Overførsel af personoplysninger til tredjelande efter Schrems II

Kandidatspeciale

Linda Vestergaard Jensen
Studienummer: 20166758

Mads Dyrting
Studienummer: 20165794

Sofie Dalsgaard Pedersen
Studienummer: 20166417

AALBORG UNIVERSITET

Titelblad

Titel:	Overførsel af personoplysninger til tredjelande efter Schrems II
Engelsk titel:	Transfer of Personal Data to Third Countries post-Schrems II
Forfattere:	Linda Vestergaard Jensen Mads Dyrting Sofie Dalsgaard Pedersen
Studieretning:	Jura
Fagområde:	Persondataret
Semester:	10. semester
Universitet:	Aalborg Universitet
Vejleder:	Line Bune Juhl
Ekstern samarbejdspartner:	Bech-Bruun advokatpartnerselskab
Dato for aflevering:	19. maj 2021

Abstract

Due to the progression in technology, crossborder data transfers have become increasingly important in most professions and contexts. The rules regarding data transfers are therefore essential to an expanding list of companies and authorities. The General Data Protection Regulation applies to the member states of the European Union and regulates the data protection within the Union. The complications arise when data is transferred to third countries outside the Union. The General Data Protection Regulation Chapter 5 states that such transfers must take place under an adequate level of protection.

In C-362/14, Schrems I and C-311/18, Schrems II it was questioned if the transfer of personal data to the United States of America on the basis of the adequacy decisions Safe Harbour and Privacy Shield fulfilled the requirements in the General Data Protection Regulation in conjunction with the Charter of Fundamental Rights of the European Union. Court of Justice of the European Union ruled Safe Harbour and Privacy Shield inadequate. In C-311/18, Schrems II it was further determined that the European Commission's standard contractual clauses were still valid in general as a basis of transfer to third countries. However, the Court additionally stated that due to the American law, which allowed for mass surveillance by the authorities, the standard contractual clauses did not provide appropriate safeguards without the implementation of supplementary measures.

The ruling has left data exporters in uncertainty regarding how to adjust to and comply with the requirements identified in C-362/14, Schrems I and C-311/18, Schrems II. The following thesis will examine which aspects the data exporter should consider and which supplementary measures to implement when transferring data to the United States of America, as well as other third countries in the absence of an adequacy decision. In this regard, it is examined whether the draft implementing decision on the new standard contractual clauses or the European Data Protection Board's Recommendations will provide clarification to this end.

It was concluded in C-362/14, Schrems I and C-311/18, Schrems II, that an adequate level of data protection must be ensured in order to transfer personal data to third countries. Thus, the protection

provided by the third country must be essentially equivalent to the level of data protection in the Union.

It is concluded that in order to determine whether an essentially equivalent level of data protection is achieved, the data exporter must assess the laws of the third country. The data exporter must assess both accessible and inaccessible foreign legislation, which will typically result in an extensive and costly assessment.

In case it is determined that the legislation in the third country together with the standard contractual clauses do not provide an essentially equivalent protection, the data exporter must implement supplementary measures to ensure this. In Recommendations 01/2020, the European Data Protection Board sets forth some examples of supplementary measures that can be implemented in different situations, e.g., pseudonymization or encryption. However, it is concluded in the thesis that the recommendations' limited number of generic examples do not offer sufficient guidance especially considering the specific circumstances of each transfer. In some specific circumstances it might not even be possible for the parties to implement effective supplementary measures, which can ensure an essentially equivalent level of protection.

While the draft implementing decision on the new standard contractual clauses elaborate the need of assessing the laws of the third country as well as the need to implement supplementary measures, it is concluded that it is not a definitive solution as the adoption of supplementary measures is still required.

Thus, the parties are in a challenging situation as they have to identify the effectiveness in the context of the transfer and in light of the third country law. Multiple data exporters will have to assess comparable circumstances and will be held accountable for their assessments. There will also be multiple supervisory authorities determining whether the data exporters are compliant. In conclusion, this structure of case-by-case assessments by both the data exporters and supervisory authorities might ultimately result in lack of uniformity throughout the Union.

Indholdsfortegnelse

1. Indledning **6**
1.1. Afgrænsning 8
1.2. Metode 10
2. Den Europæiske Unions charter om grundlæggende rettigheder **13**
2.1. Retten til privatliv 13
2.2. Ret til beskyttelse af personoplysninger 14
2.3. Ret til effektive retsmidler 16
2.4. Rækkevidde og fortolkning af rettigheder og principper 16
2.5. Overførsel af personoplysninger til tredjelande eller internationale organisationer 17
2.5.1. Overførsel 17
2.5.2. Personoplysning 18
2.5.2.1. Enhver information 19
2.5.2.2. Oplysning 'om' en person 19
2.5.2.3. Identificeret eller identificerbar person 19
2.5.2.4. Fysisk person 20
2.5.3. Tredjeland eller international organisation 20
2.6. Generelt princip for overførsler af personoplysninger 20
2.7. Overførsler på baggrund af en tilstrækkelighedsafgørelse 21
2.8. Overførsel på baggrund af SCC 23
3. C-362/14, Schrems I og C-311/18, Schrems II **25**
3.1. C-362/14, Schrems I 25
3.1.1. Tilsynsmyndighedens kompetence 26
3.1.2. Kompetencen til at erklære en tilstrækkelighedsafgørelse ugyldig 27
3.1.3. Gyldigheden af Safe Harbour 27
3.2. C-311/18, Schrems II 31
3.2.1. Betydning af overgang fra databeskyttelsesdirektivet til databeskyttelsesforordningen . 32
3.2.2. Vurdering af, hvorvidt overførslen var omfattet af EU-retten 33
3.2.3. Vurdering af, hvilket beskyttelsesniveau, der kræves ved overførsel efter SCC 34

3.2.4. Vurdering af, hvordan tilsynet skal forholde sig, når de vurderer, at en overførsel ikke overholder kravene 36
3.2.5. Vurdering af den generelle gyldighed af SCC i lyset af Charteret 37
3.2.6. Vurdering af, hvorvidt overførsler til USA krænkede rettighederne i Charteret 39
3.2.6.1. Vurdering af, hvorvidt overførsler til USA ved anvendelse af Privacy Shield krænkede rettighederne i Charteret 39
3.2.6.2. Vurdering af, hvorvidt overførsler til USA ved anvendelse af SCC krænkede rettighederne i Charteret 43
3.3. Sammenfatning af C-362/14, Schrems I og C-311/18, Schrems II 43
4. Supplerende foranstaltninger 47
4.1. 6-trins-vejledningen 47
4.1.1. Første og andet trin 47
4.1.2. Tredje trin 48
4.1.3. Fjerde trin 49
4.1.4. Femte og sjette trin 50
4.2. Tekniske foranstaltninger 50
4.2.1. Scenarier, hvor der kan konstateres effektive foranstaltninger 51
4.2.2. Scenarier, hvor der ikke kan konstateres effektive foranstaltninger 52
4.3. Yderligere kontraktmæssige foranstaltninger 53
4.4. Organisatoriske foranstaltninger 54
5. Udkast til nye SCC 56
5.1. Formålet og rækkevidden af SCC 57
5.2. Behandlingssikkerhed og supplerende foranstaltninger 58
5.2.1. De almindelige krav til behandlingssikkerhed 58
5.2.2. Tillæg med tekniske og organisatoriske foranstaltninger 60
5.3. Lovgivningen i tredjelandet 61
5.4. Myndighedsanmodninger 63
6. Cases 64
6.1. Case 1 64
6.1.1. Lovgivningen i USA 64
6.1.1.1. Særlig lovgivning ved en beskyttet modtager 66

6.1.2. Relevante supplerende foranstaltninger 67
6.1.2.1. Kryptering 67
6.1.2.2. Pseudonymisering 68
6.2. Case 2 70
6.2.1. Vurdering af tredjelandenes lovgivning 71
6.2.2. Pseudonymisering 71
6.2.3. Kryptering 73
6.2.4. Afskæring af underleverandører 74
6.3. Case 3 77
6.3.1. Det territoriale anvendelsesområde 77
6.3.2. Konsekvens af, at data adskilles 79
6.3.3. Konsekvens af risikoen for, at data sammenblandes 79
6.4. Sammenfatning af cases 81
7. Konklusion 84
Litteraturliste 88

1. Indledning

Som følge af den samfundsmæssige og teknologiske udvikling er anvendelse og overførsel af personoplysninger i stigende grad blevet en del af virksomheders og myndigheders hverdag. Dataoverførsler er essentielle for mange virksomheder og myndigheder, og er en stor del af den digitale, globale økonomi. Overførsler er nødvendige både inden for og ud af Den Europæiske Union.[1] Regulering af overførslerne ud af Unionen er derfor blevet tilsvarende central for at opretholde beskyttelsen af personoplysninger, og for at sikre at beskyttelsen i Unionen ikke bliver illusorisk.[2]

Beskyttelse af personoplysninger er en grundlæggende rettighed, som er sikret ved artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder[3] og artikel 16, stk. 1 i traktaten om Den Europæiske Unions funktionsmåde[4]. Behandling af sådanne oplysninger er reguleret ved databeskyttelsesforordningen[5] af 27. april 2016, der erstatter databeskyttelsesdirektivet[6] af 24. oktober 1995. Databeskyttelsesforordningens formål er at beskytte fysiske personers grundlæggende rettigheder i forbindelse med behandling af personoplysninger, samt sikre fri udveksling af personoplysninger i det indre marked.

Databeskyttelsesforordningen lægger i præambelbetragtning 6 vægt på, at teknologien bør fremme den frie udveksling af personoplysninger både inden for Unionen og i forbindelse med overførsel af personoplysninger til tredjelande og internationale organisationer. Databeskyttelsesforordningen fremhæver endvidere, at der er sket en stor stigning i omfanget af indsamling og deling af personoplysninger. Dermed har den teknologiske udvikling og globalisering udfordret den enkeltes rettigheder i forbindelse med behandling af dennes personoplysninger. Databeskyttelsesforordningen fastlægger

[1] Herefter 'Unionen'
[2] Blume, Peter, 2018, s. 176 f.
[3] Den Europæiske Unions charter om grundlæggende rettigheder, 2010/C 83/02, 30. marts 2010. Herefter 'Charteret'
[4] Traktaten om Den Europæiske Unions funktionsmåde af 1. december 2009. Herefter 'TEUF'
[5] 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). Herefter 'databeskyttelsesforordningen'
[6] Europa-Parlamentets og Rådets Direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. Herefter 'databeskyttelsesdirektivet'

derfor også i præambelbetragtning 7 vigtigheden af, at der er en stærk og sammenhængende ramme for databeskyttelse i Unionen.

Beskyttelsesniveauet, der er sikret som grundlæggende rettighed i Charterets artikel 8, samt den mere detaljerede beskyttelse i databeskyttelsesforordningen, bør ikke blive undermineret af, at personoplysninger overføres til lande uden for Unionen. Der er som følge heraf opstillet yderligere betingelser i databeskyttelsesforordningen kapitel 5, som skal overholdes ved overførsler til såkaldte tredjelande.

Østrigske Maximillian Schrems indgav den 25. juli 2013 en klage til det irske datatilsyn, hvor han anmodede tilsynet om at forbyde Facebook Irelands videregivelse af hans personoplysninger til Facebook Inc. i USA som følge af Edward Snowdens afsløringer om de amerikanske efterretningstjenesters masseovervågning. Schrems mente ikke, at Facebook Irelands daværende overførselsgrundlag til Facebook Inc., tilstrækkelighedsafgørelsen Safe Harbour, beskyttede hans personoplysninger tilstrækkeligt. Efter Schrems' klage blev afvist af det irske datatilsyn, anlagde han sag ved High Court, som er øverste retsinstans i Irland. Dette bevirkede, at High Court forelagde Den Europæiske Unions Domstol[7] præjudicielle spørgsmål angående gyldigheden af Safe Harbour. Overførselsgrundlaget erklærede Domstolen ugyldigt den 6. oktober 2015 i dommen C-362/14, Schrems I.

Schrems omformulerede efter dommen af 6. oktober 2015 sin klage. Herefter anførte han, at de oplysninger, som blev anvendt i forbindelse med de forskellige overvågningsprogrammer i USA, var uforenelige med Charterets artikel 7, 8 og 47. Facebook Ireland overførte efter C-362/14, Schrems I oplysninger til Facebook Inc. i USA på grundlag af Kommissionens standardkontraktbestemmelser[8], som er et kontraktretligt overførselsgrundlag efter databeskyttelsesforordningen artikel 46, stk. 2, litra c. Schrems anførte, at SCC heller ikke kunne begrunde overførslen til USA. Schrems anmodede på den baggrund endnu en gang det irske datatilsyn om at forbyde eller suspendere overførslen af hans personoplysninger til Facebook Inc. i USA.[9] Domstolen afsagde den 16. juli 2020 dom i C-311/18, Schrems II, hvorefter Domstolen blandt andet fandt, at overførsel af personoplysninger til USA på baggrund af SCC ikke alene kunne sikre et tilstrækkeligt beskyttelsesniveau på grund af lovgivningen

[7] Herefter 'Domstolen'
[8] Herefter 'SCC'
[9] C-311/18, Schrems II, præmis 77

i USA. Domstolen erklærede dog, at SCC fortsat generelt er gyldige som overførselsgrundlag. Derudover tog Domstolen også stilling til den nye tilstrækkelighedsafgørelse Privacy Shield, som den erklærede ugyldig.

C-311/18, Schrems II har efterladt en række spørgsmål vedrørende grundlaget for overførsler til såkaldte usikre tredjelande, der er en betegnelse for tredjelande, hvorom der ikke er truffet en tilstrækkelighedsafgørelse. Der er som følge af dommen en række usikkerheder, herunder hvilke forhold virksomheder skal overveje, samt hvilke foranstaltninger virksomheder skal foretage for at gennemføre overførsler til usikre tredjelande. Kommissionen har desuden fremsat forslag til nye SCC, som også har frembragt usikkerhed om, hvilken betydning dette vil have for virksomheder og myndigheder, der benytter SCC som overførselsgrundlag.

Specialets formål er derfor at undersøge, hvordan virksomheder og myndigheder, som skal overføre personoplysninger til usikre tredjelande, herunder USA, bedst muligt indretter sig på den nye virkelighed efter C-311/18, Schrems II. Specialet vil blandt andet inddrage de henstillinger, som Det Europæiske Databeskyttelsesråd[10] har udarbejdet om supplerende foranstaltninger og væsentlige garantier samt udkastet til nye SCC.

