølge EU-Domstolen indebærer dette, at lovgivningen navnlig skal angive, under hvilke omstændigheder og på hvilke betingelser, der kan behandles personoplysninger, så det sikres, at indgrebet begrænses til det "*strengt nødvendige*".

EU-Domstolen sammenholder herefter de ovennævnte krav med den amerikanske sikkerhedslovgivning. I Schrems II-dommen konstaterer EU-Domstolen, at FISA Section 702 og E.O. 12333 er den lovgivning, der hjemler overvågningsprogrammerne Prism og Upstream.[55]

FISA Section 702 giver de amerikanske efterretningstjenester mulighed for at anmode amerikanske virksomheder om indsigt i de data, virksomhederne måtte opbevare.[56] For så vidt angår denne lovgivning fremhæver EU-Domstolen i præmis 179 Kommissionens egne betragtninger til Gennemførelsesafgørelse 2016/1250. Ifølge disse betragtninger kræver FISA Section 702 ikke, at FISC, den

[53] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 170 og 171.
[54] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 172 og 174.
[55] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 165.
[56] 50 U.S.C. § 1881a(a),(i)(1) (2018).

amerikanske domstol, der skal godkende overvågning i henhold til FISA, skal foretage en individuel vurdering af, om de enkelte fysiske personer er velegnede mål for indsamlingen af personoplysningerne. FISC skal derimod udelukkende vurdere, om overvågningen er i overensstemmelse med det generelle formål om at indhente udenlandske efterretningsoplysninger. Dermed adresserer EU-Domstolen én af de bestemmelser i FISA Section 702, der ellers har til formål at begrænse den amerikanske overvågning. Af Section 702 fremgår det således, at FISC udelukkende kan godkende indsamling af oplysninger, der netop vedrører "*udenlandske efterretningsoplysninger*".[57] Denne type oplysninger defineres imidlertid særdeles bredt og omfatter ikke kun oplysninger, der er nødvendige at indsamle af hensyn til den nationale sikkerhed, men eksempelvis også enhver information fra en fremmed magt eller et fremmed territorium, der blot relaterer sig til udøvelsen af udenrigsanliggender.[58] Ligeledes indeholder Section 702 den begrænsning, at FISC udelukkende kan godkende indsamling af oplysninger fra en "*elektronisk kommunikationsudbyder*".[59] Denne definition kan dog omfatte enhver virksomhed, der giver andre, herunder virksomhedens egne ansatte, adgang til at kommunikere elektronisk via eksempelvis e-mail. Dette uanset hvad der ellers måtte være virksomhedens primære forretningsområde.[60] På denne baggrund forekommer det berettiget, når EU-Domstolen i præmis 180 fastslår, at FISA Section 702 "*på ingen måde*" fastsætter begrænsninger i relation til overvågningsprogrammerne, når der indhentes udenlandske efterretningsoplysninger, og heller ikke fastsætter garantier for ikke-amerikanere, som potentielt kan være omfattet af overvågningen.

Hvad angår E.O. 12333 fremhævede den forelæggende ret, den irske High Court, at de amerikanske efterretningstjenester efter dette dekret har adgang til oplysninger i transit til USA ved at tilgå de undersøiske kabler, der ligger på havbunden i Atlanterhavet. Dette indebærer, at efterretningstjenesterne har adgang til at indsamle og opbevare oplysninger, før de når til USA og dér bliver undergivet bestemmelserne i FISA. Overvågningsaktiviteterne udført på baggrund af E.O. 12333 er således ikke reguleret ved lov.[61] Dette kan forklare, at EU-Domstolen i præmis 182 og 183 ganske kortfattet

[57] 50 U.S.C. § 1881a(h)(2)(A)(v) (2018).
[58] 50 U.S.C. § 1801(e)(2)(B) (2018).
[59] 50 U.S.C. § 1881a(h)(2)(A)(vi) (2018).
[60] Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,* s. 117.
[61] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 63.

fastslår, at E.O.12333 ikke giver de registrerede rettigheder, som kan håndhæves overfor de amerikanske myndigheder ved domstolene, ligesom overvågningen baseret på E.O. 12333 ikke er underlagt noget retsligt tilsyn. At EU-Domstolen ved sin vurdering af E.O. 12333 tillægger det retslige tilsyn vægt må ses i sammenhæng med Chartrets art. 8, stk. 3, der udtrykkeligt fastslår, at overholdelsen af art. 8 skal underlægges en uafhængig myndigheds kontrol.

I Schrems II-dommen foretager EU-Domstolen ligeledes en vurdering af PPD-28, som skal være overholdt i forbindelse med den indsamling, der finder sted med hjemmel i FISA Section 702 og E.O. 12333. PPD-28 blev udstedt i kølvandet på Snowden-afsløringerne og har til formål at begrænse overvågningen af ikke-amerikanere.[62] I præmis 181 fastslår EU-Domstolen først og fremmest, at PPD-28 ikke giver de registrerede rettigheder, som kan håndhæves over for de amerikanske myndigheder ved domstolene. Derudover konstaterer EU-Domstolen i præmis 183, at PPD-28 tillader "*masseindsamling*" af oplysninger under omstændigheder, hvor efterretningstjenesterne ikke har mulighed for at målrette indsamlingen. EU-Domstolen sammenholder denne adgang til masseindsamling med de ulovregulerede og dermed ubegrænsede beføjelser efter E.O. 12333 og konstaterer, at PDD-28 på denne baggrund ikke tilstrækkeligt klart og præcist afgrænser indsamlingen.

På baggrund af ovenstående betragtninger fastslår EU-Domstolen herefter, at hverken FISA Section 702 eller E.O. 12333, sammenholdt med PPD-28, opfylder de krav til national lovgivning, der gælder efter proportionalitetsprincippet i Chartrets art. 52, stk. 1, 2. pkt. Ifølge EU-Domstolen kan det derfor ikke fastslås, om den amerikanske overvågning er begrænset til det strengt nødvendige. Af denne grund lever lovgivningen ikke op til de krav, som i det væsentlige svarer til dem, der fremgår af EU-retten.[63]

Det står herefter klart, at det netop er proportionalitetsprincippet efter Chartrets art. 52, stk. 1, 2. pkt., som EU-Domstolen tillægger afgørende betydning ved sin vurdering af, om den amerikanske sikkerhedslovgivning sikrer et tilstrækkeligt beskyttelsesniveau efter Chartrets art. 7 og 8. Ligeledes illustrerer EU-Domstolens præmisser, at dette proportionalitetsprincip ikke alene indebærer en

[62] CRS, Report R46724, *EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield*, 2021, s. 11 f.
[63] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 184 og 185.

vurdering af, om overvågningen går videre end strengt nødvendigt. Om overvågningen kan overholde dette materielle krav forudsætter, at selve lovgivningen, der hjemler overvågningen, lever op til en række formelle krav, herunder at lovgivningen skal være tilstrækkeligt klar og præcis. Det er netop disse formelle krav, som den amerikanske sikkerhedslovgivning ifølge EU-Domstolen ikke overholder. Lovgivningen er mangelfuld, og allerede af denne grund sikrer den ikke et tilstrækkeligt beskyttelsesniveau.

Parallelt med ovenstående vurdering af Chartrets art. 7, 8 og 52, sammenholder EU-Domstolen også den amerikanske lovgivning med Chartrets art. 47 om adgang til effektive retsmidler. Med henvisning til fast retspraksis, herunder sin tidligere dom i Schrems I, fastslår EU-Domstolen i præmis 187, at "*selve eksistensen*" af en effektiv domstolsbeskyttelse er "*uløseligt forbundet*" med eksistensen af en retsstat. En lovgivning, der ikke fastsætter nogen mulighed for at gøre brug af retsmidler med henblik på at få adgang til personoplysninger, som vedrører den pågældende, eller til at få sådanne oplysninger berigtiget eller slettet, opfylder derfor ikke den grundlæggende rettighed i Chartrets art. 47.[64] I præmis 192 henviser EU-Domstolen til ovennævnte præmis 181 og 182, hvorefter hverken E.O. 12333 eller PPD-28 giver de registrerede adgang til effektive retsmidler, der kan håndhæves ved domstolene. Eksistensen af en effektiv domstolsbeskyttelse, og ifølge EU-Domstolen dermed også en retsstat, er således helt fraværende i USA. Dette kan forklare, at EU-Domstolen i relation til sin vurdering af den amerikanske lovgivnings overensstemmelse med Chartrest art. 47 finder det unødvendigt at foretage en proportionalitetsafvejning, som den ellers gjorde i forbindelse med sin vurdering af Chartrets art. 7 og 8.

Som EU-Domstolens ovenstående præmisser illustrerer, kan der af Chartret således udledes flere grundlæggende rettigheder, som den amerikanske sikkerhedslovgivning ikke overholder.

5.2. De grundlæggende rettigheder efter den amerikanske forfatning

Hvorvidt der i det amerikanske reguleringssystem gælder grundlæggende rettigheder, der relaterer sig til beskyttelse af personoplysninger, er ikke lige så klart, som det er tilfældet inden for EU-retten.

[64] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 187.

Dette skyldes, at den amerikanske forfatning i modsætning til Chartret ikke indeholder nogen eksplicit beskyttelse af privatlivet. På grundlag af første, tredje, fjerde, femte og niende tilføjelse til forfatningen er der i amerikansk højesteretspraksis imidlertid blevet udledt en vis privatlivsbeskyttelse.[65]

Når det konkret gælder spørgsmålet om privatlivsbeskyttelse relaterende til overvågning foretaget af de amerikanske myndigheder, er det forfatningens fjerde tilføjelse omhandlende ransagning og beslaglæggelse, der påkalder sig interesse.[66] Tilføjelsen har følgende ordlyd:

> "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*"[67]

Den mest betydningsfulde praksis relaterende til privatlivsbeskyttelse er en række sager afgjort af Højesteretten, der har taget stilling til lovligheden af telefonaflytning.[68] I Olmstead-sagen afsagt af Højesteretten i 1928 fastslog fem ud af ni dommere, at telefonaflytning med henblik på at fremskaffe beviser som led i retshåndhævelse ikke var omfattet af beskyttelsesområdet i den fjerde tilføjelse. Dette bl.a. med henvisning til, at telefonaflytningen ikke udgjorde en "*search*" (ransagning) i tilføjelsens forstand, da den enhed, der blev installeret med henblik på telefonaflytningen, ikke fysisk var placeret i borgerens hjem. I stedet blev den pågældende enhed installeret på transmissionsledninger ejet af en televirksomhed. Ifølge Højesteretten omfattede den fjerde tilføjelse således udelukkende fysisk indtrængen.[69]

---

[65] Blume, Peter, *Databeskyttelsesret*, 5. udgave, 1. oplag, 2018, s. 276.
[66] Se hertil Simmons, Ric, *Smart Surveillance – How to Interpret the Fourth Amendment in the Twenty-First Century*, 2019, s. 2; Gray, David, *The Fourth Amendment in an Age of Surveillance*, 2017, s. 23; Balkin, Jack M., *The Constitution in the National Surveillance State*, Minnesota Law Review, 93.1, 2008, s. 19 ff.
[67] U.S. Const. amend. IV.
[68] Regan, Priscilla M., *Legislating Privacy: Technology, Social Values, and Public Policy*, 1995, s. 35.
[69] Olmstead v. United States, 277 U.S. 438, 464-466 (1928).

I de følgende år efter Olmstead-sagen fastholdt Højesteretten denne fortolkning.[70] Denne praksis blev imidlertid tilsidesat i 1967 med Katz-sagen. Her fastslog Højesterettens flertal, at den fjerde tilføjelse ikke blot beskytter områder, men mennesker. Bestemmelsens anvendelsesområde kunne derfor ikke afhænge af, om der forelå en fysisk indtrængen på borgerens område eller ej. Som følge af dette fandt Højesteretten i den konkrete sag, at myndighedernes elektroniske overvågning *"violated the privacy upon which he justifiably relied"*.[71] Dermed havde Højesteretten fastslået en forfatningsmæssig beskyttelse af privatlivets fred i relation til myndighedernes overvågningsforanstaltninger i det omfang, at borgeren med rette kunne forvente privatliv. Som udgangspunkt kan myndighederne herefter ikke gøre indgreb i dette privatliv uden at opnå en retskendelse udstedt med "*probable cause"* i overensstemmelse med det udtrykkelige krav i den fjerde tilføjelse.[72] Hvorvidt dette krav om retskendelse kan fraviges i forbindelse med tilfælde relaterende til den nationale sikkerhed, tog Højesteretten stilling til i United States Dist. Ct.-sagen, der blev afsagt fem år efter Katz-sagen. Her fastlog en enstemmig Højesteret, at kravet om en retskendelse gælder i forbindelse med indenrigsefterforskninger, uanset om efterforskningen sker af hensyn til den nationale sikkerhed.[73]

Katz-sagen kan således umiddelbart anskues som en højesteretssag, der tillægger den fjerde tilføjelse en sådan fortolkning, at den hjemler en vis beskyttelse mod myndighedernes urimelige overvågningsforanstaltninger – også når behandlingen sker af hensyn til den nationale sikkerhed. Hvorvidt denne beskyttelse ligeledes gælder for europæere, skal der i denne forbindelse henvises til en væsentlig begrænsning relaterende til den fjerde tilføjelses beskyttelsessubjekt. Af tilføjelsens ordlyd fremgår det indledningsvist, at det er "*the people*", der omfattes af bestemmelsen. Med Verdugo-Urquidez-sagen fastslog Højesteretten i 1990, at ordene "*the people*" refererer til personer, der er en del af et nationalt fællesskab eller på anden måde har udviklet en så betydelig forbindelse til dette land, at vedkommende kan betragtes som en del af det nationale fællesskab. Samtidig henviser Højesteretten til præamblen til forfatningen, som indledes med "*the people of the United States*". Endelig fremhæver Højesteretten, at historisk data viser, at formålet med den fjerde tilføjelse

[70] Gray, David, *The Fourth Amendment in an Age of Surveillance*, 2017, s. 75.
[71] Katz v. United States, 389 U.S. 347, 353 (1967).
[72] Katz v. United States, 389 U.S. 347, 354-359 (1967).
[73] United States v. United States Dist. Ct., 407 U.S. 297, 320-322 (1972).

er at beskytte det amerikanske folk mod arbitrære handlinger fra deres egen regerings side, men ikke at begrænse regeringens handlinger relaterende til udlændinge uden for USA's territorium. I den konkrete sag afviste Højesteretten derfor, at en mexicaner bosat i Mexico uden relationer til USA kunne gøre den fjerde tilføjelse gældende. Dette med den afsluttende bemærkning, at den amerikanske regering på godt og ondt skal kunne agere effektivt i relation til andre nationer og imødekomme trusler, der opstår uden for de amerikanske grænser, og at eventuelle begrænsninger i dette skal ske gennem diplomati, traktater og lovgivning.[74]

Højesteretten mener altså ikke, at der skal gælde forfatningsmæssige begrænsninger i den amerikanske regerings handlemuligheder ift. trusler uden for de amerikanske grænser. Derfor gælder den fjerde tilføjelse ikke for udlændinge bosat i et fremmed land uden for USA, herunder europæere bosat i EU. Da det netop er den fjerde tilføjelse, der efter omstændighederne kan hjemle en beskyttelse mod indgreb i privatlivets fred foretaget på baggrund af de amerikanske myndigheders overvågningsforanstaltninger, efterlader den amerikanske forfatning derfor europæerne særdeles sårbare mod den amerikanske sikkerhedslovgivning og overvågning.