1.1. Afgrænsning

Specialets primære fokusområde er de krav som databeskyttelsesforordningen opstiller til overførsler af personoplysninger til modtagere uden for Unionen. Charteret og anden EU-ret vil inddrages i det omfang, dette er relevant for at beskrive og analysere beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandlingsaktiviteter.

Databeskyttelsesforordningens formål er at harmonisere beskyttelsen af disse rettigheder i Unionen. Forordningens kapitel 5, der regulerer overførsler af personoplysninger til tredjelande eller internationale organisationer, opstiller således supplerende betingelser til de sædvanlige krav, der er til databehandlinger med henblik på at sikre forordningens formål. Kapitel 5 opstiller en udtømmende og

[10] Herefter 'Databeskyttelsesrådet'

prioriteret liste over behandlingsgrundlag, som gør det muligt at overføre personoplysninger til modtagere uden for Unionen.

Af hensyn til specialets omfang vil specialet være afgrænset til de dele af kapitel 5, som bliver behandlet i C-362/14, Schrems I og C-311/18, Schrems II. Specialet vil være afgrænset til at beskæftige sig med artikel 44, der regulerer det generelle princip for overførsler, artikel 45, der regulerer overførsler baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, samt artikel 46, der regulerer overførsler omfattet af fornødne garantier. Af de fornødne garantier oplistet i artikel 46, stk. 2, vil specialet alene beskæftige sig med litra c omhandlende SCC vedtaget af Kommissionen.

Specialet vil dermed ikke beskæftige sig med den resterende del af databeskyttelsesforordningens artikel 46, herunder overførsel ved hjælp af bindende virksomhedsregler specificeret i artikel 47, eller artikel 48, der regulerer muligheden for at tillade overførsler af personoplysninger til modtagere uden for Unionen i medfør af en udenlandsk dom eller afgørelse. Specialet vil desuden ikke beskæftige sig med databeskyttelsesforordningens artikel 49, der regulerer muligheden for at tillade overførsler af personoplysninger til modtagere uden for Unionen i særlige situationer. Af hensyn til specialets omfang vil der ydermere ikke foretages en nærmere analyse og beskrivelse af de øvrige bestemmelser i forordningen, herunder eksempelvis de databeskyttelsesretlige principper i artikel 5.

I forbindelse med C-362/14, Schrems I og C-311/18, Schrems II blev en ny retstilstand skabt, idet tilstrækkelighedsafgørelserne vedrørende USA blev underkendt. Ligeledes beskriver begge domme nærmere, hvilke krav der fremadrettet bør være til overførsler til modtagere uden for Unionen. Specialet vil udelukkende foretage en dybdegående beskrivelse og analyse af disse to domme.

Idet specialets fokus er databeskyttelsesforordningens regler om overførsler af personoplysninger til lande uden for Unionen, berøres databeskyttelsesreguleringen i de enkelte medlemslande ikke. Specialet vil desuden ikke inddrage lovgivning fra andre tredjelande. Det vil dog være relevant for beskrivelsen og analysen af både Safe Harbour og Privacy Shield at inddrage amerikansk lovgivning i begrænset omfang. Specialet vil dog ikke lave en dybdegående gennemgang af den relevante amerikanske lovgivning.

1.2. Metode

For at belyse problemstillingen vedrørende overførsel af personoplysninger til usikre tredjelande set i lyset af C-311/18, Schrems II anvendes den retsdogmatiske metode. Ved anvendelse af den retsdogmatiske metode beskrives, systematiseres og analyseres gældende ret. Den retsdogmatiske metode har således til formål at belyse retstilstanden på et givent område.[11]

Traditionelt opdeles dansk ret i fire retskildegrupper, som består af henholdsvis loven, retspraksis, sædvaner og forholdets natur. Der findes ingen retsregler for, hvilke retskilder der har forrang, men det antages dog i uskrevne prioriteringsprincipper, at lovgivningen har forrang i forhold til de øvrige retskildegrupper, idet lovgivningen er demokratisk legitimeret.[12] Specialet inddrager alene retskildegrupperne loven og retspraksis, da disse retskildegrupper er de relevante i forhold til undersøgelse af overførsler af personoplysninger til usikre tredjelande.

Specialet vil anvende lovgivning både fra Danmark og Den Europæiske Union. Lovgivning fra Unionen finder direkte anvendelse i Danmark, idet der er tale om supranational retsdannelse. Dette skyldes, at Danmark har overgivet en del af landets suverænitet til Unionens institutioner i Grundlovens § 20, stk. 1.[13] EU-retten har forrang frem for national ret, hvilket første gang blev fastslået i Domstolens afgørelse i Sag 6/64, Costa mod ENEL. Retspraksis fra danske domstole vil ikke inddrages, idet der ikke foreligger relevante offentliggjorte afgørelser vedrørende emnet ved de danske domstole.

Retskilderne i EU-retten består af primær EU-ret, sekundær EU-ret samt domspraksis. Traktater er den primære retskilde. En traktat er en juridisk bindende aftale mellem to eller flere stater.[14] I specialet anvendes traktaten om Den Europæiske Union[15] og traktaten om Den Europæiske Unions funktionsmåde. Ligeledes anvendes Charteret, som har samme juridiske værdi som traktaterne, jf. TEU artikel 6, stk. 1, 1. pkt.

[11] Munk-Hansen, Carsten, 2018, s. 204 f.
[12] Evald, Jens, 2019, s. 19
[13] Munk-Hansen, Carsten, 2018, s. 276
[14] Evald, Jens, 2019, s. 66
[15] Traktaten om Den Europæiske Union af 7. februar 1992. Herefter 'TEU'

De øvrige sekundære retskilder har ikke et internt hierarki, men den sekundære EU-ret må naturligt ikke stride imod den primære EU-ret. Den sekundære EU-ret består overvejende af forordninger, direktiver, beslutninger og henstillinger.[16]

I dette speciale anvendes databeskyttelsesforordningen. Forordninger er bindende og gælder umiddelbart i hver medlemsstat. Databeskyttelsesforordningen efterlader et nationalt råderum for medlemsstaterne til at lave nærmere regulering på nærmere angivne områder. Danmark har af den årsag udstedt databeskyttelsesloven, som har til hensigt at supplere og gennemføre databeskyttelsesforordningen, jf. databeskyttelseslovens § 1. Databeskyttelsesforordningen efterlader dog ikke et nationalt råderum i forordningens kapitel 5, der regulerer overførsler af personoplysninger til tredjelande.

Databeskyttelsesforordningen trådte i kraft den 25. maj 2018, og erstattede det tidligere databeskyttelsesdirektiv. I forbindelse med behandlingen af både C-362/14, Schrems I og C-311/18, Schrems II blev databeskyttelsesdirektivets bestemmelser anvendt. Et direktiv er kun bindende for medlemsstater med hensyn til det tilsigtede mål. Ved et direktiv er det derfor overladt til de enkelte nationale myndigheder at bestemme formen og midlerne for gennemførelsen af direktivet.[17] Ved overgangen fra databeskyttelsesdirektivet til databeskyttelsesforordningen er der sket en større harmonisering af databeskyttelsesreguleringen i Unionen, idet forordningen, modsat direktivet, som beskrevet ovenfor, gælder umiddelbart i hver medlemsstat uden implementering.

Specialet vil inddrage beslutninger fra Kommissionen. Beslutninger er retsakter, der retter sig mod personer, virksomheder eller medlemslande, og er bindende for adressaten.[18] Specialet anvender ligeledes henstillinger fra Unionens institutioner, herunder Databeskyttelsesrådet. Databeskyttelsesrådet har til formål at sikre ensartet anvendelse af databeskyttelsesforordningen ved at føre tilsyn, rådgive og udstede retningslinjer, henstillinger og bedste praksis, jf. databeskyttelsesforordningens artikel 70. De udstedte retningslinjer, henstillinger og bedste praksis giver ikke rettigheder og pligter for modtageren. Disse tjener dog som vejledning til fortolkningen af databeskyttelsesforordningen.[19]

[16] Evald, Jens, 2019, s. 67
[17] Evald, Jens, 2019, s. 66
[18] Munk-Hansen, Carsten, 2018, s. 277
[19] Europa-Parlamentet, Faktabladet om Den Europæiske Union: EU-retten - kilder og rækkevidde

Domstolen har ved domsafsigelser en retsskabende rolle ved fortolkning og udfyldelse af traktatens bestemmelser. Domspraksis har præjudikatsværdi, idet Domstolen ofte lægger vægt på sine tidligere afgørelser og præmisser som grundlag for nyere domme, dog uden at anse tidligere domme som bindende præjudikater for den selv.[20] Domstolens praksis bidrager således til at præcisere virkningerne af EU-retten, men har som udgangspunkt kun bindende virkning for de parter, som sagen angår.[21] Domstolenes praksis fastslår dog samtidig en række retsgrundsætninger og grundrettigheder, som agerer som en målestok for den EU-retlige lovgivnings gyldighed. Retsgrundsætningerne og grundrettighederne sætter ikke kun rammer for EU-institutionerne, men skal også iagttages af de nationale myndigheder, herunder de nationale domstole.[22] Flere af de EU-retlige grundsætninger kan påberåbes direkte, men det har været mere tvivlsomt, hvorvidt disse principper ligeledes kan påberåbes horisontalt, altså direkte over for private. Dette ses at være accepteret af Domstolen i visse tilfælde.[23] C-362/14, Schrems I og C-311/18, Schrems II tillægges stor vægt i analysen af, hvordan virksomheder og myndigheder, der skal overføre personoplysninger til usikre tredjelande, skal forholde sig. Domstolen fastlagde i C-362/14, Schrems I og C-311/18, Schrems II, hvilke krav der bør opfyldes i forbindelse med overførsler af personoplysninger til tredjelande.

Der anvendes endvidere juridisk litteratur. Juridisk litteratur er ikke at betegne som en retskilde, idet forfatteren ikke er legitimeret til at fastlægge ret. Retslitteratur er i midlertidig relevant at inddrage for at underbygge forståelsen af retstilstanden.[24]

I specialet inddrages afslutningsvist tre cases udarbejdet af Bech-Bruun advokatpartnerselskab, der er inspireret af virkelige problemstillinger, som klienter har søgt rådgivning om. Cases er velegnede til at illustrere konkrete problemstillinger, og kan anvendes til at udarbejde forslag til, hvordan problemstillingerne kan løses i praksis efter C-311/18, Schrems II. Disse cases kan dermed medvirke til at forstå gældende ret.

[20] Neergaard, Ulla, m.fl., 2020, s. 154
[21] Evald, Jens, 2019 s. 66 f.
[22] Neergaard, Ulla, m.fl., 2020, s. 155
[23] Neergaard, Ulla, m.fl., 2020, s. 213 ff.
[24] Munk-Hansen, Carsten, 2018, s. 372 ff.

2. Den Europæiske Unions charter om grundlæggende rettigheder

Charteret fastsætter omfattende rettigheder for retssubjekter i Unionen. Charteret er til dels en kodifikation af konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder[25] og Domstolens hidtidige praksis, men rettighederne går også videre end disse.[26] EMRK ikke er direkte anvendelig, idet Unionen ikke har tiltrådt konventionen.[27] Det fremgår af TEU artikel 6, stk. 1, at Unionen anerkender de rettigheder, friheder og principper, der fremgår af Charteret, og at dette har samme juridiske værdi som traktaterne. Charteret blev således juridisk bindende for medlemsstaterne ved indførelse i TEU.

Charteret angiver i artikel 52, stk. 3, at i det omfang Charteret indeholder rettigheder svarende til dem, der er sikret ved EMRK, har beskyttelsen som minimum samme omfang, men er ikke begrænset til den beskyttelse, som er sikret i EMRK. EMRK samt tilhørende retspraksis kan som følge heraf bidrage som fortolkningsgrundlag for den mindstebeskyttelse, retssubjekter er tildelt ved Charteret. Domstolen og EMRK henviser ligeledes til hinandens retspraksis, og der sker dermed en indbyrdes påvirkning.[28]

2.1. Retten til privatliv

Af Charterets artikel 7 fremgår det, at enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation. Charterets artikel 7 har samme betydning og omfang som EMRK artikel 8, jf. artikel 52, stk. 3. EMRK artikel 8 og Charterets artikel 7 supplerer Grundlovens § 72 i forhold til retten til privatliv, familieliv, sit hjem og sin kommunikation. Denne rettighed er bredt formuleret, hvilket gør det muligt at udvikle beskyttelsen af individets privatsfære i retspraksis i takt med samfundsudviklingen, særligt henset til den teknologiske udvikling og samfundets normer.[29]

[25] Konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder af 4. november 1950. Danmark ratificerede denne ved BKI nr. 20 af 11/06/1953. Herefter 'EMRK'
[26] Neergaard, Ulla, m.fl., 2020, s. 162
[27] Europa-Parlamentet, Faktabladet om Den Europæiske Union: Beskyttelse af de grundlæggende rettigheder i EU
[28] Neergaard, Ulla, m.fl., 2020, s. 173 f.
[29] Rytter, Jens Elo, 2019, s. 214

Beskyttelsen retter sig primært mod offentlige myndigheders indgreb, jf. EMRK artikel 8, stk. 2, men indebærer også en forpligtigelse for staten til at beskytte individet mod indgreb fra private.[30] Charterets artikel 7 og EMRK artikel 8 er derfor at betegne som en slags opsamlingsbestemmelser, som individet kan påberåbe sig, hvis ikke andre mere specielle rettigheder dækker området.[31]

Offentlige myndigheders indgreb i privat- og familieliv skal opfylde kravene i EMRK artikel 8, stk. 2. Ved myndigheders indgreb i privat- og familieliv skal det derfor altid overvejes, om indgrebet har hjemmel, om indgrebet forfølger en af de anerkendelsesværdige formål opremset i artikel 8, stk. 2 og om indgrebet er nødvendigt i et demokratisk samfund.

Personoplysninger er omfattet af retten til privatliv, idet personoplysninger kan anvendes, samkøres og udbredes på måder, der kan krænke individets privatliv. Offentlige myndigheders indhentning og opbevaring af personoplysninger udgør dermed et indgreb efter EMRK artikel 8 og Charterets artikel 7.[32]

2.2. Ret til beskyttelse af personoplysninger

I Charterets artikel 8 anføres det, at enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende. Oplysningerne skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørtes samtykke eller på et andet berettiget ved lov fastsat grundlag. Bestemmelsen anfører endvidere, at overholdelsen af disse regler skal være underlagt en uafhængig myndighedskontrol.

Charterets artikel 8 definerer ikke nærmere, hvordan 'behandling' skal fortolkes. Domstolen henviser dog til, at dette begreb skal fortolkes i overensstemmelse med definitionen i databeskyttelsesforordningens artikel 4, stk. 2, ligesom det er tilfældet med definitionen af 'personoplysninger'.[33] Charterets artikel 8 er formuleret adskillige år efter databeskyttelsesdirektivet, og skal forstås som en kodificering af allerede gældende databeskyttelsesret, således dette også fremgik af primær EU-ret.[34]

[30] Storgaard, Louise Halleskov, 2019, s. 324 f.
[31] Rytter, Jens Elo, 2019, s. 214 f.
[32] Rytter, Jens Elo, 2019, s. 223
[33] C-291/12, Schwarz præmis 28 og Storgaard, Louise Halleskov m.fl. 2019, s. 333
[34] Handbook on European data protection law, 2018, s. 28

Charterets artikel 8 er baseret på traktaten om oprettelse af Det Europæiske Fællesskab[35] artikel 286, som nu er erstattet af TEUF artikel 16 samt i TEU artikel 39. Artikel 8 er endvidere baseret på Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger[36] og databeskyttelsesdirektivet, som nu er ophævet og erstattet af databeskyttelsesforordningen.[37]

Afslutningsvist er Charterets artikel 8 desuden baseret delvist på EMRK artikel 8, men Charterets artikel 8 og EMRK artikel 8 er ikke tilsvarende hinanden i betydning og omfang.[38] Dette skyldes, at formålet med Charterets artikel 7 og EMRK artikel 8 er at beskytte individets privatsfære, hvor beskyttelsen af personoplysninger er udskilt til særskilt beskyttelse i Charterets artikel 8. Beskyttelsen af personoplysninger er omvendt ikke udskilt til særlig beskyttelse i EMRK.[39]

Til trods for at Charterets artikel 7 og 8 hjemler to særskilte rettigheder, er det i langt de fleste tilfælde nødvendigt at behandle sager vedrørende beskyttelse af personoplysninger med hensyntagen til begge rettigheder set i lyset af hinanden.[40] I sagen C-293/12, Digital Rights Ireland, præmis 53 fremhævede Domstolen, at beskyttelsen af personoplysninger i medfør af Charterets artikel 8 har en særlig betydning for retten til respekt for privatlivet, som er fastslået i artikel 7, ligesom Domstolen i C-468/10, ASNEF udtalte, at Charterets artikel 7 og 8 er nært beslægtet.[41]

Hverken Charterets artikel 7 eller 8 er absolutte rettigheder, og de skal derfor ses i sammenhæng med de generelle principper for begrænsninger af rettighederne, som er indeholdt i Charterets artikel 52, stk. 1, der vil gennemgås nærmere i afsnit 2.4. Charterets artikel 7, 8 og 52 skal tilsvarende indgå i vurderingen, når betingelserne og reglerne i en sekundær EU-retsakt skal vurderes, herunder eksempelvis databeskyttelsesforordningen, så reglerne sammenlagt vurderes i lyset af hinanden.[42]

---

[35] Traktaten om oprettelse af Det Europæiske Fællesskab af 25. marts 1957
[36] Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger af 28. januar 1981. Danmark ratificerede denne ved BKI nr. 59 af 16/05/1991
[37] Neergaard, Ulla, m.fl., 2020, s. 177
[38] De forenede sager C-203/15, Tele2 Sverige og C-698/15, Watson m.fl., præmis 129
[39] Rytter, Jens Elo, 2019, s. 210
[40] Storgaard, Louise Halleskov m.fl., 2019, s. 332 f.
[41] C-468/10, ASNEF, præmis 41
[42] De forenede sager C-92/09 og C-93/09 Volker og Markus Schecke og Eifert, præmis 48-52

2.3. Ret til effektive retsmidler

Adgangen til effektive retsmidler ved krænkelser af individets grundlæggende rettigheder er essentiel for beskyttelsen af netop disse rettigheder, idet beskyttelsen ellers ville blive illusorisk.[43]

Det fremgår af Charterets artikel 47, 1. pkt., at enhver, der har fået krænket sine rettigheder og friheder, som er sikret af EU-retten, skal have adgang til domstolsprøvelse under overholdelse af de betingelser, der er fastsat i artiklen. Bestemmelsen svarer i det væsentligste til EMRK artikel 13, der sikrer adgang til effektive retsmidler for borgere omfattet af denne konvention.

Charterets artikel 47, 2. og 3. pkt. tildeler ligeledes enhver ret til retfærdig og offentlig rettergang inden en rimelig frist for en uafhængig og upartisk domstol, mens enhver ligeledes har ret til rådgivning, forsvar og repræsentation. Kravet om en uafhængig domstol retter sig særligt mod domstolens uafhængighed af den udøvende og lovgivende magt. Her skal særligt lægges vægt på dommerens udnævnelse og dennes varighed, samt garantier mod indblanding.[44] Kravet om en upartisk domstol retter sig særligt mod den enkelte dommers personlige forhold. Dommeren skal fremtræde neutral, og må ikke på grund af relationer, sympatier eller andet være forudindtaget, således uvedkommende hensyn får betydning ved domsafsigelse.[45]

2.4. Rækkevidde og fortolkning af rettigheder og principper

Charterets artikel 52 regulerer rækkevidden af Charterets rettigheder og principper. Charterets artikel 52, stk. 1 indeholder en generel undtagelsesbestemmelse, hvor det fremgår ud fra hvilke betingelser, det er legitimeret, at EU-institutioner og medlemsstater kan foretage begrænsninger og indgreb i de rettigheder og friheder, der er sikret i Charteret. I Charterets artikel 52, stk. 1 fastslås det, at såfremt Charterets rettigheder og friheder skal begrænses, er det en betingelse, at indgrebet skal være fastsat i lovgivningen. Det er yderligere en betingelse, at indgrebet respekterer det væsentligste indhold af rettigheden og friheden. Dette hænger sammen med, at såfremt et indgreb er så omfattende og indgribende, at det udhuler selve indholdet af en rettighed eller en frihed, så må indgrebet allerede af den

[43] Rytter, Jens Elo, 2019, s. 470
[44] Rytter, Jens Elo, 2019, s. 477 ff.
[45] Rytter, Jens Elo, 2019, s. 482 f.

grund ikke kunne retfærdiggøres. Det er ligeledes en betingelse for at legitimere indgreb i de sikrede rettigheder og friheder, at indgrebet er nødvendigt og forfølger et mål af almen interesse, der er anerkendt af Unionen, eller at der er behov for beskyttelse af andres rettigheder og friheder. Det er i denne henseende en betingelse, at indgrebet er proportionelt.[46]

I Charterets artikel 52, stk. 2 fremgår det, at de rettigheder, som er anerkendt i Charteret, og som er fastlagt i en traktat, udøves på de samme betingelser og med samme begrænsninger, som er fastlagt i traktaten.

Charterets artikel 52, stk. 3 sikrer, som tidligere beskrevet, sammenhængen mellem Charteret og EMRK, idet denne bestemmelse fastslår, at i det omfang Charteret indeholder rettigheder svarende til dem, der er sikret ved EMRK, er deres betydning og rækkevidde de samme som i EMRK. Det fremgår desuden af sidste punktum i bestemmelsen, at Unionen har mulighed for at sikre en mere omfattende beskyttelse. Beskyttelsen i Charteret kan således aldrig være mindre end den, der er sikret i EMRK, men der er således intet til hinder for, at Charteret sikrer et højere beskyttelsesniveau end EMRK.[47]

2.5. Overførsel af personoplysninger til tredjelande eller internationale organisationer

Kapitel 5 regulerer reglerne om overførsel af personoplysninger til tredjelande eller internationale organisationer. Det er derfor i det kommende defineret, hvad der forstås ved 'overførsel', 'personoplysning', 'tredjelande' og 'internationale organisationer'.

2.5.1. Overførsel

Begrebet 'overførsel' er ikke nærmere defineret i databeskyttelsesforordningens legaldefinitioner i artikel 4. Fastlæggelse af begrebet 'overførsel' er essentiel for at fastslå, om anvendelsen af personoplysningerne skal iagttage de supplerende krav i databeskyttelsesforordningens kapitel 5.

[46] Storgaard, Louise Halleskov m.fl. 2019, s. 237 ff.
[47] Forklaringer til (*) chartret om grundlæggende rettigheder (2007/c 303/02).

Begrebet 'overførsel' dækker over den situation, hvor personoplysninger i Unionen 'videregives' til en dataansvarlig uden for Unionen, som dermed behandler personoplysningerne efter eget formål og efter eget behandlingsgrundlag.[48]

Begrebet 'overførsel' dækker desuden over den situation, hvor en dataansvarlig eller databehandler i Unionen 'overlader' personoplysninger til en databehandler uden for Unionen. En overladelse sker i den situation, hvor der foreligger en databehandlerkonstruktion, og hvor databehandleren derfor handler på den dataansvarliges vegne. Databehandleren skal dermed ikke have særskilt behandlingsgrundlag for at behandle personoplysningerne. I forbindelse med intern anvendelse i en koncern, vil der således også være tale om en 'overladelse' af personoplysninger.[49]

I forlængelse af begrebet 'overladelse' tog Datatilsynets i sag DT j.nr. 2007-214-0004 stilling til, hvorvidt en se-adgang var at betragte som en overførsel. I sagen ønskede ATP at overføre oplysninger om sine medlemmer til databehandlere i Indien og Sydafrika, idet der var betydelige besparelser for ATP ved at anvende databehandlere i tredjelande. ATP udtalte, at databehandlerne ville have begrænset adgang, således databehandlerne udelukkende ville kunne se de oplysninger, der på det givne tidspunkt befandt sig på databehandlerens skærm. Datatilsynet anførte i sagens punkt 3.1., at ATP ved en se-adgang stadig efter tilsynets opfattelse 'overførte' personoplysninger til et tredjeland, selvom den pågældende databehandler udelukkende kunne se oplysningerne. Afgørelsen relaterer sig til den dagældende persondatalov og databeskyttelsesdirektiv, men det må antages, at afgørelsen stadig kan anvendes som fortolkningsbidrag til forståelsen af begrebet 'overførsel'.[50]

2.5.2. Personoplysning

Definitionen på begrebet 'personoplysning' findes i databeskyttelsesforordningens artikel 4, nr. 1 og defineres som "*enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«)*". Definitionen rummer dermed fire kumulative kriterier, der skal være opfyldt,

[48] Betænkning nr. 1565/2017, bind 2, s. 630 ff.
[49] Betænkning nr. 1565/2017, bind 2, s. 630 ff.
[50] Betænkning nr. 1565/2017, bind 2, s. 632 f.

før der er tale om en personoplysning: 1) Det er enhver information, 2) det skal være oplysninger om en person, 3) personen skal være identificeret eller identificerbar og 4) det skal være en fysisk person.

2.5.2.1. Enhver information

Som det fremgår ovenfor, er det enhver form for information, der er omfattet. Dette hænger sammen med, at informationen ikke behøver at være skriftlig, førend denne er at betegne som en personoplysning. Informationen kan også bestå i genetiske data som DNA og blod.[51]

2.5.2.2. Oplysning 'om' en person

Det fremgår desuden, at det er en betingelse, at det er oplysningerne 'om' en person. Oplysninger om genstande og dyr er således ikke omfattet af databeskyttelsesforordningens område. For at undersøge, hvorvidt en oplysning er 'om' en person, må den dataansvarliges behandlingsgrundlag være udslagsgivende. Dette bevirker, at selvom en oplysning er om en genstand, så er dette alligevel at betegne som en oplysning 'om' en person, såfremt disse oplysninger om genstanden bruges til at behandle eller vurdere ejeren af genstanden.[52]

2.5.2.3. Identificeret eller identificerbar person

Det fremgår af databeskyttelsesforordningens præambelbetragtning 26, hvad der skal tages i betragtning, når det skal vurderes, hvorvidt en fysisk person er identificerbar. Herunder bør alle midler, der med rimelighed kan tænkes bragt i anvendelse til direkte eller indirekte at identificere eller udpege den pågældende, tages i betragtning. Dette gælder både de midler, som den dataansvarlige selv eller en hvilken som helst anden person kunne tænkes at bringe i anvendelse. Det fremgår endvidere af databeskyttelsesforordningens præambelbetragtning 26, at førend det kan fastslås, hvorvidt midlet 'med rimelighed' kan tænkes bragt i anvendelse, bør omkostninger og tid ved identifikationen tages i betragtning. I databeskyttelsesforordningens artikel 4, nr. 1, opremses en ikke-udtømmende liste over sådanne identifikatorer, for eksempel navn og identifikationsnummer. Det følger afslutningsvist af databeskyttelsesforordningens præambelbetragtning 26, at databeskyttelsesprincipperne ikke bør

[51] Databeskyttelsesforordningens præambelbetragtning 34
[52] Article 29 Data Protection Working Party Opinion 4/2007 on the concept of personal data. Vedtaget den 20. juni 2007, s. 9

gælde for personoplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke eller ikke længere kan identificeres.

2.5.2.4. Fysisk person

Den fjerde betingelse, der skal være opfyldt, førend der er tale om en personoplysning er, at det skal dreje sig om en fysisk person. Det er således en betingelse, at oplysningerne relaterer sig til en levende person eller en personligt drevet virksomhed.

2.5.3. Tredjeland eller international organisation

Et tredjeland er ikke defineret i databeskyttelsesforordningen eller databeskyttelsesloven, men var dog defineret i den dagældende persondatalovs § 3, nr. 9, hvorefter et tredjeland er at betegne som alle andre lande end EU-lande og EØS-lande. En international organisation er omvendt defineret i databeskyttelsesforordningens artikel 4, nr. 26, hvoraf det fremgår, at en international organisation forstås som en folkeretlig organisation og dens underordnede organer, samt ethvert andet organ, der er oprettet ved eller med hjemmel i en aftale mellem to eller flere lande.