5.3. De grundlæggende rettigheder efter CPR-Konventionen

I CPR-Konventionens art. 17, stk. 1, fastslås det bl.a., at ingen må udsættes for vilkårlig eller ulovlig indblanding i sit privatliv. Konventionens privatlivsbegreb har en række dimensioner.[75] Menneskerettighedskomitéen, som er et kontrolorgan oprettet i henhold til CPR-Konventionen, har i en række konkluderende observationer fastslået, at også overvågningsforanstaltninger skal være i overensstemmelse med art. 17. Dette uanset hvilken nationalitet de overvågede individer har, eller hvor de befinder sig.[76]

I Menneskerettighedskomitéen kommentar 16, afsnit 3, fastslås det, at de enkelte nationalstaters indgreb i art. 17 skal ske på baggrund af en lovhjemmel, men at denne lovhjemmel samtidig skal

[74] United States v. Verdugo-Urquidez, 494 U.S. 259, 265-267, 274, 275 (1990).
[75] Taylor, Paul M., *A Commentary on the International Covenant on Civil and Political Rights*, 2020, s. 471.
[76] Taylor, Paul M., *A Commentary on the International Covenant on Civil and Political Rights*, 2020, s. 476; Storgaard, Louise Halleskov m.fl., *Folkeret og menneskerettigheder*, 1. udgave, 1. oplag, 2019, s. 196 f.

overholde bestemmelserne i og formålet med konventionen. Lovhjemmel er derfor ikke i sig selv tilstrækkeligt. Komitéen fastslår således i kommentar 16, afsnit 4, at et vilkårligt og dermed ulovligt indgreb kan finde sted, selvom der foreligger lovhjemmel, og at et indgreb for at overholde forbuddet mod vilkårlighed i hvert tilfælde skal være rimeligt under de givne omstændigheder. Forbuddet mod vilkårlighed indebærer således et rimelighedskrav, og Menneskerettighedskomitéen har i flere sager kritiseret stater for at gøre indgreb i CPR-Konventionen alene med henvisning til den nationale sikkerhed uden nærmere forklaring.[77]

Om national lovgivning, der hjemler overvågningsforanstaltninger, fastslår Menneskerettighedskomitéen specifikt, at denne lovgivning skal være klar og præcis samt begrænse indsamling og overvågning af data til det nødvendige. Derudover skal lovgivningen indeholde en effektiv beskyttelse mod misbrug. Komitéen forholder sig således kritisk til overvågningsbeføjelser, der har hjemmel i lovbestemmelser med vide og udefinerbare formål.[78] Særligt i relation til USA har komitéen i 2014, ét år efter Snowden-afsløringerne, udtrykt bekymring over de overvågningsforanstaltninger, som NSA gennemfører af hensyn til den nationale sikkerhed. Ligesom EU-Domstolen senere gjorde det i 2020 med Schrems II-dommen, nævner komitéen i denne forbindelse udtrykkeligt FISA Section 702 og PPD-28 samt overvågningsprogrammerne Prism og Upstream. Derudover udtrykker Menneskerettighedskomitéen bekymring over, at individerne omfattet af den amerikanske masseovervågning ikke har adgang til effektive retsmidler i tilfælde af misbrug. Disse manglende effektive retsmidler er ifølge komitéen ikke kun i strid med CPR-Konventionens art. 17, men også konventionens art. 2, som i stk. 3 indeholder en udtrykkelig pligt for enhver deltagende stat til at sikre adgang til effektive retsmidler. Ligeledes er de manglende effektive retsmidler i strid med art. 5, stk. 1, som indeholder et forbud mod at begrænse konventionens rettigheder i videre omfang, end konventionen hjemler. På denne baggrund opfordrer komitéen USA til at tage alle nødvendige midler i brug for at bringe de amerikanske overvågningsaktiviteter i overensstemmelse med CPR-Konventionen.[79]

[77] Taylor, Paul M., *A Commentary on the International Covenant on Civil and Political Rights*, 2020, s. 468 og 470 f.
[78] Taylor, Paul M., *A Commentary on the International Covenant on Civil and Political Rights*, 2020, s. 476 ff.
[79] Taylor, Paul M., *A Commentary on the International Covenant on Civil and Political Rights*, 2020, s. 476 f.; Menneskerettighedskomitéen, CCPR/C/USA/CO/4, *Concluding observations on the fourth periodic report of the United States of America*, 2014, afsnit 22.

Som ovenstående illustrerer, yder CPR-Konventionen europæerne en beskyttelse mod den amerikanske overvågning, som i det væsentlige ligner den beskyttelse, der fremgår af de grundlæggende rettigheder i Chartret som fortolket af EU-Domstolen i Schrems II. De amerikanske overvågningsforanstaltninger skal således også efter CPR-Konventionen være proportionel, uanset om overvågningen sker på baggrund af sikkerhedshensyn, mens reglerne, der hjemler overvågningen, skal være klare og præcise. Endelig skal lovgivningen give individerne adgang til effektive retsmidler.

5.4. Databeskyttelseskrigen

Som EU-Domstolens dom i Schrems II illustrerer, stilles der efter Chartret klare krav til persondatabehandling som led i overvågningsforanstaltninger, som den amerikanske sikkerhedslovgivning i FISA Section 702, E.O. 12333 samt PPD-28 ikke overholder. Grundet EU-medlemsstaternes eneansvar på sikkerhedsområdet gælder de pågældende krav imidlertid ikke medlemsstaterne selv, men derimod udelukkende de tredjelande, som den dataansvarlige måtte overføre personoplysninger til, herunder USA.

Dette samtidig med, at det udelukkende er amerikanske borgere, der er omfattet af beskyttelsen i den fjerde tilføjelse i den amerikanske forfatning, der ellers hjemler en grundlæggende ret til privatliv i det omfang, at dette privatliv med rette kan forventes – også når indgrebet finder sted af hensyn til den nationale sikkerhed. Konkret kan denne begrænsning i forfatningens beskyttelsessubjekt siges at skabe en forfatningsmæssig legitimation af den amerikanske sikkerhedslovgivning og masseovervågning af ikke-amerikanere, der omvendt er i strid med de grundlæggende rettigheder i Chartret.

Af ovenstående følger det, at der gælder en skarp opdeling mellem henholdsvis EU-medlemsstater og ikke-medlemsstater samt amerikanere og ikke-amerikanere ved fastlæggelsen af, hvem der er omfattet af de grundlæggende rettigheder i det EU-retlige og amerikanske reguleringssystem. Denne skarpe opdeling har dannet grobund for en databeskyttelseskrig på grundrettighedsniveau med EU og USA på hver sin side. En krig, som det internationale verdenssamfund ikke forhindrer: Samtlige EU-lande og USA har ratificeret CPR-Konventionen, som i art. 17 indeholder et forbud mod

en sikkerhedslovgivning som den amerikanske. Alligevel fejler CPR-Konventionen i at udgøre en fælles folkeretlig databeskyttelsesstandard EU og USA imellem.

Dette folkeretlige svigt skal forstås i lyset af forholdet mellem henholdsvis det amerikanske og folkeretlige reguleringssystem. Her kan fremhæves den amerikanske forfatnings art. VI, stk. 2, hvorefter de traktater, som USA måtte indgå, skal sidestilles med forbundslove og derfor skal respektere forfatningen.[80] Da forfatningen ikke hjemler en beskyttelse mod masseovervågning af europæere, afhænger europæernes beskyttelse efter det folkeretlige reguleringssystem ifølge forfatningen således ultimativt af forholdet mellem amerikanske forbundslove og CPR-Konventionen. I forbindelse med ratifikationen af CPR-Konventionen har USA erklæret, at konventionens art. 1-27, som netop er de bestemmelser, der pålægger medlemsstaterne forpligtelser, ikke er umiddelbart eksekverbare og dermed ikke danner baggrund for privat påtaleret ved de amerikanske domstole.[81] Traktatforpligtelser, der ikke er umiddelbart eksekverbare, skal efter den generelle opfattelse i amerikansk ret ikke erstatte eksisterende føderal lovgivning.[82] FISA og E.O 12333, der som bekendt er føderal lovgivning og hjemler overvågningsprogrammerne Prism og Upstream, har efter amerikansk ret således forrang for CPR-Konventionen. Dette kan forklare, at USA har undladt at underskrive og ratificere den valgfri protokol til CPR-Konventionen, hvorved staterne, der tiltræder denne protokol, anerkender individuel klageadgang til Menneskerettighedskomitéen.[83]

Uanset denne forklaring er USA's brud på CPR-Konventionen ikke i overensstemmelse med folkeretten. Traktatkonventionen, som kodificerer de folkeretlige regler om traktaters indgåelse, fortolkning og ophør med videre, fastslår i art. 26 traktatrettens grundprincip om, at enhver ikraftværende traktat er bindende for dens deltagere og skal opfyldes af dem i god tro.[84] Videre fremgår det af

[80] Germer, Peter, *Indledning til folkeretten*, 4. udgave, 4. oplag, 2010, s. 77.
[81] United Nations Treaty Collection, *4. International Covenant on Civil and Political Rights*, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en#EndDec (sidst besøgt: 6/5 2021); Quigley, John, *The International Covenant on Civil and Political Rights and the Supremacy Clause*, DePaul Law Rewiew, 42.4, 1993, s. 1297 f.
[82] CRS, Report RL32528, Mulligan, Stephen P., *International Law and Agreements: Their Effect upon U.S. Law*, 2018, s. 20 f.
[83] United Nations Human Rights, *Optional Protocol to the International Covenant on Civil and Political Rights,* https://indicators.ohchr.org (sidst besøgt: 17/5 2021); Storgaard, Louise Halleskov m.fl., *Folkeret og menneskerettigheder*, 1. udgave, 1. oplag, 2019, s. 196 ff.
[84] Storgaard, Louise Halleskov m.fl., *Folkeret og menneskerettigheder*, 1. udgave, 1. oplag, 2019, s. 68.

konventionens art. 27, at en medlemsstat ikke må påberåbe sig national ret til retfærdiggørelse af sin undladelse af at opfylde en traktat. Endelig har USA i forbindelse med ratifikationen af CPR-Konventionen ikke afgivet nogle forbehold, der relaterer sig til art. 17.[85]

Samspillet det EU-retlige, amerikanske og folkeretlige reguleringssystem imellem skal sammenholdes med EU-Domstolens præmis 105 i Schrems II. Ifølge denne præmis kan den dataansvarlige kun gennemføre en tredjelandsoverførsel på baggrund af Kommissionens standardkontraktbestemmelser efter GDPR art. 46, stk. 2, litra c, såfremt den registrerede, hvis personoplysninger overføres til et tredjeland, sikres et databeskyttelsesniveau, der i det væsentlige svarer til det niveau, der er sikret i EU efter GDPR, sammenholdt med Chartret. Med præmis 105 udvider EU-Domstolen målestokken "*i det væsentlige*" til ikke blot at gælde bestemmelsen om sikre tredjelande i GDPR art. 45 som fastslået af EU-Domstolens dom i Schrems I, men også GDPR art. 46. Dette med henvisning til, at beskyttelsesniveauet skal være det samme, uanset hvilket overførselsgrundlag i henhold til GDPR kap. V, den pågældende tredjelandsoverførsel måtte være baseret på.[86]

Når det konkrete krav i Schrems II-dommen præmis 105 sammenholdes med uoverensstemmelserne det amerikanske og EU-retlige reguleringssystem imellem, står det klart, at den dataansvarlige, der ønsker at gennemføre en tredjelandsoverførsel til USA på baggrund af Kommissionens standardkontraktbestemmelser, befinder sig midt i skudzonen i databeskyttelseskrigen. Den dataansvarlige kan ikke uden videre overføre personoplysninger til USA, men står over for en retlig barriere, der grundet sit udspring i grundrettigheder synes ganske alvorlig og vanskelig at overvinde.

6. De retlige rammer for den dataansvarliges brug af Kommissionens standardkontraktbestemmelser

Hvorvidt den dataansvarlige ved brug af Kommissionens standardkontraktbestemmelser kan overvinde den retlige barriere på grundrettighedsniveau, starter med en undersøgelse af, hvilke retlige

[85] United Nations Treaty Collection, *4. International Covenant on Civil and Political Rights*, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en#EndDec (sidst besøgt: 6/5 2021).
[86] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 92.

rammer for anvendelsen af disse bestemmelser EU-Domstolen med Schrems II-dommen efterlader den dataansvarlige.

6.1. De fornødne garantier

De retlige rammer skal undersøges i sammenhæng med ordlyden af de bestemmelser i GDPR, som relaterer sig til Kommissionens standardkontraktbestemmelser. Som EU-Domstolen fremhæver i Schrems II-dommens præmis 128, fastslår GDPR art. 46, stk. 1, følgende:

> *"Hvis der ikke er vedtaget en afgørelse i henhold til artikel 45, stk. 3, må en dataansvarlig eller en databehandler kun overføre personoplysninger til et tredjeland, hvis vedkommende har givet de fornødne garantier, og på betingelse af at rettigheder, som kan håndhæves, og effektive retsmidler for registrerede er tilgængelige".*

Som EU-Domstolen konstaterer i præmis 131, er det i ifølge GDPR art. 46, stk. 1, den dataansvarlige eller databehandleren etableret i EU, som er forpligtet til at give de nævnte "*fornødne garantier*", som i medfør af GDPR art. 46, stk. 2, litra c, kan sikres gennem Kommissionens standardkontraktbestemmelser.