2.6. Generelt princip for overførsler af personoplysninger

Databeskyttelsesforordningens artikel 44 fastsætter det generelle princip for overførsler af personoplysninger til tredjelande eller internationale organisationer, hvoraf det fremgår, at reglerne i kapitel 5 er tillægskrav til de sædvanlige krav, som gælder til databehandlinger. Databeskyttelsesforordningen fastslår dermed, at alle overførsler af personoplysninger til tredjelande og internationale organisationer, skal opfylde betingelserne i databeskyttelsesforordningens kapitel 5, samt de øvrige bestemmelser indeholdt i forordningen. Det fremgår af databeskyttelsesforordningens præambelbetragtning 101, at strømmen af personoplysninger til og fra lande uden for Unionen eller internationale organisationer er nødvendig af hensyn til udbygningen af den internationale samhandel og det internationale samarbejde. Af databeskyttelsesforordningens artikel 44, 2. pkt. fremgår det, at bestemmelserne i forordningens kapitel 5 skal iagttages for at sikre, at det beskyttelsesniveau, som fysiske personer sikres i Unionen i medfør af denne forordning, ikke undermineres ved de nødvendige overførsler til og fra lande uden for Unionen.

Det fremgår af databeskyttelsesforordningens artikel 44, at overførslen skal underkastes behandling eller planlægges at blive behandlet for at være omfattet af forordningens kapitel 5. Det fremgår dermed, at det er en betingelse, at der befinder sig en modtager i tredjelandet, førend overførslen anses som værende omfattet af forordningens artikel 44.[53]

Det fastsættes ydermere i databeskyttelsesforordningens artikel 44, at det generelle princip for overførsler af personoplysninger til tredjelande eller internationale organisationer også gælder ved videreoverførsler. Det betyder dermed, at hvis modtageren i tredjelandet eller den internationale organisation videreoverfører de modtagne personoplysninger til dataansvarlige eller databehandlere i det samme eller et andet tredjeland eller en anden international organisation, skal databeskyttelsesforordningen samt de supplerende krav i kapitel 5 også ved videreoverførslen iagttages. Dette hænger sammen med, at hvis ikke videreoverførsler var underlagt samme skærpede krav som den primære overførsel til tredjelandet eller den internationale organisation, ville beskyttelsesniveauet sikret i Unionen blive undermineret.[54]

2.7. Overførsler på baggrund af en tilstrækkelighedsafgørelse

Databeskyttelsesforordningens artikel 45-49 opstiller en udtømmende og prioriteret liste af overførselsgrundlag.[55] Det følger af databeskyttelsesforordningens artikel 45, stk. 1, at overførsel af personoplysninger til et tredjeland eller en international organisation kan finde sted, hvis Kommissionen har fastslået, at tredjelandet, et område, sektorer i dette land eller denne organisation har et tilstrækkeligt beskyttelsesniveau. Når en dataansvarlig eller en databehandler overfører personoplysninger hertil på baggrund af en tilstrækkelighedsafgørelse efter databeskyttelsesforordningens artikel 45, stk. 1, kræves der ikke forinden en specifik godkendelse fra tilsynsmyndigheden.

Det fremgår af præambelbetragtning 104, at et passende beskyttelsesniveau i det væsentligste svarer til det, der er sikret i Unionen. Når Kommissionen skal vurdere om beskyttelsesniveauet er tilstrækkeligt, tager Kommissionen elementerne i databeskyttelsesforordningens artikel 45, stk. 2, litra a-c i

[53] Nielsen, Anders Korfits m.fl., s. 778
[54] Databeskyttelsesforordningens præambelbetragtning 101
[55] Nielsen, Anders Korfits m.fl., s. 774

betragtning. Kommissionen skal i vurderingen tage hensyn til retsstatsprincippet, respekten for grundlæggende frihedsrettigheder, relevant lovgivning i tredjelandet, herunder lovgivning om statens sikkerhed, databeskyttelse, myndigheders adgang til personoplysninger, sikkerhedsforanstaltninger, og den retspraksis, der følger heraf, samt de effektive retsmidler, der sikrer håndhævelse af disse rettigheder. Kommissionen skal desuden tage hensyn til tilstedeværelsen af velfungerende, uafhængige tilsynsmyndigheder i tredjelandet, eller tilsynsmyndigheder som den internationale organisation er underlagt. Disse uafhængige tilsynsmyndigheder skal have tilstrækkelige håndhævelsesbeføjelser til at sikre reglernes overholdelse ved at bistå og rådgive registrerede, der udøver deres rettigheder. Slutteligt skal Kommissionen tage hensyn til de internationale forpligtelser, der påhviler tredjelandet eller den internationale organisation. Det følger af endvidere databeskyttelsesforordningens præambelbetragtning 104, at tredjelandet bør give garantier om ovenstående.

Findes beskyttelsesniveauet i tredjelandet eller den internationale organisation tilstrækkeligt, kan Kommissionen som følge af databeskyttelsesforordningens artikel 45, stk. 3 ved en gennemførselsretsakt fastslå, at tredjelandet, et område, sektorer i landet eller den internationale organisation sikrer et tilstrækkeligt beskyttelsesniveau. Denne afgørelse skal revideres mindst hvert fjerde år, og skal inddrage relevant udvikling i tredjelandet eller den internationale organisation, jf. databeskyttelsesforordnings artikel 45, stk. 3 og 4.

Kommissionen kan efter databeskyttelsesforordningens artikel 45, stk. 5 ophæve, ændre eller suspendere disse gennemførelsesretsakter i det omfang, det findes nødvendigt, hvis tilgængelige oplysninger viser, at tredjelandet eller den internationale organisation ikke længere sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med artikel 45, stk. 2. Såfremt Kommissionen har ophævet, ændret eller suspenderet en tilstrækkelighedsafgørelse, fører Kommissionen i medfør af stk. 6 konsultationer med tredjelandet eller den internationale organisation, med henblik på at afhjælpe situationen, ligesom der stadig er mulighed for at overføre personoplysninger på baggrund af de andre overførselsgrundlag, jf. stk. 7.[56]

[56] Nielsen, Anders Korfits m.fl., s. 782

Tilstrækkelighedsafgørelser truffet af Kommissionen på baggrund af databeskyttelsesdirektivets artikel 25, stk. 6 gælder fortsat indtil de ændres, erstattes eller ophæves ved en afgørelse af Kommissionen, der vedtages i medfør af databeskyttelsesforordningens artikel 45, stk. 3 eller 5.

2.8. Overførsel på baggrund af SCC

Såfremt der ikke er vedtaget en tilstrækkelighedsafgørelse vedrørende tredjelandet eller den internationale organisation i medfør af databeskyttelsesforordningen artikel 45, kan overførslen til det usikre tredjeland eller den internationale organisation i stedet ske ved at afgive fornødne garantier efter forordningens artikel 46 og 47, og på betingelse af at rettigheder, som kan håndhæves, og effektive retsmidler for registrerede er tilgængelige.

Databeskyttelsesforordningens artikel 46, stk. 2, litra c giver mulighed for, at dataoverførsler kan ske på baggrund af SCC vedtaget af Kommissionen. Kommissionen har på nuværende tidspunkt vedtaget tre forskellige SCC, som kan anvendes til at sikre, at overførselsgrundlaget sker med de fornødne garantier. Det er vigtigt at skelne mellem, hvorvidt den dataansvarlige i Unionen overfører oplysninger til en dataansvarlig eller en databehandler, idet de tre vedtagne SCC skelner mellem dette.[57]

Kommissionens afgørelse af 5. februar 2010 (2010/87/EU)[58] vedrører overførsel fra en dataansvarlig i Unionen til en databehandler i et tredjeland eller international organisation. Kommissionens beslutning af 15. juni 2001 (2001/497/EF)[59] og Kommissionens beslutning af 27. december 2004 (2004/915/EF)[60] vedrører derimod begge overførsel fra en dataansvarlig i Unionen til en dataansvarlig i et tredjeland eller international organisation. Forskellen mellem SCC af 2001 og SCC af 2004 for overførsler mellem dataansvarlige er blandt andet, at ansvaret er baseret på solidarisk hæftelse i SCC af 2001, hvorimod ansvaret i SCC af 2004 bygger på principper om fornøden omhu, hvor parterne hver især er ansvarlige overfor de registrerede for deres egne forpligtelser.[61]

[57] Datatilsynets vejledning om overførsler til tredjelande, s. 15
[58] Kommissionens afgørelse af 5. februar 2010 (2010/87/EU) med ændringer meddelt i Kommissionens gennemførelsesafgørelse (EU) 2016/2297 af 16. december 2016. Herefter 'SCC af 2010'
[59] Kommissionens beslutning af 15. juni 2001 (2001/497/EF) med ændringer meddelt i Kommissionens gennemførelsesafgørelse (EU) 2016/2297 af 16. december 2016. Herefter 'SCC af 2001'
[60] Herefter 'SCC af 2004'
[61] Kommissionens beslutning af 27. december 2004 (2004/915/EF), betragtning 5

Benytter en virksomhed SCC som overførselsgrundlag, er det ikke nødvendigt forinden overførslen at søge om tilladelse ved dennes nationale tilsynsmyndighed. Det er naturligvis afgørende ved anvendelsen af SCC, at parterne nøje sætter sig ind i kontraktens indhold, og at de er i stand til at overholde de forpligtelser, der indeholdes heri. Det er endvidere en betingelse, at der ikke laves ændringer i kontaktens bestemmelser, da selv små ændringer kan medføre, at der forinden skal indhentes tilladelse fra det nationale tilsyn til anvendelse af kontrakten som overførselsgrundlag. En sådan kontrakt betegnes i stedet som en ad hoc kontrakt.[62]

Gyldigheden af SCC af 2010 var genstand for en præjudiciel forelæggelse ved Domstolen i C-311/18, Schrems II. Domstolen erklærede ikke denne ugyldig, og SCC af 2010 kan således fortsat anvendes som overførselsgrundlag under visse betingelser. På trods af at SCC stadig kan anvendes som overførselsgrundlag, fremsatte Kommissionen den 12. november 2020 et nyt udkast til SCC i høring, som endnu ikke er vedtaget. Det nye udkast er fremsat som en samlet afgørelse, som på nuværende tidspunkt er opdelt i to dokumenter. Det ene dokument udgør udkastet til afgørelsesbeslutningen om nye SCC, og det andet dokument udgør selve aftaleteksten. Udkastet skal erstatte de nugældende SCC, jf. artikel 6 i udkastet til afgørelsesbeslutningen om nye SCC.

De nugældende SCC blev vedtaget på baggrund af databeskyttelsesdirektivet, og der er ifølge udkastet til afgørelsesbeslutningen om nye SCC fremkommet et behov for at opdatere standardbestemmelserne efter de nye krav og bestemmelser i databeskyttelsesforordningen. Endvidere er der siden Kommissionens afgørelser sket stor udvikling i den digitale økonomi, de teknologiske løsninger og ændringer af virksomhedernes forretningsrelationer. Tilsvarende er der fremkommet nyere og mere komplekse databehandlingsmetoder og -systemer, som også ofte involverer adskillige dataeksportører og dataimportører. Formålet med udkastet til nye SCC er således at modernisere standardbestemmelserne, så de bedre reflekterer og passer til den realitet virksomheder og myndigheder befinder sig i. Dette sker ved at tilpasse bestemmelserne til at dække flere typer af overførselssituationer og give mulighed for en mere fleksibel tilgang til anvendelse af dem. Herunder blandt andet ved at gøre det muligt for flere parter at deltage i den pågældende kontrakt.[63]

[62] Betænkning nr. 1565/2017, bind 2, s. 660 f.
[63] Udkast til afgørelsesbeslutning om nye SCC, betragtning 6

3. C-362/14, Schrems I og C-311/18, Schrems II

Nedenfor vil de to afgørelser C-362/14, Schrems I og C-311/18, Schrems II analyses med henblik på at belyse udviklingen i retsstillingen angående, hvad virksomheder og myndigheder bør være opmærksom på inden de foretager en overførsel til et tredjeland eller en international organisation.

3.1. C-362/14, Schrems I

C-362/14, Schrems I udsprang af en klage fra den østrigske Facebook-bruger Maximillian Schrems til det irske datatilsyn, Data Protection Commisioner.[64] Schrems indgav den 25. juli 2013 klagen på baggrund af oplysningerne om de amerikanske efterretningstjenester, som Edward Snowden kort forinden havde afsløret. Heraf blev det offentliggjort, at særligt National Security Agency[65] havde programmer, der masseovervågede den globale internet- og telekommunikation, hvilket blandt andet resulterede i, at NSA kunne tilgå oplysninger fra tjenesteudbydere som eksempelvis Facebook. Schrems indgav på den baggrund klagen med den anmodning, at Facebook Ireland skulle suspendere overførslen af hans personoplysninger til moderselskabet Facebook Inc. i USA, da Schrems ikke mente, at USA havde et tilstrækkeligt beskyttelsesniveau.[66]

Det irske datatilsyn afviste indledningsvist klagen med den begrundelse, at tilsynet ikke fandt det bevist, at NSA faktisk havde skaffet sig adgang til personoplysningerne. Tilsynet bemærkede endvidere, at der var sikret et tilstrækkeligt beskyttelsesniveau i USA, idet Kommissionen den 26. juli 2000 havde vedtaget tilstrækkelighedsafgørelsen Safe Harbour (2000/520/EF).[67] Safe Harbour fungerede som en frivillig selvcertificeringsmekanisme, hvor de deltagende virksomheder forpligtede sig til at leve op til ordningen.[68]

Maximillian Schrems påklagede tilsynets afgørelse til High Court, som er den øverste retsinstans i Irland. High Court var af den opfattelse, at tilsynet skulle have undersøgt de faktiske omstændigheder, som Schrems gjorde gældende i sin klage, såfremt tvisten udelukkende skulle være afgjort efter irsk

[64] C-362/14, Schrems I, præmis 26
[65] Herefter 'NSA'
[66] C-362/14, Schrems I, præmis 28
[67] C-362/14, Schrems I, præmis 29
[68] C-362/14, Schrems I, præmis 18

ret.[69] High Court anførte dog, at tvisten efter deres opfattelse vedrørte gennemførelsen af EU-retten, og af samme årsag skulle efterprøves i henhold hertil.[70] Schrems bestred formelt set ikke gyldigheden af databeskyttelsesdirektivet eller Safe Harbour, men idet Schrems klagede over databeskyttelsessikkerheden i USA, blev Schrems' klage i realiteten en klage mod lovligheden af Safe Harbour.[71] Spørgsmålene var herefter om tilsynet var bundet af tilstrækkelighedsafgørelsen Safe Harbour, og om tilsynet tillige havde pligt til at foretage en undersøgelse trods en sådan afgørelse. Som følge heraf forelagde High Court de præjudicielle spørgsmål for Domstolen.[72]