Det nærmere indhold af "*fornødne garantier*" skal forstås i lyset af standardkontraktbestemmelsernes retlige status. I Schrems II-dommens præmis 125 og 132 understreger EU-Domstolen, at Kommissionens standardkontraktbestemmelser har kontraktlig karakter. Standardbestemmelserne binder derfor kun den dataansvarlige og dataimportøren i tredjelandet, som har vedtaget en kontrakt med henvisning til bestemmelserne. EU-Domstolen angiver udtrykkeligt i samme præmisser, at standardkontraktbestemmelserne netop af denne grund ikke binder myndighederne i tredjelandet. Når denne kendsgerning sammenholdes med den retlige barriere og den amerikanske sikkerhedslovgivning som behandlet ovenfor, synes standardkontraktbestemmelsernes karakter af inter partes-regulering derfor umiddelbart at fremstå problematisk for den dataansvarliges muligheder for at anvende bestemmelserne som grundlag for persondataoverførsler til USA.

Når EU-Domstolen i den konkrete dom alligevel ikke tilsidesætter Kommissionens 2010-bestemmelser som ugyldige, skyldes dette, at EU-Domstolen opdeler de fornødne garantier, den dataansvarlige skal sikre i henhold til GDPR art. 46, stk. 1, i to kategorier.

Selvom de fornødne garantier kan sikres gennem Kommissionens standardkontraktbestemmelser, påpeger EU-Domstolen i præmis 128, at art. 46 ikke angiver, at samtlige af de nævnte garantier nødvendigvis skal være fastsat i standardbestemmelserne. Denne fortolkning skal sammenholdes med præmis 133, hvor EU-Domstolen fastslår, at standardbestemmelserne vedtaget i henhold til GDPR art. 46, stk. 2, litra c, "*alene tager sigte på at give dataansvarlige eller databehandlere, som er etableret i unionen, kontraktlige garantier (…)*". Samtidig fastslår EU-Domstolen i samme præmis, at der ved siden af disse kontraktlige garantier, afhængigt af situationen i tredjelandet, kan være "*behov for, at den dataansvarlige vedtager supplerende foranstaltninger (…)*". Dette med henvisning til præambelbetragtning 108 i GDPR, som fastslår, at den dataansvarlige ved anvendelsen af Kommissionens standardkontraktbestemmelser må "*træffe foranstaltninger for at kompensere for den manglende databeskyttelse i et tredjeland (…)*", samt til betragtning 109, der fastslår, at anvendelsen af Kommissionens standardbestemmelser ikke udelukker muligheden for at give yderligere garantier, der "*supplerer*" de pågældende bestemmelser.[87]

De fornødne garantier efter GDPR art. 46 består således først og fremmest af den kontraktlige mekanisme. Denne mekanisme er imidlertid ikke i alle tilfælde tilstrækkelig. I generaladvokatens forslag til afgørelse understreges det da også, at Kommissionens standardkontraktbestemmelser alene kan karakteriseres som "*en generel mekanisme, der finder anvendelse på overførsler, uanset hvilket bestemmelsestredjeland der er tale om, og uanset hvilket beskyttelsesniveau der er sikret i dette tredjeland.*"[88] I Schrems II-dommens præmis 126 fremhæver EU-Domstolen, at der er situationer, hvor den kontraktlige mekanisme muligvis ikke er tilstrækkelig til at sikre den fornødne beskyttelse i praksis. Ifølge EU-Domstolen er dette navnlig tilfældet, når lovgivningen i tredjelandet tillader, at dets offentlige myndigheder gør indgreb i de registreredes rettigheder.

[87] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 131 og 132.
[88] Generaladvokat H. Saugmandsgaard Øe, *Forslag til afgørelse*, 19. december 2019, afsnit 120.

Med ovennævnte præmisser adresserer EU-Domstolen en problemstilling, der gør sig gældende generelt for samtlige overførselsgrundlag: Når personoplysninger placeres uden for EU, bliver de pågældende oplysninger omfattet af tredjelandets lovgivning. Såfremt den dataansvarlige anvender Kommissionens standardkontraktbestemmelser som overførselsgrundlag, kan tredjelandets lovgivning medføre, at de pågældende standardbestemmelser tilsidesættes og dermed ikke yder en tilstrækkelig sikkerhed mod, at oplysningerne bruges til uvedkommende formål.[89] Det skal understreges, at EU-Domstolen ikke konkret nævner USA i denne sammenhæng. I lyset af den amerikanske sikkerhedslovgivning står det dog klart, at EU-Domstolen ganske tydeligt, omend ikke direkte, understreger, at supplerende foranstaltninger er særdeles relevante at tage i betragtning i forbindelse med tredjelandsoverførsler til USA. Trods de supplerende foranstaltningers afgørende betydning nævner EU-Domstolen imidlertid ikke, hvad disse foranstaltninger konkret kan bestå i, og hvornår de supplerende foranstaltninger ifølge EU-Domstolen er tilstrækkelige. I præmis 135 nøjes EU-Domstolen med at fastslå, at den dataansvarlige eller dennes databehandler, subsidiært den kompetente tilsynsmyndighed, skal suspendere eller indstille overførslen af personoplysninger til et tredjeland, hvis de supplerende foranstaltninger ikke er tilstrækkelige til at garantere den fornødne databeskyttelse. Spørgsmålet om, hvornår de supplerende foranstaltninger efter EU-Domstolens opfattelse udgør de fornødne garantier, efterlader EU-Domstolen hos den dataansvarlige.

6.2. Undersøgelsespligten

Mens EU-Domstolen undlader at uddybe det nærmere indhold af de "*supplerende foranstaltninger*", der skal implementeres afhængigt af forholdene i tredjelandet, fokuserer EU-Domstolen på at fastlægge omfanget af de generelle forpligtelser, der altid vil gælde, når den dataansvarlige anvender Kommissionens standardkontraktbestemmelser efter GDPR art. 46, stk. 2, litra c, som overførselsgrundlag. I præmis 134 fastlår EU-Domstolen, hvilke pligter, der påhviler den dataansvarlige i forbindelse med sin vurdering af, i hvilket omfang der er behov for at implementere supplerende foranstaltninger:

[89] Blume, Peter, *Databeskyttelsesret*, 5. udgave, 1. oplag, 2018, s. 274 og 281.

> *"Det tilkommer derfor først og fremmest den dataansvarlige eller dennes databehandler i hvert enkelt tilfælde og, hvor det er relevant, i samarbejde med modtageren af overførslen at undersøge, om lovgivningen i bestemmelsestredjelandet sikrer den fornødne beskyttelse henset til EU-retten (…)."*

Med præmis 134 fortolker EU-Domstolen GDPR art. 46 således, at den dataansvarlige, der ønsker at gennemføre en tredjelandsoverførsel på baggrund af Kommissionens standardkontraktbestemmelser, pålægges en selvstændig pligt til at undersøge, om lovgivningen i tredjelandet sikrer den fornødne beskyttelse. For den enkelte dataansvarlige kan dette opleves som en særdeles byrdefuld forpligtelse, og før Schrems II-dommen herskede der stor usikkerhed om, hvorvidt en sådan undersøgelsespligt kan indeholdes i art. 46, der ikke udtrykkeligt pålægger den dataansvarlige denne forpligtelse.[90] Kun GDPR art. 45 pålægger udtrykkeligt en forpligtelse for Kommissionen til at undersøge tredjelandets lovgivning i forbindelse med en afgørelse af, om et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau. Med sin fortolkning af GDPR art. 46 overfører EU-Domstolen imidlertid Kommissionens forpligtelser efter art. 45 til den dataansvarlige. Dette kan dog anskues som en naturlig konsekvens af EU-Domstolens førnævnte krav om, at beskyttelsesniveauet skal være det samme, uanset hvilket overførselsgrundlag i GDPR kap. V den dataansvarlige måtte vælge.

For så vidt angår det nærmere indhold af den undersøgelsespligt, som den dataansvarlige pålægges, kan der henvises til Schrems II-dommens præmis 104. Her fastslås det, at den dataansvarlige i forbindelse med en tredjelandsoverførsel baseret på Kommissionens standardkontraktbestemmelser navnlig skal tage hensyn til de *"relevante forhold*" i tredjelandets retssystem. Ved fastlæggelsen af, hvad der kan udgøre sådanne relevante forhold, henviser EU-Domstolen til de elementer, der "*på ikke udtømmende vis*" er opregnet i GDPR art. 45, stk. 2, der omhandler de forhold, som Kommissionen skal tage i betragtning i forbindelse med en afgørelse om et sikkert tredjeland. Dette skal sammenholdes med EU-Domstolens præmis 134, hvorefter den dataansvarlige skal iagttage undersøgelsespligten "*i hvert enkelt tilfælde*". Hvad der menes med dette understøttes af afsnit 126 i

[90] Udsen, Henrik, *IT-ret*, 4. udgave, 1. oplag, 2019, s. 446.

generaladvokatens forslag til afgørelse, som EU-Domstolen henviser til i samme præmis. Her udpensles det, at undersøgelsen skal ske "*i hvert enkelt tilfælde, for hver enkelt konkrete overførsel (…)*".[91]

Samlet fremgår det af ovennævnte præmisser, at den dataansvarliges undersøgelser af tredjelandets lovgivning ifølge EU-Domstolen er en væsentlig forpligtelse, som skal bidrage til at fastsætte de rette supplerende foranstaltninger og dermed sikre det fornødne beskyttelsesniveau henset til EU-retten. EU-Domstolen foretager imidlertid ikke nogen nærmere afgrænsning af, hvilke forhold den dataansvarlige kan inddrage i sine undersøgelser. Det står dog klart, at den dataansvarlige må gennemføre sine undersøgelser med udgangspunkt i den konkrete tredjelandsoverførsel.

6.3. Den generelle gyldighed af Kommissionens standardkontraktbestemmelser

Efter at have fastslået de ovennævnte generelle krav til den dataansvarliges anvendelse af Kommissionens standardkontraktbestemmelser, sammenholder EU-Domstolen i præmis 138-148 disse krav med de konkrete standardkontraktbestemmelser, der var under pådømmelse, nemlig 2010-bestemmelserne. EU-Domstolen fandt, at bestemmelserne var i overensstemmelse med disse krav og dermed omfattede "*effektive mekanismer*", der kunne sikre, at kontraktsparterne kunne overholde de generelle krav. Derfor var 2010-bestemmelserne gyldige i lyset af Chartrets art. 7, 8, og 47.[92]

Gyldigheden af selve Kommissionens standardkontraktbestemmelser afhænger således af, om de muliggør overholdelse af forpligtelserne som nævnt ovenfor. Dette uanset, hvilket sæt standardbestemmelser, der måtte komme under pådømmelse. På trods af, at EU-Domstolen tager konkret stilling til 2010-bestemmelserne, har Schrems II således også retskildeværdi i relation til de øvrige sæt standardbestemmelser, herunder de kommende 2020-bestemmelser.

Såfremt standardbestemmelserne er generelt gyldige, afhænger lovligheden af den konkrete tredjelandsoverførsel imidlertid af, om den dataansvarlige i praksis formår at sikre et beskyttelsesniveau

[91] Generaladvokat H. Saugmandsgaard Øe, *Forslag til afgørelse*, 19. december 2019, afsnit 126.
[92] EU-Domstolen, Sag C-311/18, *Facebook Ireland og Schrems,* præmis 148 og 149.

for den registrerede, der i det væsentlige svarer til beskyttelsesniveauet efter EU-retten. Dette ved at overholde de kontraktuelle forpligtelser, der følger af Kommissionens standardkontraktkontraktbestemmelser, men efter omstændighederne også ved at fastsætte supplerende foranstaltninger på baggrund af nøje undersøgelser af de relevante forhold i tredjelandets retssystem.

7. De praktiske muligheder for anvendelsen af Kommissionens standardkontraktbestemmelser

På det overordnede plan bygger persondataretten på privatlivshensyn, nærmere bestemt en forudsætning om, at individet har et behov for og et krav på at kunne bevare oplysninger om sig selv inden for en privatsfære. Enhver lovregel er imidlertid baseret på modsatrettede hensyn og en afvejning heraf, og her er de persondataretlige regler ingen undtagelse. Det er en afgørende forudsætning for, at vores samfund kan fungere, at dataansvarlige, herunder virksomheder, har mulighed for at behandle personoplysninger i forskellige sammenhænge. Der er derfor en række praktiske hensyn, der efter omstændighederne strider mod de hensyn, der tilsiger beskyttelse af personoplysninger. Som et eksempel på et sådant praktisk hensyn kan nævnes muligheden for at drive virksomhed og i denne forbindelse overføre personoplysninger til en handelspartner i USA.[93]

Grundet EU-Domstolens tilsidesættelse af Privacy Shield-ordningen kan GDPR art. 45 ikke længere anvendes som overførselsgrundlag ved tredjelandsoverførsler til USA. Videre kan overførselsgrundlagene i GDPR art. 49 kun kan anses som undtagelsessituationer. Derfor tilsiger pragmatiske hensyn, at tredjelandsoverførsler til USA på baggrund af GDPR art. 46 bør kunne lade sig gøre. På denne baggrund skal det afsøges, hvordan den dataansvarlige inden for rammerne af EU-Domstolens ovennævnte krav lovligt kan anvende Kommissionens standardkontraktbestemmelser ved tredjelandsoverførsler til en amerikansk dataimportør og dermed overvinde den retlige barriere på grundrettighedsniveau.

[93] Udsen, Henrik, *IT-ret*, 4. udgave, 1. oplag, 2019, s. 321 ff.

7.1. Supplerende foranstaltninger, der udelukker risikoen for amerikansk overvågning

Når det i lyset af Schrems II-dommen skal fastlægges, hvilke konkrete supplerende foranstaltninger, der skal træffes ved tredjelandsoverførsler til en amerikansk dataimportør, er Det Europæiske Databeskyttelsesråd, EDPB, en central aktør at tage i betragtning. EDPB er et uafhængigt organ oprettet i medfør af GDPR art. 68, stk. 1. Ifølge GDPR art. 68, stk. 3, består EDPB af Den Europæiske Tilsynsførende for Databeskyttelse, EDPS, og chefen for de nationale tilsynsmyndigheder, herunder det danske Datatilsyn.

Efter GDPR art. 70, stk. 1, har EDPB til opgave at sikre ensartet anvendelse af reglerne i GDPR, og med henblik herpå kan EDPB efter art. 70, stk. 1, litra e, bl.a. udstede henstillinger. I kølvandet på Schrems II-dommen har EDPB vedtaget Henstilling 01/2020, der har til formål at yde den dataansvarlige vejledning i at afgøre, om der i forbindelse med tredjelandsoverførsler til et tredjeland er behov for supplerende foranstaltninger, og i givet fald hvilke, der skal indføres.[94] Om EU-retlige henstillinger skal det fastslås, at disse ikke er bindende for den dataansvarlige, jf. TEUF art. 288, 5. pkt. Henstilling 01/2020 er således udelukkende EDPB's bud på, hvordan EU-Domstolens præmisser i Schrems II skal fortolkes. Derudover skal det understreges, at Henstilling 01/2020 i skrivende stund udelukkende foreligger i høringsversionen, hvorfor EDPB endnu ikke har vedtaget den endelige version. Høringsversionen kan dog anskues som udgangspunktet for EDPB's opfattelse.