Domstolen afsagde den 6. oktober 2015 dom i sagen. I dommen behandlede Domstolen de præjudicielle spørgsmål og konkluderede endvidere, at en klage over en overførsel i medfør af Safe Harbour, skulle betragtes som en klage mod selve ordningens forenelighed med beskyttelsen af privatlivet og personers frihedsrettigheder og grundlæggende rettigheder.[73] Domstolen fandt, at førend den kunne give en fyldestgørende besvarelse af de præjudicielle spørgsmål, var det også nødvendigt for Domstolen at tage stilling til, hvorvidt tilstrækkelighedsafgørelsen Safe Harbour var i overensstemmelse med de krav, der fulgte af databeskyttelsesdirektivet sammenholdt med Charteret.[74]

3.1.1. Tilsynsmyndighedens kompetence

I forbindelse med afgørelsen af det præjudicielle spørgsmål om, hvorvidt tilsynsmyndigheder er bundet af Kommissionens tilstrækkelighedsafgørelser, gennemgik Domstolen i præmis 38 til 58 tilsynsmyndighedens beføjelser, der var reguleret i det dagældende databeskyttelsesdirektivs artikel 28. I forlængelse heraf anførte Domstolen, at medlemsstaterne og deres organer, herunder tilsynsmyndigheden, ikke kan vedtage foranstaltninger i strid med en kommissionsafgørelse, så længe Domstolen ikke har fastslået, at afgørelsen er ugyldig. Domstolen anførte yderligere, at der er en formodning for, at EU-institutionernes retsakter er lovlige, og at dette afføder retsvirkninger, så længe retsakterne ikke er blevet trukket tilbage, annulleret eller erklæret ugyldige.[75]

[69] C-362/14, Schrems I, præmis 33
[70] C-362/14, Schrems I, præmis 34
[71] C-362/14, Schrems I, præmis 35 og 59
[72] C-362/14, Schrems I, præmis 35 og 36
[73] C-362/14, Schrems I, præmis 59
[74] C-362/14, Schrems I, præmis 67
[75] C-362/14, Schrems I, præmis 52

Domstolen kom frem til, at det dog ikke skal forhindre eller ophæve tilsynsmyndighedernes beføjelser, der udtrykkeligt er tillagt i Charterets artikel 8, stk. 3 og det dagældende databeskyttelsesdirektivs artikel 28.[76] De nationale tilsynsmyndigheder skal således i fuld uafhængighed kunne undersøge en klage fra en person, der gør gældende, at lovgivningen og praksissen i tredjelandet, hvortil personoplysningerne overføres, ikke sikrer et tilstrækkeligt beskyttelsesniveau. Såfremt tilsynsmyndigheden ikke havde denne beføjelse, ville personer, hvis oplysninger er blevet videregivet til et tredjeland, blive berøvet deres ved Charterets artikel 8, stk. 1 og 3 sikrede ret til at indgive anmodning til tilsynet med henblik på at beskytte deres grundlæggende rettigheder.[77]

3.1.2. Kompetencen til at erklære en tilstrækkelighedsafgørelse ugyldig

I dommens præmis 63 til 66 fastlagde Domstolen nærmere, hvordan både de nationale tilsynsmyndigheder samt de nationale domstole skal forholde sig, når en person bestrider, at en tilstrækkelighedsafgørelse er forenelig med beskyttelsen af privatlivet og personers frihedsrettigheder og grundlæggende rettigheder. Domstolen konkluderede blandt andet, at hverken de nationale tilsynsmyndigheder eller de nationale domstole har kompetence til at erklære en EU-retsakt for ugyldig, men at Domstolen er enekompetent til dette. I C-362/14, Schrems I blev det fastlagt, at dette skyldes, at det er nødvendigt for at sikre en ensartet anvendelse af EU-retten og dermed også er nødvendigt for at garantere for retssikkerheden.[78] Henset til specialets omfang, vil der dog ikke laves en nærmere analyse af Domstolens undersøgelse af kompetencen til at erklære en tilstrækkelighedsafgørelse ugyldig.

3.1.3. Gyldigheden af Safe Harbour

Som tidligere beskrevet skal en klage over en overførsel i medfør af Safe Harbour betragtes som en klage mod selve ordningens forenelighed med beskyttelsen af privatlivet og personers frihedsrettigheder og grundlæggende rettigheder. Domstolen skulle dermed undersøge, hvorvidt Safe Harbour stadig var gyldig, og om USA dermed sikrede et tilstrækkeligt beskyttelsesniveau.

[76] C-362/14, Schrems I, præmis 53
[77] C-362/14, Schrems I, præmis 57, 58 og 66
[78] C-362/14, Schrems I, præmis 61

Domstolen bemærkede indledningsvist, at det ikke fremgik af databeskyttelsesdirektivets artikel 25, stk. 2, hvordan et 'tilstrækkeligt beskyttelsesniveau' skulle defineres.[79] Det fremgik dog af databeskyttelsesdirektivets artikel 25, stk. 2, at vurderingen af, hvorvidt et tilstrækkeligt beskyttelsesniveau var sikret, skulle ske på baggrund af samtlige forhold, der havde indflydelse på en videregivelse. Bestemmelsen fastlagde, at der i vurderingen blandt andet skulle lægges vægt på oplysningernes art, behandlingernes formål og varighed, samt de retsregler, der gjaldt i det pågældende tredjeland. Bestemmelsens opremsning af vurderingspunkter var dog ikke udtømmende.

På baggrund af generaladvokatens forslag til afgørelsen[80] punkt 141, fastslog Domstolen, at 'et tilstrækkeligt beskyttelsesniveau' skulle forstås på den måde, at tredjelandet skulle sikre et beskyttelsesniveau for frihedsrettighederne og de grundlæggende rettigheder, der i det væsentligste svarede til niveauet sikret i Unionen. Det var dog ikke et krav, at der sikredes et beskyttelsesniveau, der var identisk med niveauet sikret inden for Unionens område, men midlerne, som tredjelandet anvendte, skulle være effektive til at sikre et væsentligt tilsvarende beskyttelsesniveau. Årsagen til at niveauet i det væsentligste skulle svare til niveauet sikret i Unionen skyldtes, at rettigheden sikret i Charterets artikel 8, stk. 1 ville blive undermineret, såfremt virksomheder og myndigheder ved at føre oplysninger ud af Unionen og senere føre oplysninger tilbage igen ville kunne omgå rettigheden.[81]

Domstolen bemærkede, at det var nødvendigt løbende at overvåge udviklingen i tredjelandet med henblik på at vurdere, hvorvidt tredjelandet, efter Kommissionens afsigelse af en tilstrækkelighedsafgørelse, stadig sikrede et tilstrækkeligt beskyttelsesniveau. Det blev i den henseende bemærket, at denne forpligtelse for Kommissionen nu er direkte reguleret i databeskyttelsesforordningens artikel 45, stk. 4.[82]

Som det fremgik af Safe Harbours artikel 1, stk. 2 og 3, var Safe Harbour et selvcertificeringssystem. Domstolen fastslog, at dette ikke i sig selv medførte, at beslutningen var i strid med databeskyttelsesdirektivets krav om, at tredjelandet sikrede et tilstrækkeligt beskyttelsesniveau. Domstolen anførte,

[79] C-362/14, Schrems I, præmis 70 og 71
[80] Forslag til afgørelse fra generaladvokat Y. Bot, fremsat den 23. september 2015 (1), Sag C-362/14, Maximillian Schrems mod Data Protection Commissioner
[81] C-362/14, Schrems I, præmis 72-74
[82] C-362/14, Schrems I, præmis 76 og 77

at pålideligheden af dette system hvilede på tilstedeværelsen af effektive afslørings- og kontrolmekanismer.[83] Kommissionen udarbejdede meddelelse KOM(2013) 846 endelig[84], idet både Unionen, medlemsstater og borgere i Unionen havde udtrykt bekymring i forlængelse af Edward Snowdens afsløringer. Af meddelelsens punkt 2 fremgik det, at ordningens gennemsigtighed og håndhævelse var tvivlsom som følge af den frivillige og deklaratoriske karakter. Vigtigheden af at overførselsgrundlaget til USA faktisk sikrede et tilstrækkeligt beskyttelsesniveau kom til udtryk, idet Kommissionen påpegede, at Safe Harbour kom til at virke som en kanal for personoplysninger om unionsborgere til de amerikanske efterretningstjenester.[85] Dette skyldtes, at amerikanske, offentlige myndigheder ikke var undergivet overholdelse af Safe Harbour-principperne.[86] Vigtigheden manifesteredes særligt, da Kommissionen henviste til, at ordningen omfattede virksomheder med hundreder af millioner af kunder i Europa, der overførte personoplysninger til USA med henblik på behandling.[87]

Domstolen konstaterede, at det var problematisk, at Safe Harbours bilag IV, afsnit B, første afsnit, 2. punkt gav amerikansk ret forrang, såfremt der i den amerikanske lovgivning var principper, der var modstridende med Safe Harbour-principperne.[88] Domstolen anførte videre, at der ikke var lavet tilstrækkelige konstateringer om, hvorvidt USA på grundlag af landets lovgivning havde mulighed for at sikre et tilstrækkeligt sikkerhedsniveau.[89]

Herunder fandt Domstolen det problematisk, at det i Safe Harbour hverken var konstateret, om der i USA var regler, der begrænsede indgreb i registreredes grundlæggende rettigheder, eller om der forelå en effektiv domstolsbeskyttelse mod denne type indgreb. Domstolen bemærkede endvidere, at voldgiftsmekanismen, der var beskrevet i Safe Harbour, bilag II, FAQ 11, som skulle behandle sager om påståede overtrædelser af Safe Harbour-principperne, alene vedrørte handelstvister, og dermed ikke kunne benyttes ved statslige foranstaltninger.[90]

---

[83] C-362/14, Schrems I, præmis 81
[84] KOM(2013) 846 endelig, "Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet: Genopbygning af tilliden til datastrømmene mellem EU og USA" af 27. november 2013
[85] C-362/14, Schrems I, præmis 15
[86] C-362/14, Schrems I, præmis 82
[87] KOM(2013) 847 endelig, "Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om, hvordan safe harbor-ordningen fungerer for så vidt angår EU-borgerne og virksomhederne i EU" af 27. november 2013, punkt 8
[88] C-362/14, Schrems I, præmis 85
[89] C-362/14, Schrems I, præmis 83
[90] C-362/14, Schrems I, præmis 88 og 89

I forlængelse heraf fremhævede Kommissionen i meddelelse KOM(2013) 847 endelig, punkt 7.2., at de sikkerhedsforanstaltninger, som faktisk fandtes i amerikansk ret, primært gjaldt for amerikanske statsborgere, ligesom de registrerede manglede mulighed for at opnå indsigt i, berigtigelse eller sletning af oplysninger.

På baggrund af Domstolens konstateringer blev det konkluderet, at Safe Harbour var ugyldig som overførselsgrundlag. Domstolen tilsluttede sig således Kommissionen betragtning i KOM(2013) 846 endelig, punkt 3.2., hvor Kommissionen bemærkede, at fastholdelse af Safe Harbour var urealistisk. Dette skyldtes, at den amerikanske lovgivning var indrettet på en sådan måde, at de amerikanske myndigheder kunne få adgang til personoplysninger og behandle disse, selvom det blandt andet var i strid med det oprindelige formål, som oplysningerne blev videregivet i medfør af. Den amerikanske lovgivning foretog desuden ikke nogen form for differentiering, begrænsning eller undtagelse af indsamlingen, ligesom der heller ikke var fastsat noget objektivt kriterium til afgrænsningen af de offentlige myndigheders adgang og anvendelse af oplysningerne, og det gik således ud over, hvad der var strengt nødvendigt. De amerikanske myndigheders mulighed for vilkårlig adgang til personoplysninger anså Domstolen for et indgreb i den grundlæggende ret til respekt for privatliv sikret i Charterets artikel 7.[91]

I ugyldighedsvurderingen lagde Domstolen ligeledes vægt på den manglende adgang til effektive retsmidler var uforenelig med Charterets artikel 47.[92]

Domstolen bemærkede, at Kommissionen ikke i Safe Harbour havde anført, at USA på grundlag af landets lovgivning eller internationale forpligtelser sikrede et tilstrækkeligt beskyttelsesniveau. Domstolen kunne som følge heraf erklære Safe Harbour ugyldig uden at gå ind i en nærmere undersøgelse af indholdet af Safe Harbour-principperne.

Slutteligt konkluderede Domstolen, at Kommissionen ved vedtagelse af artikel 3, stk. 1 i Safe Harbour, havde overskredet deres beføjelser tillagt i databeskyttelsesdirektivets artikel 25, stk. 6, idet

[91] C-362/14, Schrems I, præmis 90, 93 og 94
[92] C-362/14, Schrems I, præmis 95

Kommissionen havde begrænset de nationale tilsynsmyndigheders beføjelser ved at fastsætte restriktive betingelser for, hvornår de nationale tilsynsmyndigheder kunne gøre brug af deres beføjelser, herunder suspension af overførsler i medfør af Safe Harbour.[93]

3.2. C-311/18, Schrems II

Efter Domstolens afgørelse i C-362/14, Schrems I annullerede den forelæggende ret det irske datatilsyns afslag på Schrems' klage og hjemviste den til behandling i det irske datatilsyn. Tilsynet indledte herefter en undersøgelse i anledning af den oprindelige klage. I den forbindelse forklarede Facebook Ireland, at en stor del af de oplysninger, de overførte, skete på baggrund af SCC af 2010. Schrems omformulerede herefter sin klage, og gjorde gældende, at tjenesteudbydere, såsom Facebook, i medfør af amerikansk lovgivning skulle stille oplysninger til rådighed for de amerikanske efterretningstjenester, og at dette var uforeneligt med beskyttelsen i Charterets artikel 7, 8 og 47. Selv anvendelsen af SCC af 2010 kunne efter hans mening ikke begrunde overførslen, og Schrems anmodede således om suspension af overførslen.[94]

I C-362/14, Schrems I, præmis 16, konkluderede Kommissionen, at ophævelsen af Safe Harbour ville få negativ indvirkning på virksomhederne i Unionen og i USA, idet overførsler til USA i så fald skulle suspenderes eller ske på et andet grundlag. Af samme årsag tilføjede Kommissionen, at det var af høj prioritet for dem at finde en ny løsning på de brister, der kunne konstateres. Efter Schrems indgav sin omformulerede klage, vedtog Kommissionen som følge heraf en ny tilstrækkelighedsafgørelse. Tiltrækkelighedsafgørelsen blev vedtaget den 12. juli 2016 med navnet Privacy Shield.[95]

Kommissionen undersøgte i forbindelse med vedtagelsen af Privacy Shield begrænsningerne og garantierne i amerikansk ret, herunder myndighedernes adgang til personoplysninger overført fra Unionen. Privacy Shield fungerede tilsvarende Safe Harbour som en selvcertificeringsmekanisme for de amerikanske virksomheder og myndigheder, men forskellen fra Safe Harbour var, at der i Privacy Shield skulle være øget gennemsigtighed for, hvornår de amerikanske myndigheder kunne få adgang

[93] C-362/14, Schrems I, præmis 101-104
[94] C-311/18, Schrems II, præmis 54 og 55
[95] Kommissionens gennemførelsesafgørelse (EU) 2016/1250 af 12. juli 2016

til at indsamle personoplysninger. Det amerikanske justitsministerium lavede i den anledning en udredning af de gældende amerikanske regler, som blev offentliggjort i USA's Federal Register. Yderligere blev der i Privacy Shield tilsvarende indført en ny tilsynsmekanisme, som bestod af en ombudsmand, der skulle agere som et uafhængigt tilsyn.[96]

Det irske datatilsyn fandt, at Schrems' klage skulle opfattes som en klage mod gyldigheden af SCC, og indbragte derfor sagen for High Court. High Court fastslog, at de havde pligt til at undersøge samtlige faktiske omstændigheder og argumenter, samt pligt til at tage hensyn til eventuelle ændringer af lovgivningen siden sagens anlæggelse. High Court fandt det nødvendigt at lave en præjudiciel forelæggelse for Domstolen.[97] Domstolen tog herefter stilling til de præjudicielle spørgsmål, og fandt desuden behov for at undersøge gyldigheden af Privacy Shield for at give den forelæggende ret en fyldestgørende besvarelse af de præjudicielle spørgsmål.[98] Domstolens behandling af de præjudicielle spørgsmål vil analyseres nærmere nedenfor.

3.2.1. Betydning af overgang fra databeskyttelsesdirektivet til databeskyttelsesforordningen

Facebook Ireland gjorde i forbindelse med sagens præjudicielle forelæggelse ved Domstolen indsigelse mod, at de præjudicielle spørgsmål var baseret på et nu ophævet direktiv. Domstolen gjorde i den forbindelse gældende, at databeskyttelsesdirektivet stadig var gældende ved High Courts anmodning om præjudiciel afgørelse, samt at direktivets bestemmelser, som spørgsmålene henviste til, i det væsentligste er gengivet i databeskyttelsesforordningen. Domstolen bemærkede i den forbindelse, at Domstolen skal fortolke alle bestemmelser i EU-retten, som nationale domstole skal anvende for at træffe afgørelser i verserende tvister, også selvom de pågældende bestemmelser ikke er udtrykkeligt omtalt i de forelagte præjudicielle spørgsmål.[99] Domstolen bemærkede yderligere, at eftersom der ikke var truffet en national afgørelse under databeskyttelsesdirektivet, skulle de præjudicielle spørgsmål besvares på grundlag af bestemmelserne i databeskyttelsesforordningen.[100]

[96] C-311/18, Schrems II, præmis 43
[97] C-311/18, Schrems II, præmis 58 og 59
[98] C-311/18, Schrems II, præmis 151, 153 og 161
[99] C-311/18, Schrems II, præmis 70 og 71
[100] C-311/18, Schrems II, præmis 77-79

High Court forelagde Domstolen elleve præjudicielle spørgsmål. Domstolen valgte i forbindelse med besvarelsen at behandle nogle af spørgsmålene samlet på grund af spørgsmålenes sammenhæng, mens andre spørgsmål blev behandlet separat.

3.2.2. Vurdering af, hvorvidt overførslen var omfattet af EU-retten

Domstolen valgte at behandle det første spørgsmål separat. Spørgsmålet omhandlede, hvorvidt overførslen fra Facebook Ireland til Facebook Inc. i USA faktisk var omfattet af EU-retten, når det i TEU artikel 4, stk. 2 er bestemt, at den nationale sikkerhed inden for Unionen forbliver den enkelte medlemsstats eneansvar. Årsagen til spørgsmålet var, at Schrems' klage hovedsageligt var møntet på, at USA's offentlige myndigheder, herunder USA's efterretningstjenester, behandlede de oplysninger, som blev overført til Facebook Inc. i USA, af hensyn til USA's nationale sikkerhed.[101]

Domstolen konkluderede indledningsvist, at TEU kun gælder medlemsstaterne henset til ordlyden i TEU artikel 4, stk. 2. Undtagelsen kan således ikke anvendes af de amerikanske offentlige myndigheder. En overførsel fra Facebook Ireland til Facebook Inc. faldt derfor ikke uden for EU-rettens anvendelsesområde.[102]

Domstolen konkluderede, at en sådan overførsel er omfattet af databeskyttelsesforordningens anvendelsesområde, også selvom at tredjelandets offentlige myndigheder behandler de overførte oplysninger af hensyn til offentlige sikkerhed, forsvaret og statens sikkerhed. I denne henseende kommenterede Domstolen på, at Kommissionen allerede i forbindelse med undersøgelsen af, hvorvidt der kunne laves en tilstrækkelighedsafgørelse havde lagt vægt på tredjelandets lovgivning vedrørende offentlig sikkerhed, forsvar og statens sikkerhed, jf. databeskyttelsesforordningens artikel 45, stk. 2, litra a.[103]

[101] C-311/18, Schrems II, præmis 80
[102] C-311/18, Schrems II, præmis 81
[103] C-311/18, Schrems II, præmis 86-89

3.2.3. Vurdering af, hvilket beskyttelsesniveau, der kræves ved overførsel efter SCC

Domstolen behandlede efterfølgende det andet, tredje og sjette spørgsmål samlet. Med disse tre spørgsmål anmodede den forelæggende ret Domstolen om nærmere at vurdere, hvilket beskyttelsesniveau der kræves i forbindelse med en overførsel af personoplysninger til tredjelande efter SCC. I forbindelse med denne vurdering anmodede den forelæggende ret også om en nærmere præcisering af, hvilke forhold der skal tages i betragtning ved vurderingen af tredjelandets beskyttelsesniveau, samt om det relevante sammenligningsgrundlag er EU-retlige bestemmelser eller medlemsstaters nationale ret.[104]

Domstolen henviste i sin besvarelse til databeskyttelsesforordningens artikel 46, stk. 1. Heraf fremgår det, som beskrevet i afsnit 2.8., at en dataansvarlig eller databehandler må overføre personoplysninger til et tredjeland eller en international organisation, hvis vedkommende har givet de fornødne garantier og på betingelse af at rettigheder, som kan håndhæves, og effektive retsmidler for registrerede er tilgængelige.

I forbindelse med fortolkningen af hvad der skal forstås ved 'fornødne garantier', 'rettigheder, der kan håndhæves' og 'effektive retsmidler', henviste Domstolen til databeskyttelsesforordningens artikel 44. Af denne bestemmelse fremgår det, som beskrevet i afsnit 2.6., at databeskyttelsesforordningens beskyttelsesniveau ikke må undermineres ved en overførsel til et tredjeland eller en international organisation. Domstolen anvendte derfor deres fortolkning i C-362/14, Schrems I, af 'et tilstrækkeligt beskyttelsesniveau' til at fortolke, hvordan 'fornødne garantier' skal forstås.[105]

Som anført i afsnit 3.1.3. udledte Domstolen i C-362/14, Schrems I på baggrund af generaladvokatens forslag til afgørelsen punkt 141, at et tilstrækkeligt beskyttelsesniveau er sikret, når beskyttelsesniveauet i det væsentligste svarer til niveauet, der er sikret i Unionen. Generaladvokaten fremhævede i forslag til afgørelsen C-311/18, Schrems II[106] punkt 115, at han ligeledes var af den opfattelse, at de

[104] C-311/18, Schrems II, præmis 90
[105] C-311/18, Schrems II, præmis 91
[106] Forslag til afgørelse fra generaladvokat H. Saugmandsgaard Øe, fremsat den 19. december 2019 (1), Sag C-311/18, Data Protection Commissioner mod Facebook Ireland Limited og Maximillian Schrems

fornødne garantier i henhold til databeskyttelsesforordningen artikel 46 tilsvarende skulle sikre et beskyttelsesniveau, der i det væsentligste svarer til niveauet sikret i Unionen.

På baggrund heraf konkluderede Domstolen, at fortolkningen af 'et tilstrækkeligt beskyttelsesniveau' i C-362/14, Schrems I også må finde anvendelse på fortolkningen af 'fornødne garantier'. Hertil henviste Domstolen til databeskyttelsesforordningens præambelbetragtning 108, hvoraf det fremgår, at såfremt en overførsel sker på baggrund af fornødne garantier, skal de fornødne garantier kompensere for den manglende databeskyttelse i et tredjeland for at sikre overholdelse af databeskyttelseskravene og de registreredes rettigheder.[107] Anvendelsen af ordet 'kompensere' henviser til det tilfælde, hvor tredjelandet ikke sikrer et tilstrækkeligt beskyttelsesniveau, og det derfor ikke har været muligt at træffe en tilstrækkelighedsafgørelse. Virksomheders og myndigheders afgivelse af fornødne garantier skal således kompensere for det utilstrækkelige beskyttelsesniveau i tredjelandet, således at det i det væsentligste svarer til beskyttelsesniveauet i Unionen.

High Court havde endvidere forespurgt, hvorvidt beskyttelsesniveauet skal fastlægges på grundlag af EU-retten, EMRK eller medlemsstaternes nationale ret.[108] Domstolen konkluderede, at medlemsstaternes nationale ret ikke anvendes som fortolkning af EU-ret.[109] Derudover konkluderede Domstolen også, at EMRK ikke udgør et retligt instrument i Unionen, idet Unionen ikke har tiltrådt EMRK, og at EMRK dermed heller ikke direkte anvendes til fastlæggelse af beskyttelsesniveauet.[110]

Domstolen konkluderede dernæst, at Charteret skal anvendes til fastlæggelse af beskyttelsesniveauet i databeskyttelsesforordningen. EMRK kan anvendes som fortolkningsbidrag til Charterets bestemmelser, jf. Charterets artikel 52, stk. 3, hvilket også nærmere er behandlet i afsnit 2.4. Domstolen anførte i den forbindelse, at anvendelse af Charteret sikrer en ensartet fortolkning af EU-rettens bestemmelser.[111]

[107] C-311/18, Schrems II, præmis 95
[108] C-311/18, Schrems II, præmis 97
[109] C-311/18, Schrems II, præmis 100
[110] C-311/18, Schrems II, præmis 98
[111] C-311/18, Schrems II, præmis 98, 99 og 101

Konklusionen var dermed, at når der sker overførsel af personoplysningerne efter SCC skal beskyttelsesniveauet fortolkes i sammenhæng med databeskyttelsesforordningens artikel 44 og 45, samt rettighederne tillagt i Charteret. Selve gyldigheden af SCC i lyset af Charteret behandles nærmere i afsnit 3.2.5.

3.2.4. Vurdering af, hvordan tilsynet skal forholde sig, når de vurderer, at en overførsel ikke overholder kravene

I det ottende spørgsmål ønskede den forelæggende ret en nærmere præcisering af, hvordan de nationale tilsynsmyndigheder skal forholde sig, såfremt de vurderer, at en overførsel af personoplysninger til et tredjeland i medfør af SCC ikke kan overholde bestemmelserne heri eller i øvrigt er i strid med databeskyttelsesforordningen eller Charteret. Den forelæggende ret ønskede i denne forbindelse nærmere præciseret, hvorvidt den kompetente tilsynsmyndighed i så fald har pligt til at suspendere eller forbyde en overførsel af personoplysninger til et tredjeland på grundlag af SCC.[112]

Domstolen henviste til tilsynsmyndighedernes pligt til at undersøge indgivne klager om, at der ikke er tilstrækkeligt beskyttelsesniveau i det tredjeland, som personoplysningerne er overført til. Til dette bemærkede Domstolen, at tilsynsmyndigheden har væsentlige undersøgelsesbeføjelser, og en pligt til at afhjælpe utilstrækkeligheden ved den korrigerende foranstaltning, der er mest hensigtsmæssig og nødvendig.[113] Dette skal ske under hensyntagen til samtlige omstændigheder.[114] I forlængelse heraf har tilsynsmyndigheden, såfremt hverken den dataansvarlige eller databehandleren selv har suspenderet overførslen, og såfremt der ikke foreligger en tilstrækkelighedsafgørelse, pligt til at suspendere eller forbyde en overførsel, i det tilfælde, hvor tilsynsmyndigheden ikke finder, at tredjelandet sikrer et tilstrækkeligt beskyttelsesniveau.[115]

Afslutningsvist blev det fastslået, at når Domstolen ikke har erklæret en tilstrækkelighedsafgørelse ugyldig, kan de nationale tilsynsmyndigheder ikke foretage foranstaltninger, der er i strid med tilstrækkelighedsafgørelsen. En tilsynsmyndighed kan således ikke forbyde eller suspendere en

[112] C-311/18, Schrems II, præmis 106
[113] Databeskyttelsesforordningens artikel 58, stk. 2
[114] C-311/18, Schrems II, præmis 111 og 112
[115] C-311/18, Schrems II, præmis 113

overførsel af personoplysninger til et tredjeland, hvorom der er truffet en tilstrækkelighedsafgørelse. Som det også blev konkluderet i C-362/14, Schrems I, er tilsynsmyndighederne, til trods for at de er bundet af disse tilstrækkelighedsafgørelser, dog fortsat forpligtet til at undersøge og behandle klager vedrørende beskyttelsesniveauet i tredjelandet.[116] Se mere herom i afsnit 3.1.1.