I medfør af Henstilling 01/2020 kan de supplerende foranstaltninger, som den dataansvarlige måtte vælge at implementere, være af både kontraktlig, teknisk eller organisatorisk art. I henstillingen angiver EDPB imidlertid udtrykkeligt, at kontraktlige og organisatoriske foranstaltninger alene generelt ikke vil overkomme offentlige myndigheders adgang til personoplysninger som led i overvågning. Kun tekniske foranstaltninger vil kunne forhindre denne adgang.[95] Med henvisning til den amerikanske sikkerhedslovgivning står det herefter klart, at det efter EDPB's opfattelse først og fremmest er de tekniske foranstaltninger, der er afgørende ved tredjelandsoverførsler til USA.

[94] BILAG A, s. 9, afsnit 6 og 7.
[95] BILAG A, s. 17, afsnit 47 og 48.

Bilag 2 i Henstilling 01/2020 indeholder et længere katalog af ikke-udtømmende forslag til supplerende foranstaltninger, herunder tekniske foranstaltninger, der kan sikre de overførte personoplysninger et beskyttelsesniveau, der i det væsentlige svarer til det niveau, der er sikret efter EU-retten. Samtidig angiver EDPB eksempler på situationer, hvor EDPB ikke på nuværende tidspunkt er i stand til at forestille sig, at der findes effektive tekniske foranstaltninger.[96]

EDPB fremhæver, at en dataansvarlig under visse betingelser kan anvende en udbyder i et tredjeland til at lagre personoplysninger, f.eks. til sikkerhedskopiering. De nærmere betingelser indebærer først og fremmest, at de overførte personoplysninger underlægges kryptering inden overførslen til tredjelandet.[97] Samtidig fastslår EDPB, at der ved overførsel til dataimportører, som kræver adgang til ikke-krypterede data, ikke kan identificeres nogle effektive tekniske foranstaltninger, såfremt de offentlige myndigheder i tredjelandet har en disproportional adgang til de pågældende data.[98] Ligeledes vil der ifølge EDPB ej heller kunne fastsættes effektive tekniske foranstaltninger, såfremt en dataimportør har fjernadgang til ikke-krypterede data til forretningsmæssige formål.[99] Dermed adresserer EDPB det brede overførselsbegreb, der som bekendt indebærer, at også en dataimportørs "se-adgang" vil indebære en tredjelandsoverførsel.

Det står herefter klart, at den amerikanske dataimportør efter EDPB's opfattelse ikke må have adgang til de personoplysninger, der overføres, og at kryptering i denne forbindelse kan være et afgørende redskab, når den dataansvarlige skal nå dette mål. Kryptering nævnes udtrykkeligt i GDPR art. 6, 32 og 34 samt præambelbetragtning 83 som ét ud af flere mulige redskaber til at sikre overholdelse af de nærmere forpligtelser efter GDPR. Selvom kryptering er en anerkendt sikkerhedsforanstaltning efter GDPR, indeholder legaldefinitionerne i GDPR art. 4 imidlertid ikke en nærmere definition af krypteringsbegrebet, ligesom GDPR ikke fastsætter krav til den pågældende kryptering. Den dataansvarlige er derfor henvist til Henstilling 01/2020, som fastlægger de nærmere betingelser for, at krypteringen efter EDPB's opfattelse kan anses for at udgøre en effektiv supplerende foranstaltning. EDPB fastslår, at krypteringen skal være "*stærk*" og leve op til det "*aktuelle tekniske*

[96] BILAG A, s. 23-29, afsnit 72-91.
[97] BILAG A, s. 24 f., afsnit 79.
[98] BILAG A, s. 28 f., afsnit 88 og 89.
[99] BILAG A, s. 29, afsnit 90 og 91.

niveau", ligesom krypteringen skal anses for at være "*robust*" mod den kryptoanalyse, som udføres af offentlige myndigheder i modtagerlandet. Krypteringen skal ifølge EDPB ligeledes være implementeret "*fejlfrit*" af "*korrekt vedligeholdt software",* ligesom krypteringsnøglen skal forvaltes "*pålideligt*" og opbevares inden for EU eller et sikkert tredjeland, jf. GDPR art. 45.[100]

Det kan konstateres, at EDPB fastsætter høje standarder for, hvornår den anvendte kryptering er tilstrækkelig. Dette må anses som en naturlig konsekvens af, at krypteringen for helt at eliminere risikoen for, at offentlige myndigheder opnår adgang til de overførte personoplysninger, nødvendigvis skal være på et sådant niveau, at selv efterretningstjenester som NSA ikke kan omgå den. At krypteringsnøglen ifølge EDPB's krypteringsstandard skal opbevares inden for EU eller et sikkert tredjeland, skal i øvrigt ses i lyset af, at de amerikanske dataimportører efter FISA Section 702 også kan være forpligtede til at udlevere kryptografiske nøgler til de amerikanske efterretningstjenester.[101]

Selvom det er de tekniske supplerende foranstaltninger, der ifølge EDPB er afgørende ved tredjelandsoverførsler til USA, påpeger EDPB i Henstilling 01/2020, at kontraktmæssige foranstaltninger kan supplere de tekniske foranstaltninger og styrke personoplysningernes samlede beskyttelsesniveau.[102] I denne forbindelse fastslår EDPB, at det efter omstændighederne er nødvendigt, at den dataansvarlige og dataimportøren aftaler, at specifikke tekniske foranstaltninger skal etableres, før overførsler kan finde sted.[103] Ingen af Kommissionens standardkontraktbestemmelser indeholder en udtrykkeligt pligt for den dataansvarlige til om nødvendigt at iværksætte tekniske foranstaltninger, eksempelvis kryptering, inden tredjelandsoverførslen til dataimportøren gennemføres. Bestemmelserne synes derimod at forudsætte, at det er dataimportøren, der skal iværksætte sådanne foranstaltninger, og dermed at foranstaltningerne først skal implementeres efter overførslen. Eksempelvis fastslår 2010-bestemmelsernes standardbestemmelse 5(c), at dataimportøren bl.a. skal iværksætte de tekniske sikkerhedsforanstaltninger, der nærmere aftales i

[100] BILAG A, s. 24 f., afsnit 79.
[101] 50 U.S.C. § 1881a(a),(i)(1) (2018); BILAG A, s. 24, afsnit 76.
[102] BILAG A, s. 17, afsnit 47; BILAG A, s. 30, afsnit 93.
[103] BILAG A, s. 30 f., afsnit 97 og 98.

standardbestemmelsernes tillæg 2. Videre fremgår det af standardbestemmelse 4(c), at den dataansvarlige accepterer og garanterer, at dataimportøren iværksætter disse foranstaltninger.

Den dataansvarlige og dataimportøren kan ikke foretage ændringer i Kommissionens standardkontraktbestemmelser, uden at der skal indhentes tilladelse fra Datatilsynet efter GDPR art. 46, stk. 3, litra a, om ad-hoc-kontrakter. Som både 2004- og 2010-bestemmelserne udtrykkeligt fastslår, udelukker dette dog ikke, at parterne om nødvendigt indføjer supplerende bestemmelser.[104] På denne baggrund kan den dataansvarlige og den amerikanske dataimportør med fordel udarbejde et tillæg til de indgåede standardkontraktbestemmelser, hvorefter enhver tredjelandsoverførsel til dataimportøren afskæres, før de pågældende oplysninger er underlagt den ifølge EDPB nødvendige kryptering og krypteringsnøglen er overdraget til en pålidelig tredjepart etableret inden for EU eller et sikkert tredjeland.

7.2. Supplerende foranstaltninger, der ikke udelukker risikoen for amerikansk overvågning

Kryptering er en teknologi, som ikke alle dataansvarlige har den nødvendige teknologiske indsigt til at anvende, særligt ikke når EDPB's høje krypteringsstandarder tages i betragtning. EDPB's løsning er derfor rettet mod de ressourcestærke dataansvarlige, der enten selv har mulighed for at fastlægge og anvende den fornødne krypteringssoftware eller til at søge professionel hjælp. Da der ligeledes er væsentlige modgående hensyn til en stærk kryptering, herunder at den amerikanske dataimportør har adgang til og kan anvende de overførte personoplysninger, afføder høringsversionen af Henstilling 01/2020 ligeledes praktiske barrierer.[105]

Selvom supplerende foranstaltninger i medfør af Schrems II-dommen umiddelbart var den dataansvarliges mulighed for at overkomme den retlige barriere på grundrettighedsniveau EU og USA imellem, synes Henstilling 01/2020 således at skabe nye ressourcemæssige og praktiske barrierer, som den dataansvarlige må overkomme i forbindelse med tredjelandsoverførsler til USA. Derfor er det

[104] 2001-bestemmelserne, standardbestemmelse 11; 2004-bestemmelserne, standardbestemmelse VII; 2010-bestemmelserne, standardbestemmelse 10; Nielsen, Kristian Korfits og Lotterup, Anders, *Databeskyttelsesforordningen og databeskyttelsesloven*, 2020, 1. udgave, s. 793.
[105] Blume, Peter, *Databeskyttelsesret*, 5. udgave, 1. oplag, 2018, s. 288.

af væsentlig interesse, om den dataansvarlige uden at gå på kompromis med persondatarettens regler i visse tilfælde kan træffe supplerende foranstaltninger, der ikke helt udelukker de amerikanske efterretningstjenesters adgang til de overførte personoplysninger.

7.2.1. Princippet om ansvarlighed og den risikobaserede tilgang

Efter GDPR art. 44, skal en tredjelandsoverførsel både have hjemmel i ét af de konkrete overførselsgrundlag som fastsat i GDPR, kap. V, men samtidig overholde de øvrige bestemmelser i GDPR. I denne forbindelse er særligt GDPR art. 5, stk. 2, af interesse. Bestemmelsen udtrykker det såkaldte ansvarlighedsprincip og indebærer dels, at den dataansvarlige er ansvarlig for overholdelsen af reglerne i GDPR, dels at den dataansvarlige skal kunne dokumentere, at dette er tilfældet. Spørgsmålet er derfor, hvornår den dataansvarlige i sine bestræbelser på at overholde EU-Domstolens krav i Schrems II kan siges at have udvist den fornødne grad af ansvarlighed i forbindelse med sin tredjelandsoverførsel til USA.

EU-Domstolen giver selv en del af svaret. Med Schrems II fastslås det som bekendt, at den dataansvarlige i forbindelse med anvendelsen af Kommissionens standardkontraktbestemmelser med udgangspunkt i den konkrete tredjelandsoverførsel skal iagttage sin undersøgelsespligt med henblik på at fastsætte, hvilke supplerende foranstaltninger, der eventuelt skal implementeres. Ved sin opfyldelse af ansvarlighedsprincippet i GDPR art. 5, stk. 2, er det således ikke udelukkende de konkrete supplerende foranstaltninger, der bliver afgørende, men også den forudgående vurdering, der ligger til grund for de pågældende foranstaltninger. I Henstilling 01/2020 er EDPB af samme opfattelse, og henviser i denne forbindelse til den kendsgerning, at persondataretten går videre end en erkendelse af eller passiv overholdelse af reglerne. Persondataretten har *"aktiv karakter"*.[106] I overensstemmelse med ansvarlighedsprincippet må den dataansvarlige således tage aktivt stilling til den konkrete tredjelandsoverførsel.

Som det fremgår af Schrems II-dommen, er det ikke umiddelbart givet, hvilke forhold i tredjelandet den dataansvarlige kan inddrage i forbindelse med sin iagttagelse af undersøgelsespligten og

[106] BILAG A, s. 8, afsnit 3; BILAG A, s. 9, afsnit 7 og fodnote 21.

dermed ansvarlighedsprincippet. Det amerikanske handelsministerium, justitsministerium samt direktøren for de amerikanske efterretningstjenester synes dog at gøre et forsøg på at imødekomme denne uklarhed. I et "*white paper*" udgivet i kølvandet på Schrems II-dommen påpeger de pågældende myndigheder, at det for mange amerikanske virksomheder er "*usandsynligt*", at de bliver genstand for den overvågning, som EU-Domstolen adresserer i Schrems II. Dette med henvisning til at de oplysninger, virksomhederne håndterer, ikke er af interesse for de amerikanske efterretningstjenester. Ligeledes fremhæves det, at det "*overvældende flertal*" af virksomhederne aldrig er blevet beordret til at udlevere data til amerikanske efterretningstjenester i henhold til FISA Section 702, ligesom der ikke er nogle indikationer på, at efterretningstjenesterne vil søge at opnå adgang til disse virksomheders data uden for USA i medfør af E.O. 12333.[107]

Det amerikanske white paper afføder det spørgsmål, om den dataansvarlige i sine bestræbelser på at dokumentere ansvarligheden i sin beslutning om at gennemføre en tredjelandsoverførsel til USA kan lægge vægt på subjektive vurderinger af den reelle risiko for, at den konkrete amerikanske dataimportør bliver genstand for de amerikanske efterretningstjenesters overvågning af de overførte personoplysninger. Dette eventuelt ved at inddrage oplysninger om dataimportørens erfaringer med efterretningstjenesternes anmodninger om indsigt i de personoplysninger, som dataimportøren måtte behandle. Såfremt risikoen i det konkrete tilfælde vurderes at være begrænset, vil den dataansvarlige eventuelt kunne legitimere supplerende foranstaltninger, der ikke helt udelukker risikoen for, at de amerikanske efterretningstjenester opnår adgang til de overførte oplysninger.

Det er af væsentlig praktisk interesse for den dataansvarlige, om en sådan risikobaseret tilgang kan rummes i Schrems II-dommens præmisser. Med EU-Domstolens præmis 135 fastslås det som bekendt, at den dataansvarlige efter omstændighederne skal træffe supplerende foranstaltninger, der er tilstrækkelige til at garantere den fornødne beskyttelse henset til EU-retten. Dette kan pege i retning af, at den dataansvarlige i forbindelse med sin implementering af supplerende foranstaltninger ikke må tillægge den konkrete risiko for disproportional amerikansk overvågning vægt. Den dataansvarlige kan næppe garantere den fornødne beskyttelse, hvis der foreligger en risiko for

[107] Department of Commerce m.fl., *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, 2020, s. 2 f.; Gjerstad, Marianne og Vanebo, Ole A., *Schrems II: Faktisk risiko bør spille en rolle ved overføring av personopplysninger til tredjestater*, Lov & Data, 145.1, 2021, s. 13.

overvågning i strid med EU-retten, uanset om denne risiko i det konkrete tilfælde er beskeden. Selvom EU-Domstolen udtrykkeligt adresserer problemstillingen med offentlige myndigheders adgang til personoplysninger, nævner EU-Domstolen imidlertid på intet tidspunkt, at disse myndigheder i visse tilfælde skal udelukkes enhver adgang til de overførte personoplysninger. Som nævnt undlader EU-Domstolen derimod at gå nærmere ind i spørgsmålet om, hvornår de konkrete supplerende foranstaltninger efter EU-Domstolens opfattelse kan siges at udgøre de fornødne garantier. Dette skal sammenholdes med den kendsgerning, at EU-Domstolen hverken foretager en klar positiv eller negativ afgrænsning af de forhold, som den dataansvarlige kan tillægge vægt i forbindelse med sine undersøgelser af databeskyttelsesniveauet i tredjelandet. Når EU-Domstolen samtidig understreger, at den dataansvarlige skal iagttage sin undersøgelsespligt med udgangspunkt i den konkrete tredjelandsoverførsel, kan dette desuden efterlade det indtryk, at den dataansvarlige også bør kunne tillægge betragtninger om den konkrete risiko for overvågning vægt.

Tages der alene udgangspunkt i Schrems II-dommens præmisser, må det således anses for uklart, om den dataansvarlige i forbindelse med implementeringen af supplerende foranstaltninger efter EU-Domstolens opfattelse kan lægge en risikobaseret tilgang til grund. Ved fastlæggelsen af gældende ret på området må der herefter henvises til en række af de bestemmelser i GDPR, der har til formål at skabe den ansvarlighed, der efter GDPR art. 5, stk. 2, kræves af den dataansvarlige. I generalklausulen i GDPR art. 24, stk. 1, der gælder på tværs af samtlige bestemmelser i GDPR, uddybes den dataansvarliges forpligtelser efter ansvarlighedsprincippet. Bestemmelsen pålægger den dataansvarlige en forpligtelse til at etablere passende foranstaltninger under hensyntagen til bl.a. "*risiciene af varierende betydning*". En tilsvarende formulering findes i GDPR art. 25, stk. 1, omhandlende princippet om databeskyttelse gennem design og standardindstillinger, samt i GDPR art. 32, stk. 1, om behandlingssikkerhed. Endelig fremgår det af GDPR art. 35, stk. 1, at den dataansvarlige forud for en behandlingsaktivitet skal vurdere risikoen ved denne, såfremt behandlingen vurderes at udgøre en "*høj risiko*" for den registrerede. Efter GDPR art. 35, stk. 7, skal den dataansvarlige i denne vurdering bl.a. inddrage betragtninger om risiciene for de registrerede samt de foranstaltninger, der påtænkes for at imødegå disse risici.[108]

[108] Udsen, Henrik, *IT-ret*, 4. udgave, 1. oplag, 2019, s. 415 ff.; Gjerstad, Marianne og Vanebo, Ole A., *Schrems II: Faktisk risiko bør spille en rolle ved overføring av personopplysninger til tredjestater*, Lov & Data, 145.1, 2021, s. 12 f.

Det påkalder det sig særlig praktisk interesse, at den dataansvarlige i forbindelse med opfyldelsen af ansvarlighedsforpligtelsen efter GDPR kan inddrage sine egne subjektive vurderinger af de risici, som den konkrete behandlingsaktivitet måtte afføde. Generelt set er denne risikobaserede tilgang en væsentlig del af GDPR, når den dataansvarlige skal iagttage forordningens krav. Ordene "*risiko*", "*risici*" eller "*risiciene*" indgår da også hele 76 gange i forordningen.[109] I denne forbindelse skal det dog samtidig understreges, at hverken GDPR art. 44 og 46 eller de tilhørende præambelbetragtninger 101, 102, 108 og 109 indeholder formuleringer om vurderinger af risici. Heller ikke GDPR giver således et klart svar på, om den dataansvarlige må inddrage betragtninger om risiko i forbindelse med tredjelandsoverførsler til usikre tredjelande som USA.

Efter 2010-bestemmelsernes standardbestemmelse 4(d) fremgår det dog, at den dataansvarlige i forbindelse med en tredjelandsoverførsel accepterer og garanterer, at de sikkerhedsforanstaltninger, der implementeres, giver et *"passende databeskyttelsesniveau i forhold til de risici, der er forbundet med behandlingen og arten af de oplysninger, der skal beskyttes, under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse"*. Tilsvarende fremgår det af Kommissionens udkast til 2020-bestemmelserne, at den dataansvarlige og dataimportøren ved vurderingen af de relevante sikkerhedsforanstaltninger skal tage behørigt hensyn til de risici, der er forbundet med behandlingen.[110]

Samtlige af Kommissionens standardkontraktbestemmelser adresserer udtrykkeligt spørgsmålet om tredjelandets lovgivning og dens indvirkning på overholdelsen af standardbestemmelserne. I 2001- og 2010-bestemmelserne forpligter dataimportøren sig til at garantere, at denne ikke har grund til at tro, at lovgivningen i tredjelandet forhindrer dataimportøren i at opfylde sine forpligtelser i henhold til de øvrige klausuler i standardbestemmelserne.[111] Tilsvarende fremgår det af 2004-bestemmelserne, at dataimportøren ved kontraktens indgåelse garanterer, at denne ikke har

[109] Gonçalves, Maria Eduarda, *The risk-based approach under the new EU data protection regulation: a critical perspective*, Journal of Risk Research, 23.2, 2020, s. 142 f. og s. 149 (fodnote 7); Gjerstad, Marianne og Vanebo, Ole A., *Schrems II: Faktisk risiko bør spille en rolle ved overføring av personopplysninger til tredjestater*, Lov & Data, 145.1, 2021, s. 12.
[110] BILAG B, s. 14, clause 1.5(a); BILAG B, s. 17, clause 1.6(a).
[111] 2001-bestemmelserne, standardbestemmelse 5(a); 2010-bestemmelserne, standardbestemmelse 5(b).

kendskab til eventuel lovgivning, der kan have betydelig negativ indvirkning på den beskyttelse, der ellers fremgår af standardbestemmelserne. [112] Om dataimportøren i forbindelse med afgivelsen af denne garanti må lægge vægt på den konkrete risiko for, at tredjelandets lovgivning vil medføre en tilsidesættelse af forpligtelserne i standardbestemmelserne, er, som det fremgår af gennemgangen af Schrems II-dommen, ikke klart. Med sit udkast til 2020-bestemmelserne synes Kommissionen dog at gøre et forsøg på at imødekomme denne usikkerhed. I disse bestemmelser lægger Kommissionen op til, at både den dataansvarlige og dataimportøren i forbindelse med afgivelsen af den pågældende garanti bl.a. skal tage hensyn til enhver "*praktisk erfaring*" med tidligere forekomster eller fraværet af påbud om videregivelse af data fra offentlige myndigheder modtaget af dataimportøren for den type data, der overføres. Efter Kommissionens umiddelbare opfattelse synes parterne således at kunne inddrage egne subjektive vurderinger af risikoen for, at de overførte oplysninger vil blive genstand for tredjelandets overvågning.[113]

På linje med den generelle risikobaserede tilgang i GDPR synes Kommissionens standardkontraktbestemmelser herefter samlet set at pege i retning af, at den dataansvarlige også i forbindelse med tredjelandsoverførsler til usikre tredjelande gennemført på baggrund af dette overførselsgrundlag bør gennemføre en konkret vurdering af risikoen for, at de overførte oplysninger rent faktisk vil blive genstand for amerikansk overvågning.

7.2.2. De grundlæggende rettigheder som fortolkningsmoment

Uanset de risikobaserede bestemmelser i såvel GDPR som Kommissionens standardkontraktbestemmelser, afviser EDPB i høringsversionen af Henstilling 01/2020 udtrykkeligt, at den dataansvarlige ved vurderingen af tredjelandets lovgivning kan henholde sig til subjektive faktorer, såsom risikoen for, at offentlige myndigheder tilgår personoplysningerne i strid med EU's standarder.[114] Denne opfattelse afspejler sig i EDPB's høje krypteringsstandarder, der uden hensyntagen til konkrete vurderinger har til formål helt at udelukke myndighedernes disproportionale adgang til de overførte personoplysninger. Ligeledes kommer EDPB's opfattelse til udtryk i EDPB's og EDPS'

[112] 2004-bestemmelserne, standardbestemmelse II(c).
[113] BILAG B, s. 23, clause 2(b)(i); Gjerstad, Marianne og Vanebo, Ole A., *Schrems II: Faktisk risiko bør spille en rolle ved overføring av personopplysninger til tredjestater*, Lov & Data, 145.1, 2021, s. 12.
[114] BILAG A, s. 15, afsnit 42.

bemærkninger til Kommissionens udkast til 2020-bestemmelserne. Her foreslår EDPB og EDPS, at Kommissionen helt fjerner bestemmelsen om, at kontraktsparterne ved sin vurdering af tredjelandets beskyttelsesniveau kan lægge vægt på praktiske erfaringer med indsigtsanmodninger fra tredjelandets myndigheder. Dette med henvisning til, at EU-Domstolen i Schrems II-dommen ikke udtrykkeligt henviser til subjektive faktorer som et moment, som den dataansvarlige kan tillægge vægt i forbindelse med sine undersøgelser af tredjelandets lovgivning.[115] I denne forbindelse skal det dog atter fremhæves, at EU-Domstolen ikke foretager en klar afgrænsning af de forhold, som den dataansvarlige kan tillægge vægt. Spørgsmålet om, hvorvidt der gælder en sådan afgrænsning, efterlader EU-Domstolen åbent.

Selvom der kan stilles spørgsmålstegn ved EDPB's opfattelse og dens konkrete hjemmel, er EDPB's bekymringer relaterende til den risikobaserede tilgang ikke nye. Allerede i 2014 blev den risikobaserede tilgang adresseret af EDPB's forgænger under databeskyttelsesdirektivet, den såkaldte Artikel 29-Gruppe. I forbindelse med udarbejdelsen af GDPR fandt Artikel 29-Gruppen det nødvendigt at understrege, at den risikobaserede tilgang ikke er et alternativ til den velfunderede ret til databeskyttelse, men at den registreredes rettigheder skal være beskyttede på det samme niveau, uanset om en given behandling er af relativ beskeden risiko. I denne forbindelse henviser Artikel 29-Gruppen til den kendsgerning, at beskyttelsen af personoplysninger er en grundlæggende rettighed i henhold til Chartrets art. 8, og at enhver behandling skal respektere denne rettighed.[116]

Netop de grundlæggende rettigheder kan være et vigtigt moment ved vurderingen af, om den dataansvarlige kan lægge en risikobaseret tilgang til grund i forbindelse med tredjelandsoverførsler til USA.

Spørgsmålet om den risikobaserede tilgang indebærer en afvejning af, om det er praktiske hensyn eller privatlivshensynet, der skal veje tungest ved tredjelandsoverførsler til USA. Praktiske hensyn

[115] EDPB og EDPS, *Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46(2)(c) of Regulation (EU) 2016/679*, afsnit 87; Gjerstad, Marianne og Vanebo, Ole A., *Schrems II: Faktisk risiko bør spille en rolle ved overføring av personopplysninger til tredjestater*, Lov & Data, 145.1, 2021, s. 12.
[116] Artikel 29-Gruppen, *Statement on the role of a risk-based approach in data protection legal frameworks (WP 218)*, 30. maj 2014, s. 2 f.

tilsiger, at den dataansvarlige som led i eksempelvis forretningsmæssige dispositioner bør indrømmes muligheder for at overføre personoplysninger til en amerikansk dataimportør, der ikke vurderes at blive genstand for indsigtsanmodninger fra efterretningstjenesterne. Privatlivshensynet tilsiger, at de overførte personoplysninger skal undergives den samme stærke beskyttelse uanset den konkrete risiko. Med EU-Domstolens fortolkning af GDPR art. 46 pålægges den dataansvarlige som bekendt en vidtgående undersøgelsespligt, der ellers kun gjaldt for Kommissionen. EU-Domstolens fortolkning er et fingerpeg om, at det i forbindelse med tredjelandsoverførsler til usikre tredjelande ifølge EU-Domstolen er privatlivshensynet, der vægtes højest. Dette kan ses i sammenhæng med, at retten til privatliv og databeskyttelse netop hviler på de grundlæggende rettigheder i Chartret, der efter EU-retten gælder på traktatniveau. Ved fortolkningen af de brede bestemmelser i GDPR kan den stærke grundrettighedsbeskyttelse således have afgørende betydning for, om det på den ene side er praktiske hensyn eller på den anden side hensynet til privatlivsbeskyttelse, der i det konkrete tilfælde tillægges størst betydning.[117]

Disse betragtninger må også gælde ved vurderingen af rækkevidden af den risikobaserede tilgang, der synes at hvile på brede formuleringer i eksempelvis generalklausulen i GDPR art. 24, stk. 1, og Kommissionens standardkontraktbestemmelser. Med henvisning til de grundlæggende rettigheders betydelige vægt kan der stilles spørgsmålstegn ved, om den dataansvarlige på baggrund af egne subjektive vurderinger bør indrømmes adgang til i visse tilfælde at implementere mindre indgribende supplerende foranstaltninger end eksempelvis kryptering, når der overføres personoplysninger til et usikkert tredjeland som USA. Såfremt den dataansvarlige overfører personoplysninger i en forretningsmæssig sammenhæng, er det desuden en nærliggende mulighed, at denne vil have en tendens til at undervurdere de eventuelle risici forbundet med overførslen. Bliver de overførte personoplysninger genstand for overvågning, vil det fra et juridisk perspektiv imidlertid kunne have fatale konsekvenser: De amerikanske myndigheder kan forårsage et brud på flere af den registreredes grundlæggende rettigheder efter eksempelvis Chartrets art. 7, 8 og 47. Om der findes forretningsmæssige hensyn, der kan opveje denne risiko, er tvivlsomt.

[117] Udsen, Henrik, *IT-ret*, 4. udgave, 1. oplag, 2019, s. 328 f.