3.2.5. Vurdering af den generelle gyldighed af SCC i lyset af Charteret

Dernæst behandlede Domstolen det syvende og ellevte spørgsmål samlet. Her anmodede den forelæggende ret Domstolen om at tage stilling til den generelle gyldighed af SCC i lyset af Charterets artikel 7, 8 og 47. Dette skyldtes, at den forelæggende ret stillede spørgsmålstegn ved, hvorvidt SCC stadig kunne anvendes som gyldigt overførselsgrundlag, når disse alene forpligter kontraktens parter. Den forelæggende ret argumenterede i den forbindelse for, at når de nationale myndigheder ikke er bundet af disse SCC, så kan nationale myndigheder pålægge en dataimportør i tredjelandet at stille personoplysninger til rådighed.[117]

Domstolen konkluderede, at gyldigheden af SCC i lyset af Charterets artikel 7, 8 og 47 afhænger af om der faktisk opstilles effektive mekanismer, der gør det muligt i praksis at håndhæve og sikre det beskyttelsesniveau, der kræves i Unionen. Det påvirker ikke gyldigheden af SCC, at disse ikke binder tredjelandets myndigheder.[118]

Domstolen kommenterede endvidere på, at såfremt tredjelandets lovgivning umuliggør, at der kan træffes en tilstrækkelighedsafgørelse, bevirker dette ikke, at der ikke kan ske overførsler af personoplysninger til samme tredjeland efter SCC.[119] Ved vedtagelse af en tilstrækkelighedsafgørelse skal Kommissionen konstatere, at al relevant lovgivning i tredjelandet faktisk sikrer de grundlæggende rettigheder. Modsat er dette ikke en betingelse, når Kommissionen vedtager afgørelse om SCC, da disse ikke tager sigte på et bestemt tredjeland, et område eller sektorer, og kan anvendes generelt.[120]

[116] C-311/18, Schrems II, præmis 118-120 og C-362/14, Schrems I, præmis 63-66
[117] C-311/18, Schrems II, præmis 122
[118] C-311/18, Schrems II, præmis 136 og 137
[119] C-311/18, Schrems II, præmis 129
[120] C-311/18, Schrems II, præmis 129 og 130

Det blev yderligere fastslået, at overførsler i medfør af SCC ikke altid udgør et tilstrækkeligt middel til at sikre effektiv beskyttelse af personoplysninger. Dette er navnlig tilfældet, når tredjelandets lovgivning tillader, at de offentlige myndigheder får adgang til personoplysninger.[121] Eftersom SCC gælder generelt, kan det være nødvendigt at supplere de garantier, som SCC'erne indeholder. Her henviste Domstolen til databeskyttelsesforordningens præambelbetragtning 109, hvoraf det fremgår, at anvendelsen af SCC ikke er til hinder for, at den dataansvarlige og databehandleren medtager andre bestemmelser eller yderligere garantier, såfremt det er nødvendigt for at sikre, at beskyttelsen ikke undermineres.[122]

Domstolen konkluderede, at det dermed er den dataansvarlige og databehandleren, der er ansvarlig for, at tredjelandets lovgivning kombineret med SCC sikrer den væsentlige samme beskyttelse som i Unionen. Såfremt dette ikke er tilfældet, er det den dataansvarlige og databehandleren, der er ansvarlige for at opstille supplerende foranstaltninger til SCC'erne, således den væsentlige samme beskyttelse sikres.[123] Hertil opstiller SCC af 2010 betingelser for modtageren af personoplysninger. I SCC af 2010, bestemmelse 5 forpligter modtageren sig til at underrette den dataansvarlige i Unionen, såfremt modtageren ikke er i stand til at overholde forpligtelserne. I samme bestemmelse skal modtageren bekræfte, at denne ikke har grund til at tro, at modtagerlandets lovgivning forhindrer overholdelse af forpligtelserne i henhold til kontrakten. Ydermere har modtageren også pligt til at underrette den dataansvarlige i Unionen, såfremt der kommer ny lovgivning, der ikke længere muliggør overholdelse af modtagerens forpligtelser, således overførslen bør suspenderes eller forbydes af den dataansvarlige. Kommissionen fremhævede endvidere i fodnoten til standardbestemmelse 5, at det ikke er i strid med SCC'erne, når tredjelandets lovgivning giver adgang til personoplysninger, så længe disse regler ikke er mere vidtgående end dem, der er nødvendige i et demokratisk samfund af hensyn til blandt andet statens sikkerhed, forsvaret og den nationale sikkerhed.[124] Der skal således foretages en proportionalitetsafvejning, når det vurderes om reglerne faktisk er nødvendige.

[121] C-311/18, Schrems II, præmis 126
[122] C-311/18, Schrems II, præmis 132 og 133
[123] C-311/18, Schrems II, præmis 134
[124] C-311/18, Schrems II, præmis 139-141

Henset til, at den dataansvarlige og databehandleren har pligt til at foretage supplerende foranstaltninger for at sikre den væsentlige samme beskyttelse som i Unionen, så konkluderede Domstolen, at SCC fortsat er generelt gyldige som overførselsgrundlag. Hertil fremhævede Domstolen, at konsekvensen af, at der ikke kan sikres de fornødne garantier er, at den dataansvarlige og subsidiært tilsynsmyndigheden har pligt til at suspendere eller forbyde overførslen. Derudover kan et tilsyn med henblik på at sikre ensartethed anmode Databeskyttelsesrådet om en udtalelse om, hvorvidt en overførsel til et tredjeland generelt skal forbydes.[125]

3.2.6. Vurdering af, hvorvidt overførsler til USA krænkede rettighederne i Charteret

I det niende spørgsmål anmodede den forelæggende ret om at få præciseret, i hvilket omfang en medlemsstats tilsynsmyndighed var bundet af, at Kommissionen i Privacy Shield havde afgjort, at USA sikrede et tilstrækkeligt beskyttelsesniveau.[126] I samme forbindelse behandlede Domstolen det fjerde, femte og tiende spørgsmål samlet, idet disse tre spørgsmål omhandlede, hvorvidt en overførsel til USA ved anvendelse af SCC krænkede privatpersoners rettigheder efter Charterets artikel 7, 8 og 47. Det fjerde spørgsmål omhandlede krænkelsen af Charterets artikel 7 og 8, mens spørgsmål 5a omhandlede krænkelse af Charterets artikel 47. Den forelæggende ret anmodede herunder i det tiende spørgsmål om en præcisering af, hvorvidt ombudsmanden var et tilstrækkeligt retsmiddel efter Charterets artikel 47. I spørgsmål 5b anmodede den forelæggende ret ydermere om en præcisering af, hvorvidt disse indgreb i privatpersoners rettigheder kunne anses som proportionelle efter Charterets artikel 52.

3.2.6.1. Vurdering af, hvorvidt overførsler til USA ved anvendelse af Privacy Shield krænkede rettighederne i Charteret

I Domstolens vurdering af, hvorvidt overførsler til USA krænkede rettighederne sikret i Charterets artikel 7, 8 og 47, startede Domstolen med at vurdere, hvorvidt en overførsel ved anvendelse af Privacy Shield krænkede rettighederne i Charteret. Dette var til trods for, at den forelæggende ret faktisk havde anmodet Domstolen om at vurdere, hvorvidt overførsler til USA ved anvendelsen af SCC

[125] C-311/18, Schrems II, præmis 146-149
[126] C-311/18, Schrems II, præmis 150

krænkede rettighederne i Charteret. Domstolen fremhævede, at de anså sig forpligtet til at vurdere, hvorvidt overførsler ved anvendelse af Privacy Shield var gyldige, idet Privacy Shield blev vedtaget efter anlæggelsen af de præjudicielle spørgsmål, og idet Domstolen konstaterede, at de var forpligtet til at medtage alle relevante omstændigheder i forbindelse med deres afgørelse.[127]

Som det fremgik af betragtning 140 i Privacy Shield var det muligt for de amerikanske myndigheder at gøre indgreb i de grundlæggende rettigheder, når det skete med henblik på beskyttelse af den nationale sikkerhed, retshåndhævelse og andre offentlige interesser, såfremt indgrebene blev begrænset til det, der var strengt nødvendigt ud fra legitime mål, samtidig med at der var en effektiv retsbeskyttelse mod indgrebene. Domstolen bemærkede dog i denne forbindelse, at der i undtagelsesbestemmelsen i Privacy Shield, bilag 2, punkt 1.5., var åbnet op for, at de selvcertificerede virksomheder kunne se bort fra principperne i Privacy Shield, såfremt amerikansk lovgivning var modstridende med disse. Amerikansk lovgivning havde derfor forrang for principperne i Privacy Shield. Domstolen bemærkede i den forbindelse, at undtagelsen var af så generel karakter, at der potentielt blev åbnet op for indgreb i de registreredes grundlæggende rettigheder, der gik videre, end hvad der var nødvendigt og proportionelt. Derfor undersøgte Domstolen, hvorvidt der i den amerikanske lovgivning var hjemmel til at foretage indgreb, der gik videre, end hvad der var nødvendigt og proportionelt.[128] Domstolen vurderede i denne forbindelse overvågningsprogrammerne i USA, herunder Foreign Intelligence Surveillance Act (FISA), Executive Order (E.O.) 12333 og Presidential Policy Directive (PPD) 28.

Som beskrevet tidligere i afsnit 2.4., fremgår det af Charterets artikel 52, stk. 1, 2. pkt., at indgrebet skal være proportionelt, samt begrænset til det, der er strengt nødvendigt. Førend et indgreb kan anses som strengt nødvendigt, er det en betingelse, at lovhjemlen til indgrebet er angivet klart og præcist. Domstolen undersøgte indledningsvist FISA, der er en vedtægt, som indeholder en række retsgrundlag, der kan bruges til at overvåge ikke-amerikanske personer. Hertil konkluderede Domstolen, at idet FISA sec. 702 (50 USC § 1881a) ikke nærmere angiver begrænsninger i beføjelsen til at overvåge, er FISA ikke i overensstemmelse med Charterets artikel 52, stk. 1, 2. pkt.[129]

[127] C-311/18, Schrems II, præmis 151
[128] C-311/18, Schrems II, præmis 164, 165 og 167
[129] C-311/18, Schrems II, præmis 176, 178 og 180

Dernæst vurderede Domstolen E.O. 12333, der er et præsidentielt dekret. Dekretet fungerer som et retsgrundlag, som efterretningsmyndigheder kan anvende til at indsamle og behandle personoplysninger. E.O. 12333 punkt 2.3. fastsætter begrænsninger for, hvornår amerikanske efterretningstjenester må indsamle og behandle oplysninger om amerikanske borgere. Unionsborgere er dermed ikke omfattet af disse begrænsninger, hvorfor E.O. 12333 ikke bidrager til at sikre et tilstrækkeligt beskyttelsesniveau. Desuden konstaterede Domstolen, at E.O. 12333 tillader, at der gives adgang til de oplysninger, som er undervejs til USA ved at tilgå undersøiske kabler, og at der intet retligt tilsyn er med denne adgang, ligesom der som angivet ikke er nogen begrænsning for omfanget af masseindsamlingen af personoplysninger om unionsborgere.[130]

Afslutningsvist vurderede Domstolen PPD-28, der er et amerikansk direktiv, som pålægger begrænsninger for amerikanske efterretningstjenesters muligheder for at indsamle oplysninger. PPD-28 blev indført med henblik på at afhjælpe de problemer, der blev konstateret i C-362/14, Schrems I. PPD-28 tillader dog, at der foretages masseindsamling af et højt antal personoplysninger uden en identifikator for at målrette indsamlingen, idet der i PPD-28 alene er angivet, at efterretningsaktiviteterne skal være så målrettede som muligt.[131]

Konklusionen fra Domstolen var dermed, at hverken FISA sec. 702 eller E.O. 12333 sammenholdt med PPD-28 opfylder proportionalitetsprincippet i Charterets artikel 52, idet overvågningen ikke er begrænset til det, der er strengt nødvendigt.[132] Beskyttelsen sikret i USA svarer derfor ikke i det væsentligste til den, der er sikret i Unionen.

Domstolen undersøgte endvidere, hvorvidt Privacy Shield var i strid med Charterets artikel 47, der hjemler, at der skal være adgang til effektive retsmidler og en upartisk domstol. Se nærmere herom i afsnit 2.3. Efter FISA sec. 702 kan fysiske personer anlægge søgsmål med henblik på at få økonomisk erstatning på grund af uretmæssig anvendelse af personoplysninger, ligesom den gør det muligt for personer at anmode om at få oplysninger fjernet.[133] FISA sec. 702 giver dog ikke garantier for ikke-

[130] C-311/18, Schrems II, præmis 63 og 183
[131] C-311/18, Schrems II, præmis 49 og 64
[132] C-311/18, Schrems II, præmis 184
[133] C-311/18, Schrems II, præmis 45, 112. betragtning

amerikanske personer. Hertil konstaterede Domstolen, at overvågningsprogrammer vedtaget i henhold til FISA sec. 702 skal overholde de krav, der følger af PPD-28. Domstolen konstaterede, at kravene i PPD-28 binder de amerikanske efterretningstjenester, men at PPD-28 ikke giver de registrerede rettigheder, der faktisk kan håndhæves overfor myndighederne ved domstolene. Hertil konkluderede Domstolen, at lovgivningen var i strid med Charterets artikel 47, men også i strid med kravene til et tilstrækkeligt beskyttelsesniveau efter databeskyttelsesforordningens artikel 45, stk. 2, litra a.[134]

Efter C-362/14, Schrems I indførte USA en ombudsmand i forbindelse med vedtagelsen af Privacy Shield. Ombudsmanden skulle agere som tilsynsmekanisme, der var uafhængig af de amerikanske efterretningstjenester. Ombudsmanden skulle afhjælpe, at det i C-362/14, Schrems I blev konstateret, at der ingen effektive retsmidler var for ikke-amerikanske personer. Domstolen konstaterede i C-311/18, Schrems II, at indførelsen af en ombudsmand ikke, som det var tiltænkt, afhjalp de mangler, der blev konstateret i C-362/14, Schrems I. Domstolen argumenterede i denne sammenhæng for, at idet ombudsmanden udgjorde en del af det amerikanske udenrigsministerium, udgjorde en klagemulighed til ombudsmanden ikke en upartisk og uafhængig domstol. Dette skyldtes, at der ikke forelå oplysninger om ombudsmandens reelle uafhængighed i form af udnævnelse, tilbagekaldelse af udnævnelse eller nedlæggelse af stillingen.[135] Den amerikanske regering påtog sig at sikre, at den pågældende enhed inden for efterretningstjenesterne faktisk bragte overtrædelser, som ombudsmanden konstaterede, til ophør. Ombudsmanden havde dog ikke reelle beføjelser til at træffe bindende afgørelser over for efterretningstjenesterne, såfremt disse ikke efterkom ombudsmandens konstateringer.[136] Ombudsmanden kunne derfor ikke afbøde den manglende domstolsbeskyttelse, idet indførelsen af en ombudsmand ikke skabte et retsmiddel, der i det væsentligste svarede til de retsmidler, der kræves efter Charterets artikel 47.