7.2.3. Teoretisk usikkerhed og praktiske realiteter

Selvom de grundlæggende rettigheder tilsiger, at den dataansvarlige ikke bør kunne lægge vægt på subjektive vurderinger af den konkrete risiko for amerikansk overvågning, er dette udelukkende en fortolkning og ikke udtryk for en klar retstilstand. Når den dataansvarlige overfører personoplysninger til USA på baggrund af Kommissionens standardkontraktbestemmelser, må denne derfor forholde sig til en vis teoretisk usikkerhed om indholdet og rækkevidden af de risikobaserede bestemmelser i GDPR og standardkontraktbestemmelser. Denne usikkerhed styrkes blot af høringsversionen af EDPB's Henstilling 01/2020 og Kommissionens udkast til 2020-bestemmelserne, som synes at give udtryk for forskellige opfattelser.

Selvom EDPB ikke intervenerer i Datatilsynets kompetence, må det i kraft af Datatilsynets medlemskab af EDPB forventes, at Datatilsynet i vidt omfang vil lægge EDPB's opfattelse til grund. Dette skal sammenholdes med den kendsgerning, at Datatilsynet i medfør af DBL § 27, stk. 1, fører tilsyn med overholdelsen af de persondataretlige regler, og at Datatilsynet i denne forbindelse eksempelvis kan indgive en politianmeldelse, når tilsynet vurderer, at domstolene kan idømme en bøde for brud på persondatarettens regler. Selvom Henstilling 01/2020 som bekendt ikke er retligt bindende, vil den dataansvarlige derfor sædvanligvis bestræbe sig på at behandle personoplysninger i overensstemmelse med EDPB's opfattelse og dermed implementere de supplerende foranstaltninger, der ifølge EDPB er de rette, eksempelvis kryptering. I praksis har Henstilling 01/2020 derfor betydelig vægt og en højere retskildeværdi, end sædvanlig retskildeopfattelse tilsiger.[118]

Af netop denne årsag er det af væsentlig praktisk interesse, hvilken position EDPB indtager i sin endelige version af Henstilling 01/2020. Såfremt EDPB fastholder sin tilgang som fastsat i høringsversionen, vil spørgsmålet om, hvorvidt den dataansvarlige ved tredjelandsoverførsler til USA kan lægge en risikobaseret tilgang til grund, nærmere være af teoretisk fremfor praktisk interesse. Det retlige efterspil, der ses i kølvandet på Schrems II-dommen, illustrerer derfor, at de nationale tilsynsmyndigheder og EDPB har en høj status i dansk persondataret. Dette kan ses i sammenhæng med Chartret, der i art. 8, stk. 3, som bekendt indeholder et udtrykkeligt krav om oprettelse af

[118] Blume, Peter, *Persondatarettens kilder og metode*, 1. udgave, 1. oplag, 2020, s. 48 f. og 64; Udsen, Henrik, *IT-ret*, 4. udgave, 1. oplag, 2019, s. 457 og 473.

nationale tilsynsmyndigheder, der skal føre tilsyn med beskyttelsen af personoplysninger. I persondataretten har også tilsynsmyndighederne grundrettighedsstatus.

8. Hvordan løses den grundlæggende problematik?

Uagtet Schrems II-dommens afledte krav og teoretiske usikkerhed er den grundlæggende problematik klar. Det er et samspil mellem grundlæggende rettigheder i flere reguleringssystemer, der har dannet grobund for den gordiske knude, som den dataansvarlige må forholde sig til, når der overføres personoplysninger til USA på baggrund af Kommissionens standardkontraktbestemmelser. Spørgsmålet er derfor, hvordan den grundlæggende problematik kan adresseres.

8.1. Den dataansvarliges brug af databehandlere etableret i EU

I praksis vil den dataansvarlige ofte lade en databehandler behandle personoplysninger på den dataansvarliges vegne. Dette vil eksempelvis kunne ske i tilfælde, hvor den dataansvarlige anvender IT-tjenester leveret af en IT-udbyder.[119] I denne forbindelse påkalder det sig særlig interesse, at disse IT-udbydere ofte vil være amerikanske virksomheder som Amazon, Microsoft og Google. Hele 90 % af EU's data håndteres således af amerikanske virksomheder.[120] Dog vil den dataansvarliges brug af de amerikanske tjenester ikke altid indebære en direkte tredjelandsoverførsel til USA, men kan derimod også indebære en overførsel til et selskab etableret i EU, som vil være et datterselskab til et moderselskab etableret i USA.

At den dataansvarlige kan anvende databehandlere etableret i EU, imødekommer EU-Domstolen med Schrems II-dommen, som i præmis 134 ikke blot pålægger den dataansvarlige en undersøgelsespligt, men også "*dennes databehandler, som er etableret i Unionen*". EU-Domstolen går imidlertid ikke ind i en nærmere ansvarsfordeling den dataansvarlige og dennes databehandler imellem. Dette skal sammenholdes med den kendsgerning, at det i forbindelse med tredjelandsoverførsler både er den dataansvarlige og dennes databehandler, der er selvstændige pligtsubjekter, jf. GDPR

[119] Blume, Peter, *Databeskyttelsesret*, 5. udgave, 1. oplag, 2018, s. 67.
[120] EU-Kommissionen, *Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions – 2030 Digital Compass: the European way for the Digital Decade*, 9. marts 2021, s. 3 (fodnote 8).

art. 44. Dette giver anledning til at vurdere, om den dataansvarlige ved at anvende databehandlere etableret i EU helt kan undgå at tage stilling til Schrems II-dommens afledte krav og usikkerhed.

Ansvarlighedsprincippet i GDPR art. 5, stk. 2, indebærer som bekendt, at det er den dataansvarlige, der er ansvarlig for og skal kunne påvise overholdelse af reglerne i GDPR. Ansvarlighedsprincippet skal læses i sammenhæng med GDPR art. 28, stk. 1. Hvis en behandling, herunder en tredjelandsoverførsel, skal foretages på vegne af en dataansvarlig, må den dataansvarlige ifølge denne bestemmelse udelukkende anvende databehandlere, der kan sikre tilstrækkelig sikkerhed og i øvrigt sikre, at behandlingen kan ske under overholdelse af kravene efter EU-retten. Dette indebærer, at den dataansvarlige, inden denne påbegynder samarbejdet med en databehandler, skal tage aktivt stilling til, om databehandleren har vilje og evne til at sikre overholdelse af disse krav. Også i denne forbindelse skal den dataansvarlige tage amerikansk lovgivning i betragtning. Efter den føderale lovgivning i den såkaldte CLOUD Act fremgår det eksempelvis, at de amerikanske myndigheder kan kræve data udleveret fra en elektronisk kommunikationsudbyder eller en udbyder af fjerndatabehandling, uanset om den pågældende data er lokaliseret i USA.[121] Hvornår en udbyder etableret i EU kan være omfattet af denne lovgivning er ikke klart, men kunne tænkes at være tilfældet i situationer, hvor udbyderen har visse forbindelser til USA, eksempelvis hvis udbyderen er et datterselskab til et amerikansk moderselskab. Under alle omstændigheder har EDPB og EDPS bekræftet, at den amerikanske lovgivnings eksterritoriale virkning for visse udbydere etableret i EU kan give anledning til en lovkonflikt mellem amerikansk ret og EU-retten, da en udlevering af personoplysninger som bekendt kan være i strid med de europæiske databeskyttelsesregler.[122]

Den dataansvarlige skal således, eventuelt i samarbejde med databehandleren, vurdere, om databehandleren kan være omfattet af CLOUD Act og dermed også kan blive genstand for indsigtsanmodninger fra de amerikanske efterretningstjenester. Såfremt det vurderes, at dette er tilfældet, må det anses som usikkert, om den dataansvarlige ved sin vurdering af databehandlerens sikkerhedsniveau må inddrage betragtninger om risikoen for indsigtsanmodninger fra de amerikanske

[121] 18 U.S.C. § 2713 (2018); 18. U.S.C. § 2703 (2018).
[122] EDPB og EDPS, *ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence*, 10. juli 2019, s. 1 f.

efterretningstjenester. Den ovennævnte usikkerhed om rækkevidden af den risikobaserede tilgang, når den dataansvarlige gennemfører en direkte tredjelandsoverførsler til USA, gør sig således også gældende, når den dataansvarlige overfører personoplysninger til en EU-baseret databehandler med forbindelser til USA. Såfremt den dataansvarlige lægger EDPB's restriktive forståelse af den risikobaserede tilgang til grund, vil den dataansvarlige som bekendt være forpligtet til at udelukke enhver risiko for de amerikanske myndigheders disproportionale adgang til personoplysninger om europæiske registrerede. I givet fald er det nærliggende, at den dataansvarlige inden overførslen til databehandleren etableret i EU krypterer de pågældende personoplysninger, evt. med udgangspunkt i EDPB's krypteringsstandarder i Henstilling 01/2020.

Såfremt den dataansvarlige vurderer, at databehandleren i overensstemmelse med GDPR art. 28, stk. 1, kan sikre den fornødne sikkerhed, skal den dataansvarlige og databehandleren indgå en databehandleraftale, jf. GDPR art. 28, stk. 3. I denne aftale skal den dataansvarlige angive, hvornår og under hvilke betingelser, databehandleren må gennemføre en tredjelandsoverførsel, eller om tredjelandsoverførsler overhovedet tillades, jf. GDPR art. 28, stk. 3, litra a. Med henvisning til det brede overførselsbegreb skal det i denne forbindelse fremhæves, at også et amerikansk etableret selskabs fjernadgang til at se oplysninger, der lagres hos et europæisk selskab, uden at disse oplysninger overføres ud af EU som sådan, også vil udgøre en tredjelandsoverførsel til USA. Såfremt den dataansvarlige tillader overførsler til et usikkert tredjeland som USA, skal den dataansvarlige pålægge databehandleren at gennemføre den efter Schrems II-dommen påkrævede undersøgelsespligt og implementere de nødvendige supplerende foranstaltninger, eventuelt den i Henstilling 01/2020 nævnte kryptering. I overensstemmelse med ansvarlighedsprincippet skal den dataansvarlige løbende føre tilsyn med, at databehandleren overholder de forpligtelser, den er blevet pålagt i kraft af databehandleraftalen.[123]

Undlader den dataansvarlige at iagttage ovennævnte forpligtelser, vil det være en selvstændig overtrædelse af GDPR art. 5 og 28, som begge er strafbelagte, jf. DBL § 41, stk. 2, nr. 1, og § 41, stk. 1, nr. 1. Selvom databehandleren er et selvstændigt pligtsubjekt efter reglerne om

[123] Mortensen, Bent Ole Gram m.fl., *Dansk persondataret*, 1. udgave, 1. oplag, 2020, s. 189 f.; Blume, Peter, *Databeskyttelsesret*, 5. udgave, 1. oplag, 2018, s. 67 f.

tredjelandsoverførsler i GDPR, står det således klart, at den dataansvarlige ikke i kraft af databehandlerkonstruktioner kan undgå at tage aktivt stilling til de krav og den usikkerhed, der efter Schrems II-dommen formelt set ellers kun gælder, når der gennemføres en direkte tredjelandsoverførsel på baggrund af Kommissionens standardkontraktbestemmelser. Den dataansvarlige kan ikke uden videre forlade sig på, at databehandleren overholder reglerne.

8.2. En ny Privacy Shield-ordning, lovændringer og teknologiens udvikling

Det står herefter klart, at det er ude af den dataansvarliges hænder at løse de grundlæggende problematikker. Derfor er det af væsentlig interesse, hvilke tiltag lovgiver, Kommissionens samt de amerikanske myndigheder kan iværksætte.

Det er i teorien blevet hævdet, at en global ordning i form af en konvention, som flere lande tilslutter sig, på længere sigt kan være løsningen på de problematikker, som internationale tredjelandsoverførsler giver anledning til.[124] I en stadig mere globaliseret verden kan der utvivlsomt stilles spørgsmålstegn ved, om reguleringen af tredjelandsoverførsler overhovedet bør udspringe af lokal EU-retlig regulering. Umiddelbart kan en international konventionen, der regulerer tredjelandsoverførsler, derfor fremstå som en oplagt mulighed. Med henvisning til de grundlæggende rettigheder i CPR-Konventionens art. 17, der som bekendt adresserer spørgsmål relaterende til databeskyttelse, kan det imidlertid påpeges, at verdenssamfundet allerede har forsøgt sig med globale løsninger. I relation til tredjelandsoverførsler fra EU til USA har disse løsninger ikke vist sig holdbare. Erfaringerne med CPR-Konventionen viser, at dette navnlig skyldes manglende håndhævelsesmuligheder, hvilket netop er ét af folkerettens grundlæggende karakteristika. En global ordning er derfor ikke nærliggende.

Det amerikanske forskningsinstitut, CRS, der yder viden til Kongressen i USA, fremhæver imidlertid andre løsninger.[125] I en rapport fra marts 2021 foreslås det bl.a., at de amerikanske myndigheder og Kommissionen forhandler en ny rammeaftale på plads, der kan erstatte Privacy Shield-ordningen.[126]

[124] Blume, Peter, *Databeskyttelsesret*, 5. udgave, 1. oplag, 2018, s. 282 ff.
[125] Library of Congress, *About CRS,* https://www.loc.gov/crsinfo/about/ (sidst besøgt: 9/5 2021).
[126] CRS, Report R46724, *EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield*, 2021, s. 12 f.

Allerede i august 2020 blev det i en pressemeddelelse fra Kommissionen og det amerikanske handelsministerium tilkendegivet, at parterne har indledt forhandlinger om mulighederne for en "*forbedret*" aftale, ligesom forhandlingerne i marts 2021 blev "*intensiveret*".[127] Med et nyt overførselsgrundlag vedtaget med hjemmel i GDPR art. 45 vil den dataansvarlige selvsagt kunne undgå at anvende Kommissionens standardkontraktbestemmelser og dermed også at tage stilling til EU-Domstolens krav som fastsat i Schrems II. Løsningen vil dog ikke i sig selv adressere den amerikanske sikkerhedslovgivning, der begrundede tilsidesættelsen af såvel Safe Harbor- og Privacy Shield-ordningen. Medmindre en ny ordning og de deri indeholdte persondataretlige principper tillægges forrang for den amerikanske sikkerhedslovgivning, vil det blot være et spørgsmål om tid, før ordningen lider samme skæbne som dens forgængere.

Ændringer af den amerikanske sikkerhedslovgivning er derfor nærliggende. CRS foreslår, at den amerikanske præsident kan udstede et præsidentielt dekret lignende PPD-28, der begrænser den amerikanske overvågning af udlændinge yderligere. Derudover kan der i FISA indføjes et krav om retskendelse fra domstolene for hver enkelt person, der bliver genstand for overvågning. Som CRS selv understreger, skal de nye amerikanske regler ligeledes tildele de registrerede adgang til at anlægge sag mod efterretningstjenesterne ved domstolene, såfremt de måtte mene, at de er blevet genstand for ulovlig overvågning. Netop dette vil ifølge CRS dog rejse komplekse forfatningsmæssige problematikker i relation til bl.a. forfatningens art. III. [128]

Selv går CRS ikke nærmere ind i dette spørgsmål. Det skal dog fremhæves, at forfatningens art. III indeholder et krav om, at en sagsøger for at kunne gøre en krænkelse gældende mod en sagsøgt skal have en retlig interesse i sagen. I relation til sager om retten til privatliv efter forfatningens fjerde tilføjelse har Højesteretten i Rakas-sagen fortolket kravet således, at sagsøgeren skal bevise,

[127] Kommissionen, *Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross*, https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en (sidst besøgt: 9/5 2021); Kommissionen, *Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo,* https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1443 (sidst besøgt: 9/5 2021).

[128] CRS, Report R46724, *EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield*, 2021, s. 12 f.

at vedkommende har været genstand for en personlig krænkelse af sit privatliv.[129] Hvilke konsekvenser denne processuelle begrænsning har i relation til den amerikanske overvågning, viste sig i Clapper-sagen. Her gjorde amerikanske sagsøgere gældende, at de i kraft af deres samarbejde med ikke-amerikanere i udlandet blev genstand for overvågning med hjemmel i FISA Section 702, da bestemmelsen angiveligt giver efterretningstjenesterne mulighed for at opnå adgang til oplysninger om både amerikanere og ikke-amerikaner, hvis blot én af personerne er ikke-amerikaner. Ifølge de amerikanske sagsøgere var dette i strid med deres rettigheder efter den fjerde tilføjelse. Højesteretten afviste imidlertid søgsmålet, da sagsøgerne ikke kunne bevise, at de rent faktisk havde været genstand for den pågældende overvågning. Sagsøgernes påstande var ifølge Højesteretten baseret på rene spekulationer.[130]

Selvom en ændring af FISA eller et nyt præsidentielt dekret synes oplagt, illustrerer Clapper-sagen, at der i amerikansk ret gælder væsentlige processuelle begrænsninger på forfatningsniveau, når der skal anlægges sag mod myndighederne på baggrund af en påstand om ulovlig overvågning. Dette er meget vel begrænsninger, der kan forhindre, at ændringer af føderal lovgivning er tilstrækkeligt for at bringe amerikansk lovgivning i overensstemmelse med Chartret, navnlig art. 47 om adgang til effektive retsmidler.

Indtil der måtte findes en juridisk løsning, der både er holdbar i længden og kan accepteres på begge sider af Atlanten, ulmer teknologien i baggrunden. Selvom GDPR er et teknologineutralt regelsæt, der i princippet skulle kunne håndtere alle former for teknologi, er forordningen i kraft af de særlige regler om tredjelandsoverførsler baseret på en forudsætning om geografisk afgrænsning rundt om EU.[131] Dette går imidlertid ikke hånd i hånd med de europæiske virksomheders hyppige brug af IT-løsninger leveret af amerikanske leverandører. Kommissionen har imidlertid tilkendegivet, at der skal arbejdes for europæisk digital suverænitet. I denne henseende er det ifølge Kommissionen relevant at tage den såkaldte cloud-computing-teknologi i betragtning. Cloud-teknologien indebærer leje og brug af ekstern software, der opbevares på cloud-udbyderens server, hvilket er særdeles

[129] Rakas v. Illinois, 439 U.S. 128, 132-134 (1978).
[130] Clapper v. Amnesty International USA, 568 U.S. 398 (2013), Opinion of the Court, pp. 7-15; Gray, David, *The Fourth Amendment in an Age of Surveillance*, 2017, s. 89 ff.
[131] Blume, Peter, *Persondatarettens kilder og metode*, 1. udgave, 1. oplag, 2020, s. 13.

populært i Danmark og resten af EU.[132] Ifølge Kommissionen har EU-baserede cloud-udbydere imidlertid en for lille andel i cloud-markedet, og derfor skal der arbejdes for en fælleseuropæisk cloud-infrastruktur. De enkelte EU-medlemsstater har i en deklaration fra oktober 2020 tilkendegivet, at de er villige til at arbejde sammen om en sådan cloud-løsning, og i deklarationen henvises der til europæiske initiativer, der allerede er blevet iværksat.[133] Selvom der endnu er lang vej til egentlig europæisk datasuverænitet, der helt vil frigøre europæiske virksomheder fra de amerikanske leverandører, tyder det således på, at der er politisk vilje til at forene teknologien med de europæiske regler om databeskyttelse og europæernes grundlæggende rettigheder.

9. Konklusion

Siden Edward Snowdens afsløringer i 2013 har det været kendt, at de amerikanske efterretningstjenester gennemfører masseovervågning af individers kommunikation ved hjælp af overvågningsprogrammer. Også den danske dataansvarlige må forholde sig til denne overvågning, når denne ønsker at overføre personoplysninger til USA, EU's vigtigste handelspartner. Dette gør sig også gældende, når Kommissionens standardkontraktbestemmelser efter GDPR art. 46, stk. 2, litra c, anvendes som overførselsgrundlag.

Med EU-Domstolens dom i Schrems II står det klart, at den dataansvarlige kun kan gennemføre en tredjelandsoverførsel på baggrund af Kommissionens standardkontraktbestemmelser, såfremt de personer, hvis personoplysninger overføres til et tredjeland, sikres et databeskyttelsesniveau, der *"i det væsentlige"* svarer til det niveau, der er sikret efter EU-retten. Som Schrems II-dommen illustrerer, gælder der i det EU-retlige reguleringssystem imidlertid flere grundlæggende rettigheder efter Chartret, som den amerikanske sikkerhedslovgivning ikke overholder. Hverken FISA Section 702, E.O. 12333 samt PPD-28 definerer rækkevidden af eventuelle indgreb i europæernes grundlæggende rettigheder til privatliv og databeskyttelse efter Chartrets art. 7 og 8, hvorfor lovgivningen

[132] Eurostat, *Cloud computing - statistics on the use by enterprises*, https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises (sidst besøgt: 9/5 2021).
[133] EU-Kommissionen, *Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions – 2030 Digital Compass: the European way for the Digital Decade*, 9. marts 2021, s. 1 og 7; Kommissionen, *Towards a next generation cloud for Europe*, https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe (sidst besøgt: 9/5 2021).

er i strid med proportionalitetsprincippet i Chartrets art. 52, stk. 1, 2. pkt. Derudover er adgangen til effektive retsmidler efter den amerikanske lovgivning helt fraværende, hvorfor lovgivningen ligeledes er i strid Chartrets art. 47. Grundet EU-medlemsstaternes eneansvar på sikkerhedsområdet er medlemsstaterne imidlertid ikke selv underlagt de pågældende krav efter Chartret, når medlemsstaterne behandler personoplysninger af hensyn til den nationale sikkerhed. Modsat er de tredjelande, som den dataansvarlige måtte overføre personoplysninger til, herunder USA, omfattet. Dette samtidig med, at den fjerde tilføjelse i den amerikanske forfatning, der i et vist omfang ellers indeholder en grundlæggende ret til privatliv, kun omfatter amerikanske borgere og dermed indeholder en forfatningsmæssig legitimation af masseovervågning af ikke-amerikanere. Selvom USA har ratificeret CPR-Konventionens art. 17, der ligesom Chartret indeholder en beskyttelse mod den amerikanske sikkerhedslovgivning, fejler det internationale verdenssamfund imidlertid i at skabe en fælles folkeretlig databeskyttelsesstandard EU og USA imellem.

Når den dataansvarlige ønsker at gennemføre en tredjelandsoverførsel til USA, står den dataansvarlige således over for en retlig barriere, der udspringer af et samspil mellem grundrettigheder i flere reguleringssystemer. Om den dataansvarlige kan overkomme denne retlige barriere med Kommissionens standardkontraktbestemmelser, afhænger i første række af de retlige rammer for den dataansvarliges brug af dette overførselsgrundlag. Med Schrems II-dommen og EU-Domstolens fortolkning af GDPR art. 46 fastslås det, at den dataansvarlige pålægges to grundlæggende forpligtelser i forbindelse med brug af standardkontraktbestemmelserne. For det første skal den dataansvarlige for hver enkelt tredjelandsoverførsel undersøge, om lovgivningen i tredjelandet sikrer den fornødne beskyttelse henset til EU-retten. I denne forbindelse foretager EU-Domstolen imidlertid ikke en nærmere afgrænsning af de konkrete forhold, den dataansvarlige kan inddrage i sine undersøgelser. For det andet skal den dataansvarlige efter omstændighederne implementere foranstaltninger, der supplerer de kontraktuelle beskyttelsesmekanismer, der fremgår af standardkontraktbestemmelserne. Med udgangspunkt i EU-Domstolens præmisser står det klart, at sådanne supplerende foranstaltninger navnlig er nødvendige, når der overføres personoplysninger til et usikkert tredjeland som USA, som i kraft af en disproportional sikkerhedslovgivning gør indgreb i den registreredes rettigheder. EU-Domstolen går imidlertid ikke nærmere ind i, hvad de supplerende foranstaltninger konkret kan bestå i.

Når den dataansvarlige anvender Kommissionens standardkontraktbestemmelser som overførselsgrundlag ved tredjelandsoverførsler til USA, står denne herefter overfor et vigtigt valg mellem to forskellige muligheder.

Den ene mulighed indebærer, at den dataansvarlige i overensstemmelse med EDPB's opfattelse i høringsversionen af Henstilling 01/2020 anvender supplerende foranstaltninger, der helt udelukker risikoen for amerikansk overvågning af de personoplysninger, der overføres til USA. Ifølge EDPB kan en teknisk supplerende foranstaltning som stærk, forudgående kryptering af de overførte personoplysninger være et middel til at nå dette mål. Da der er væsentlige modgående hensyn til en sådan kryptering, herunder at den amerikanske dataimportør kan se og anvende oplysningerne, afføder krypteringsløsningen imidlertid praktiske barrierer, som den dataansvarlige må overkomme.

Den anden mulighed er forbundet med teoretisk usikkerhed. Denne mulighed hviler på spørgsmålet om, hvorvidt den dataansvarlige uden at gå på kompromis med persondatarettens regler i visse tilfælde kan træffe supplerende foranstaltninger, der ikke helt udelukker risikoen for, at de amerikanske efterretningstjenester opnår adgang til de overførte personoplysninger. I praksis kunne dette tænkes at være tilfældet i den situation, hvor den dataansvarlige overfører personoplysninger til en amerikansk dataimportør, der ikke har erfaring med efterretningstjenesternes indsigtsanmodninger i de personoplysninger, som den konkrete dataimportør behandler. Om den dataansvarlige kan indrømmes en sådan adgang, afhænger af, hvornår denne kan siges at have udvist den fornødne grad af ansvarlighed efter GDPR art. 5, stk. 2. I denne forbindelse er den dataansvarliges forudgående undersøgelser af det amerikanske databeskyttelsesniveau af væsentlig betydning, men det er uklart, om den dataansvarlige som led i disse undersøgelser kan tillægge subjektive vurderinger af den konkrete risiko for overvågning vægt. Generelt set er den dataansvarliges risikovurderinger en væsentlig del af GDPR, når forordningens krav om ansvarlighed skal iagttages. Ydermere indikerer formuleringen af Kommissionens standardkontraktbestemmelser, at dette også gør sig gældende ved tredjelandsoverførsler til et usikkert tredjeland som USA. På den anden side afviser EDPB, at den dataansvarlige kan lægge en risikobaseret tilgang til grund. Ligeledes peger de grundlæggende rettigheder til privatliv og databeskyttelse i retning af, at fortolkningen af de risikobaserede

bestemmelser i såvel GDPR og standardkontraktbestemmelser må falde ud til fordel for privatlivshensyn på bekostning af det praktiske hensyn til at kunne overføre personoplysninger til USA. Uanset denne teoretiske usikkerhed må det dog forventes, at den dataansvarlige i kraft af Datatilsynets og EDPB's særlige rolle i dansk persondataret vil bestræbe sig på at implementere de supplerende foranstaltninger, der efter Henstilling 01/2020 er de rette, eksempelvis kryptering. Dette uanset, at Henstilling 01/2020 efter TEUF art. 288, 5. pkt. ikke er formelt bindende for den dataansvarlige.

Den dataansvarlige kan ikke ved at anvende databehandlere etableret i EU undgå at forholde sig til de krav og den teoretiske usikkerhed, der er blevet affødt af Schrems II-dommen og grundlæggende rettigheder. I medfør af GDPR art. 5, stk. 2, og art. 28, stk. 1, skal den dataansvarlige tage aktivt stilling til databehandlerens vilje og evne til at sikre overholdelse af de krav, der gælder efter EU-retten. Ligeledes skal den dataansvarlige føre løbende tilsyn med, at databehandleren ikke overfører personoplysninger til USA i strid med de krav, der følger af Schrems II-dommen. Da det således er ude af den dataansvarliges hænder at løse de grundlæggende problematikker, er det af væsentlig interesse, hvad lovgiver, de amerikanske myndigheder og Kommissionen kan foretage sig. Der er angiveligt en ny overførselsordning på vej, der kan erstatte Privacy Shield. Da EU-Domstolen med henvisning til den amerikanske sikkerhedslovgivning ad to omgange har tilsidesat ordninger som disse, synes det mere holdbart, at den amerikanske lovgiver ændrer den amerikanske sikkerhedslovgivning. Da forfatningens art. III indeholder processuelle begrænsninger i, hvornår ulovlig overvågning kan gøres gældende, er ændringer af føderal lovgivning dog muligvis ikke tilstrækkeligt til at bringe amerikansk lovgivning i overensstemmelse med Chartret. I denne forbindelse skal det dog påpeges, at det ikke kun er juridiske løsninger, der er tilgængelige. Udmeldinger fra Kommissionen og EU-medlemsstaterne synes at indikere, at der politisk vilje til at skabe teknologiske løsninger, der med tiden kan sikre, at europæernes grundlæggende rettigheder ikke sættes på spil.

10. Litteraturliste

Artikler

Balkin, Jack M., *The Constitution in the National Surveillance State*, Minnesota Law Review, 93.1, 2008.

Gjerstad, Marianne og Vanebo, Ole A., *Schrems II: Faktisk risiko bør spille en rolle ved overføring av personopplysninger til tredjestater*, Lov & Data, 145.1, 2021.

Gonçalves, Maria Eduarda, *The risk-based approach under the new EU data protection regulation: a critical perspective*, Journal of Risk Research, 23.2, 2020.

Patel, Oliver og Lea, Nathan, *EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows*, UCL European Institute, 2020.
Tilgængelig her: https://www.ucl.ac.uk/european-institute/sites/european-institute/files/privacy_shield_brexit_and_the_future_of_transatlantic_data_flows_1.pdf (sidst besøgt: 4/5 2020).

Quigley, John, *The International Covenant on Civil and Political Rights and the Supremacy Clause*, DePaul Law Rewiew, 42.4, 1993.

Bøger

Blume, Peter, *Databeskyttelsesret*, Jurist- og Økonomforbundets Forlag, 5. udgave, 1. oplag, 2018.

Blume, Peter, *Den nye persondataret*, Jurist- og Økonomforbundets Forlag, 2. udgave, 1. oplag, 2018.

Blume, Peter, *Persondatarettens kilder og metode*, Djøf Forlag, 1. udgave, 1. oplag, 2020.

Christoffersen, Jonas m.fl., *EU's Charter om Grundlæggende Rettigheder med kommentarer*, Jurist- og Økonomforbundets Forlag, 2. udgave, 1. oplag, 2018.

Germer, Peter, *Indledning til folkeretten*, Jurist- og Økonomforbundets Forlag, 4. udgave, 4. oplag, 2010.

Gray, David, *The Fourth Amendment in an Age of Surveillance*, Cambridge University Press, 2017.

Gregory, Anthony, *American Surveillance*, University of Wisconsin Press, 2016.

Mortensen, Bent Ole Gram m.fl., *Dansk persondataret*, Ex Tuto Publishing A/S, 1. udgave, 1. oplag, 2020.

Nielsen, Kristian Korfits og Lotterup, Anders, *Databeskyttelsesforordningen og databeskyttelsesloven*, Jurist- og Økonomforbundets Forlag, 1. udgave, 1. oplag, 2020.

Regan, Priscilla M., *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, 1995.

Rytter, Jens Elo, *Individets grundlæggende rettigheder*, Karnov Group Denmark A/S, 3. udgave, 1. oplag, 2019.

Simmons, Ric, *Smart Surveillance – How to Interpret the Fourth Amendment in the Twenty-First Century*, Cambridge University Press, 2019.

Storgaard, Louise Halleskov m.fl., *Folkeret og menneskerettigheder*, Karnov Group Denmark A/S, 1. udgave, 1. oplag, 2019.

Taylor, Paul M., *A Commentary on the International Covenant on Civil and Political Rights*, Cambridge University Press, 2020.

Tvarnø, Christina D. og Nielsen, Ruth, Jurist- og Økonomforbundets Forlag, *Retskilder og retsteorier*, 5. reviderede udgave, 1. oplag, 2017.

Udsen, Henrik, *IT-ret*, Ex Tuto Publishing A/S, 4. udgave, 1. oplag, 2019.

Domme

<u>EU-Domstolen</u>

Dom af 16. juli 2020, Sag C-311/18, *Facebook Ireland og Schrems*.
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:62018CJ0311&from=DA (sidst besøgt: 5/5 2021).

Dom af 6. oktober 2015, Sag C-362/14, *Schrems*.
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:62014CJ0362&from=DA (sidst besøgt: 5/5 2021).

Udtalelse 2/13 af 18. december 2014.
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:62013CV0002&from=da (sidst besøgt: 5/5 2021).

<u>Højesteretten</u>

Clapper v. Amnesty International USA, 568 U.S. 398 (2013).
Tilgængelig her: https://supreme.justia.com/cases/federal/us/568/11-1025/case.pdf (sidst besøgt: 9/5 2021).

Katz v. United States, 389 U.S. 347 (1967).
Tilgængelig her: https://supreme.justia.com/cases/federal/us/389/347/ (sidst besøgt: 5/5 2021).

Olmstead v. United States, 277 U.S. 438 (1928).
Tilgængelig her: https://supreme.justia.com/cases/federal/us/277/438/ (sidst besøgt: 5/5 2021).

Rakas v. Illinois, 439 U.S. 128 (1978).
Tilgængelig her: https://supreme.justia.com/cases/federal/us/439/128/ (sidst besøgt: 9/5 2021).

United States v. United States Dist. Ct., 407 U.S. 297 (1972).
Tilgængelig her: https://supreme.justia.com/cases/federal/us/407/297/ (sidst besøgt: 5/5 2021).

United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).
Tilgængelig her: https://supreme.justia.com/cases/federal/us/494/259/ (sidst besøgt: 5/5 2021).

EDPB og EDPS

EDPB, *Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies*, version 2.0, 15. december 2020.
Tilgængelig her: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf (sidst besøgt: 4/5 2021).

EDPB, *Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger*, version til offentlig høring, 10. november 2020.
Tilgængelig her: BILAG A.

EDPB og EDPS, *ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence*, 10. juli 2019.
Tilgængelig her: https://edps.europa.eu/sites/edp/files/publication/19-07-10_edpb_edps_cloudact_annex_en.pdf (sidst besøgt: 8/5 2021).

EDPB og EDPS, *Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46(2)(c) of Regulation (EU) 2016/679.*
Tilgængelig her: https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf (sidst besøgt: 7/5 2021).

EDPB, *Retningslinjer 2/2018 vedrørende undtagelser i artikel 49 i forordning 2016/679*, 25. maj 2018.
Tilgængelig her: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_da.pdf (sidst besøgt: 4/5 2021).

Internetsider

EUR-Lex, *EU-rettens direkte virkning*.
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/ALL/?uri=uriserv%3Al14547 (sidst besøgt: 4/5 2021).

Eurostat, *Cloud computing - statistics on the use by enterprises*.
Tilgængelig her: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises (sidst besøgt: 9/5 2021).

Fieldfisher, *US surveillance: s702 FISA, EO 12333, PRISM and UPSTREAM.*
Tilgængelig her: https://www.fieldfisher.com/en/insights/us-surveillance-s702-fisa-eo-12333-prism-and-ups (sidst besøgt: 5/5 2021).

Kommissionen, *Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo.*
Tilgængelig her: https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1443 (sidst besøgt: 9/5 2021).

Kommissionen, *Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross*.
Tilgængelig her: https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en (sidst besøgt: 9/5 2021).

Kommissionen, *Towards a next generation cloud for Europe*.
Tilgængelig her: https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe (sidst besøgt: 9/5 2021).

Kommissionen, *Trade, policy, Countries and regions, United States.*
Tilgængelig her: https://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/ (sidst besøgt: 4/5 2021).

Library of Congress, *About CRS.*
Tilgængelig her: https://www.loc.gov/crsinfo/about/ (sidst besøgt: 9/5 2021).

National Constitution Center, *The Supremacy Clause*.
Tilgængelig her: https://constitutioncenter.org/interactive-constitution/interpretation/article-vi/clauses/31 (sidst besøgt: 4/5 2021).

United Nations Human Rights, *Optional Protocol to the International Covenant on Civil and Political Rights.*
Tilgængelig her: https://indicators.ohchr.org (sidst besøgt: 17/5 2021).

United Nations Treaty Collection, *4. International Covenant on Civil and Political Rights*.
Tilgængelig her: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en#EndDec (sidst besøgt: 6/5 2021).

USA.gov, *How Laws Are Made and How to Research Them.*
Tilgængelig her: https://www.usa.gov/how-laws-are-made (sidst besøgt: 4/5 2021).

Kommissionen

COMMISSION IMPLEMENTING DECISION (EU) …/… on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Document Ares(2020)6654686).
Tilgængelig her: BILAG B.

Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions – 2030 Digital Compass: the European way for the Digital Decade (COM(2021) 118 final), 9. marts 2021.
Tilgængelig her: https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02/DOC_1&format=PDF (sidst besøgt: 8/5 2021).

Kommissionens afgørelse af 5. februar 2010 om standardkontraktbestemmelser for videregivelse af personoplysninger til registerførere etableret i tredjelande i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF (EU-Tidende nr. L 39 af 12. februar 2010, s. 5).
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32010D0087&from=DA (sidst besøgt: 4/5 2021).

Kommissionens beslutning af 15. juni 2001 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til direktiv 95/46/EF (De Europæiske Fællesskabers Tidende nr. L 181 af 4. juli 2001, s. 19).
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32001D0497&from=DA (sidst besøgt: 4/5 2021).

Kommissionens beslutning af 27. december 2004 om ændring af beslutning 2001/497/EF for at indføre en alternativ standardkontrakt om overførsel af personoplysninger til tredjelande (EU-Tidende nr. L 385 af 29. december 2004, s. 74).
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32004D0915&from=DA (sidst besøgt: 4/5 2021).

Kommissionens beslutning 2000/520/EF af 26. juli 2000 i henhold til direktiv 95/46 om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af Safe Harbor-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium (De Europæiske Fællesskabers Tidende nr. L 215 af 25. august 2000).
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32000D0520&from=DA (sidst besøgt: 5/5 2021).

Kommissionens gennemførelsesafgørelse (EU) 2016/1250 af 12. juli 2016 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred (EU-Tidende nr. L 207 af 1. august 2016, s. 1).
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016D1250&from=DA (sidst besøgt: 5/5 2021).

Kommissionens gennemførelsesafgørelse (EU) 2016/2297 af 16. december 2016 om ændring af beslutning 2001/497/EF og afgørelse 2010/87/EU om standard-kontraktbestemmelser for videregivelse af personoplysninger til tredjelande og registerførere etableret i tredjelande i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF (EU-Tidende nr. L 344 af 17. december 2016, s. 100).
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016D2297&from=DA (sidst besøgt: 4/5 2021).

Lovgivning

<u>Amerikansk ret</u>

U.S. Const. amend. IV.
Tilgængelig her: https://law.justia.com/constitution/us/amendments-text-only.html (sidst besøgt: 13/5 2021).

18. U.S.C. § 2703 (2018).
Tilgængelig her: https://statecodesfiles.justia.com/us/2018/title-18/part-i/chapter-121/sec-2703/sec-2703.pdf?ts=1588213471 (sidst besøgt: 16/5 2021).

18 U.S.C. § 2713 (2018).
Tilgængelig her: https://statecodesfiles.justia.com/us/2018/title-18/part-i/chapter-121/sec-2713/sec-2713.pdf?ts=1588213472 (sidst besøgt: 16/5 2021).

50 U.S.C. § 1801 (2018).
Tilgængelig her: https://statecodesfiles.justia.com/us/2018/title-50/chapter-36/subchapter-i/sec-1801/sec-1801.pdf?ts=1588215885 (sidst besøgt: 16/5 2021).

50 U.S.C. § 1881a (2018).
Tilgængelig her: https://statecodesfiles.justia.com/us/2018/title-50/chapter-36/subchapter-vi/sec-1881a/sec-1881a.pdf?ts=1588215888 (sidst besøgt: 16/5 2021).

Dansk ret

Databeskyttelsesloven (lov nr. 502 af 23. maj 2018).
Tilgængelig her: https://www.retsinformation.dk/eli/lta/2018/502 (sidst besøgt: 13/5 2021).

Persondataloven (lov nr. 429 af 31. maj 2000).
Tilgængelig her: https://www.retsinformation.dk/eli/lta/2000/429 (sidst besøgt: 13/5 2021).

EU-ret

Den Europæiske Unions charter om grundlæggende rettigheder (EU-Tidende nr. C 202/2 af 7. juni 2016, s. 389).
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN (sidst besøgt: 13/5 2021).

Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (De Europæiske Fællesskabers Tidende nr. L 281 af 23. november 1995, s. 31).
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:31995L0046&from=DA (sidst besøgt: 13/5 2021).

Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EU-Tidende nr. L 119 af 4. maj 2016, s. 1).
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=DA (sidst besøgt: 13/5 2021).

Konsolideret udgave af traktaten om Den Europæiske Union (EU-Tidende nr. C 202/1 af 7. juni 2016, s. 13).
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=OJ:C:2016:202:FULL&from=FR (sidst besøgt: 13/5 2021).

Konsolideret udgave af traktaten om Den Europæiske Unions funktionsmåde (EU-Tidende nr. C 202/1 af 7. juni 2016, s. 47).
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=OJ:C:2016:202:FULL&from=FR (sidst besøgt: 13/5 2021).

Folkeret

FN's konvention om borgerlige og politiske rettigheder med tilhørende valgfri protokol (UNTS Vol. 999, No. 14668, p. 171; bekendtgørelse nr. 30 af 29. marts 1976).
Tilgængelig her: https://www.retsinformation.dk/eli/ltc/1976/30 (sidst besøgt: 13/5 2021).

Wienerkonventionen om traktatretten (UNTS Vol. 1155, No. 18232, p. 331; bekendtgørelse nr. 34 af 29. april 1980).
Tilgængelig her: https://www.retsinformation.dk/eli/ltc/1980/34 (sidst besøgt: 13/5 2021).

Øvrige

Artikel 29-gruppen, *Statement on the role of a risk-based approach in data protection legal frameworks (WP 218)*, 30. maj 2014.
Tilgængelig her: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf (sidst besøgt: 7/5 2021).

CRS, *Presidential Directives: An Introduction*, 2019.
Tilgængelig her: https://fas.org/sgp/crs/natsec/IF11358.pdf (sidst besøgt: 4/5 2021).

CRS, Report RL32528, Mulligan, Stephen P., *International Law and Agreements: Their Effect upon U.S. Law*, 2018.
Tilgængelig her: https://fas.org/sgp/crs/misc/RL32528.pdf (sidst besøgt: 6/5 2021).

CRS, Report R46724, *EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield,* 2021.
Tilgængelig her: https://crsreports.congress.gov/product/pdf/R/R46724 (sidst besøgt: 5/5 2021).

Department of Commerce m.fl., *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, 2020.
Tilgængelig her: https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF (sidst besøgt: 6/5 2021).

Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,* Office of Legal Education, Executive Office for United States Attorneys. *Tilgængelig her: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf (sidst besøgt: 7/5 2021).*

Generaladvokat H. Saugmandsgaard Øe, *Forslag til afgørelse,* 19. december 2019.
Tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:62018CC0311&from=DA (sidst besøgt: 5/5 2021).

Menneskerettighedskomitéen, CCPR/C/USA/CO/4, *Concluding observations on the fourth periodic report of the United States of America*, 2014.
Tilgængelig her: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR/C/USA/CO/4&Lang=En (sidst besøgt: 10/5 2021).

Menneskerettighedskomitéen, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 1988.
Tilgængelig her: https://www.refworld.org/docid/453883f922.html (sidst besøgt: 5/5 2021).

11. Skærmprint med antal anslag