På baggrund af ovenstående konkluderede Domstolen, at Privacy Shield var ugyldig, idet tilstrækkelighedsafgørelsen sammenholdt med den amerikanske lovgivning krænkede rettighederne sikret i

[134] C-311/18, Schrems II, præmis 181 og 187
[135] C-311/18, Schrems II, præmis 190, 194 og 195
[136] C-311/18, Schrems II, præmis 196

Charterets artikel 7, 8 og 47. Privacy Shield sikrede dermed ikke et tilstrækkeligt beskyttelsesniveau efter databeskyttelsesforordningens artikel 45.

Med den forelæggende rets niende spørgsmål, ønskede retten at få oplyst, i hvilket omfang medlemslandenes tilsynsmyndigheder og retsinstanser var bundet af Kommissionens tilstrækkelighedsafgørelse Privacy Shield, der fastslog, at USA sikrede et tilstrækkeligt beskyttelsesniveau. I overensstemmelse med besvarelsen af ottende spørgsmål, som beskrevet i afsnit 3.2.4., konkluderede Domstolen, at når tilstrækkelighedsafgørelsen ikke er underkendt, kan tilsynsmyndigheden ikke suspendere eller forbyde en overførsel til en virksomhed eller myndighed, som er certificeret efter Privacy Shield. Tilsynsmyndigheden skal dog fortsat i fuld uafhængighed undersøge om den pågældende overførsel opfylder kravene i databeskyttelsesforordningen.[137]

3.2.6.2. Vurdering af, hvorvidt overførsler til USA ved anvendelse af SCC krænkede rettighederne i Charteret

Som det blev konkluderet i afsnit 3.2.5., er den dataansvarlige og databehandleren forpligtet til at opstille supplerende foranstaltninger til SCC'erne, hvis ikke tredjelandets lovgivning sikrer den væsentlige samme beskyttelse som i Unionen. På baggrund af konklusionerne vedrørende USA's lovgivning i afsnit 3.2.6.1. kan det konstateres, at USA ikke sikrer det væsentlige samme beskyttelsesniveau, som sikret i Unionen. Domstolens konklusion på fjerde, femte og tiende spørgsmål må derfor være, at en overførsel til USA på grundlag af SCC ikke tilsidesætter rettighederne i Charterets artikel 7, 8 og 47, når blot den dataansvarlige og databehandleren opstiller effektive supplerende foranstaltninger.

3.3. Sammenfatning af C-362/14, Schrems I og C-311/18, Schrems II

Domstolen konkluderede, at tilstrækkelighedsafgørelserne Safe Harbour og Privacy Shield var ugyldige. Angående Safe Harbour påpegede Domstolen i C-362/14, Schrems I, at Kommissionen ikke ved Safe Harbours vedtagelse havde foretaget tilstrækkelige konstateringer vedrørende den amerikanske lovgivning. Domstolen påpegede, at det i Safe Harbour hverken var konstateret, om der i USA

[137] C-311/18, Schrems II, præmis 156 og 157

var regler, der begrænsede indgreb i de registreredes grundlæggende rettigheder, eller om der forelå en effektiv domstolsbeskyttelse mod denne type indgreb.

I C-311/18, Schrems II undersøgte Domstolen gyldigheden af Privacy Shield, og hvorvidt den amerikanske lovgivning krænkede rettighederne sikret i Charterets artikel 7, 8 og 47. Herunder undersøgte Domstolen FISA sec. 702, som indeholder retsgrundlag, der kan bruges til at overvåge ikke amerikanske personer, men den indeholder ikke begrænsninger i beføjelsen til at overvåge. I PPD-28 var der dog indført begrænsninger for de amerikanske efterretningstjenesters mulighed for at indhente kommunikation, men indsamlingen gik stadig ud over, hvad der var strengt nødvendigt, idet indsamlingen blot skulle være 'så målrettet som muligt'. Domstolen undersøgte endvidere E.O 12333, som hjemlede begrænsninger for indsamling og behandling af personoplysninger. Det blev dog hertil fastslået, at disse begrænsninger alene var gældende for amerikanske statsborgere, og dermed ikke kunne afhjælpe de fremsatte kritikpunkter. Ligeledes blev det konstateret, at E.O. 12333 faktisk gav mulighed for, at USA allerede kunne tilgå personoplysninger, der var undervejs til USA ved at tilgå undersøiske kabler.

Det blev derfor konstateret, at problemerne i forhold til den amerikanske lovgivning, som Domstolen fandt i C-362/14, Schrems I, ikke blev afhjulpet, og derfor stadig udgjorde et problem i C-311/18, Schrems II. Lovgivningen i USA gør det dermed fortsat yderst problematisk at overføre oplysninger til USA på en måde, der er forenelig med databeskyttelsesforordningen sammenholdt med Charteret. Tilsvarende kritiserede Domstolen i C-362/14, Schrems I, at Safe Harbour gav amerikansk ret forrang, når den amerikanske lovgivning var i modstrid med Safe Harbour-principperne. Dette var dog ikke blevet afhjulpet i Privacy Shield, idet amerikansk lovgivning stadig havde forrang frem for principperne i Privacy Shield.

Domstolen fandt det ligeledes problematisk, at der ikke forelå en effektiv domstolsbeskyttelse i Safe Harbour. Ved vedtagelsen af Privacy Shield blev ombudsmanden indført med henblik på at afhjælpe problemet. Ombudsmanden var tiltænkt som en tilsynsmyndighed, der skulle være uafhængig af de amerikanske efterretningsmyndigheder. Domstolen konkluderede, at denne foranstaltning fortsat ikke var tilstrækkelig til at afhjælpe den manglende domstolsbeskyttelse. Dette skyldtes, at

ombudsmanden ikke var en uafhængig domstol, ligesom ombudsmanden ingen reelle beføjelser havde til at træffe afgørelser overfor efterretningstjenesterne. Konklusionen var derfor, at ombudsmanden ikke udgjorde et effektivt retsmiddel efter Charterets artikel 47. Det kan dertil undre, at Kommissionen mente, at de havde afhjulpet det manglende retsmiddel efter Charterets artikel 47 ved at indføre en ombudsmand, når denne ingen reel beføjelse havde til at træffe afgørelse.

Det er endvidere bemærkelsesværdigt, at Kommissionen indledningsvist vedtog Safe Harbour og Privacy Shield uden tilstrækkelig hensyntagen til den nationale lovgivning, særlig henset til begge afgørelser tillod den nationale lovgivning forrang frem for principperne i tilstrækkelighedsafgørelserne. Henset til at Kommissionen to gange har truffet en tilstrækkelighedsafgørelse vedrørende USA, som er blevet tilsidesat som ugyldige, fordi der ikke var taget tilstrækkelig stilling til den amerikanske lovgivning, kan dette stille spørgsmålstegn ved gyldigheden af andre tilstrækkelighedsafgørelser vedtaget af Kommissionen i henhold til både databeskyttelsesforordningen og databeskyttelsesdirektivet. Forhåbentligt har Kommissionen været særlig opmærksom på dette i deres løbende kontrol af tilstrækkelighedsafgørelserne i medfør af databeskyttelsesforordningens artikel 45, stk. 4.

Domstolen konkluderede både i C-362/14, Schrems I og i C-311/18, Schrems II, at et tilstrækkeligt beskyttelsesniveau er sikret, når tredjelandets beskyttelsesniveau i det væsentligste svarer til det, der er sikret i Unionen. Der kræves således ikke en beskyttelse, der er identisk med den, der er sikret i Unionen. Domstolen fremkom ikke med en nærmere definition af, hvad 'det væsentlige samme beskyttelsesniveau' er, og henviste til vurderingselementerne i databeskyttelsesforordningens artikel 45, stk. 2 og databeskyttelsesdirektivets artikel 25, stk. 2. Det er derfor fortsat vanskeligt for virksomheder og myndigheder at vide, hvornår der er sikret et væsentligt samme beskyttelsesniveau, når de ønsker at overføre oplysninger til et tredjeland, hvorom der ikke er truffet en tilstrækkelighedsafgørelse. Der skal tilsvarende sikres det væsentlige samme beskyttelsesniveau, når SCC anvendes som overførselsgrundlag. Domstolens konklusion på det fjerde, femte og tiende præjudicielle spørgsmål, må forstås således, at SCC kan anvendes til at sikre det væsentlige samme beskyttelsesniveau, såfremt der foretages effektive supplerende foranstaltninger, der går videre end bestemmelserne indeholdt i SCC.

Domstolen fremkom ikke med forslag til, hvilke supplerende foranstaltninger virksomheder og myndigheder kunne iagttage med henblik på at kompensere for den manglende beskyttelse. Det er således vanskeligt for myndigheder og virksomheder at overføre personoplysninger til usikre tredjelande. Virksomheder og myndigheder blev derfor stillet i en vanskelig situation, da det hidtidige overførselsgrundlag til USA blev underkendt, mens det ligeledes blev konstateret, at SCC uden implementering af supplerende foranstaltninger ikke altid er tilstrækkelige. Samtidig fik virksomheder og myndigheder ikke oplyst, hvilke supplerende foranstaltninger, der skal implementeres. Henset til at det er den dataansvarlige, der er ansvarlig for, at overførslen til et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, er det problematisk, at Domstolen ikke fremkom med yderligere bemærkninger hertil. Det er et betydeligt ansvar at pålægge virksomheder og myndigheder at vurdere, hvornår et væsentligt samme beskyttelsesniveau er sikret. Det overlades endvidere til de nationale tilsyn at afgøre, hvorvidt de dataansvarliges vurdering er korrekt, når Domstolen ikke har fremsat nærmere retningslinjer. Til trods for at tilsynene har mulighed for at anmode Databeskyttelsesrådet om en udtalelse, gælder denne adgang kun almengyldige spørgsmål eller spørgsmål, der har virkning i mere end én medlemsstat, jf. databeskyttelsesforordningens artikel 64, stk. 2. Det synes derfor urealistisk at forvente, at Databeskyttelsesrådet vil kunne give en udtalelse i alle tilfælde. Den dataansvarliges og tilsynets vurderinger kan derfor stadig resultere i en uensartet retsanvendelse i Unionen.

Databeskyttelsesrådet er efter C-311/18, Schrems II fremkommet med to henstillinger, Henstilling 01/2020[138] vedrørende supplerende foranstaltninger og Henstilling 02/2020[139] vedrørende væsentlige europæiske garantier. Henstilling 01/2020 har som den eneste været i høring, men var direkte anvendelig allerede fra offentliggørelse.[140] Henstillingerne har til formål at hjælpe virksomheder og myndigheder med at få klarhed over, hvilke supplerende foranstaltninger, de kan iværksætte, for at sikre et beskyttelsesniveau, der i det væsentligste svarer til det i Unionen. Disse vil nærmere gennemgås nedenfor i afsnit 4. Til trods for at Domstolen ikke erklærede de nugældende SCC ugyldige som overførselsgrundlag, har Kommissionen alligevel udarbejdet udkast til nye SCC. Dette udkast vil ligeledes nærmere gennemgås nedenfor i afsnit 5.

[138] Databeskyttelsesrådets Henstilling 01/2020 af 10. november 2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger. Herefter 'Henstilling 01/2020'
[139] Databeskyttelsesrådets Henstilling 02/2020 af 10. november 2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger. Herefter 'Henstilling 02/2020'
[140] EDPB: 41st Plenary session: EDPB adopts recommendations on supplementary measures following Schrems II

4. Supplerende foranstaltninger

Som Domstolen understregede i C-311/18, Schrems II, skal der i medfør af databeskyttelsesforordningen sammenholdt med Charteret sikres et beskyttelsesniveau, som i det væsentlige svarer til det, der er sikret i Unionen. I dommen blev det ikke nærmere specificeret, hvilke supplerende foranstaltninger en virksomhed eller myndighed som dataeksportør skal iværksætte. Selvom Domstolen ikke nærmere specificerede dette, er det dataeksportørens ansvar at sikre et tilstrækkeligt beskyttelsesniveau. Databeskyttelsesrådet har siden C-311/18, Schrems II vedtaget Henstilling 01/2020 med henblik på at hjælpe dataeksportører med at implementere effektive supplerende foranstaltninger.

4.1. 6-trins-vejledningen

I Henstilling 01/2020 er der opstillet en 6-trins-vejledning, der skal hjælpe dataeksportører med at overholde deres forpligtelser i medfør af databeskyttelsesforordningen og Charteret. Denne vil blive behandlet nedenfor.

4.1.1. Første og andet trin

Først og fremmest skal dataeksportøren klarlægge, hvilke overførsler denne har ud af Unionen. Dernæst skal dataeksportøren i andet trin klarlægge, hvilket overførselsgrundlag denne benytter til at overføre personoplysninger ud af Unionen. Såfremt dataeksportøren konstaterer, at overførslen sker på baggrund af en tilstrækkelighedsafgørelse efter databeskyttelsesforordningens artikel 45, skal der ikke træffes yderligere foranstaltninger i anledningen af overførslen. Dog skal dataeksportøren være opmærksom på, at tiltrækkelighedsafgørelser kan trækkes tilbage eller kendes ugyldig, ligesom det skete i Schrems-afgørelserne.[141] Såfremt databeskyttelsesforordningens artikel 46 om fornødne garantier er overførselsgrundlaget, kan det være nødvendigt at opstille supplerende foranstaltninger. Henstilling 01/2020 udpeger, at de vigtigste typer af overførselsværktøjer efter artikel 46 udgør overførsler på baggrund af SCC, bindende virksomhedsregler, adfærdskodekser, certificeringsmekanismer og ad hoc-kontraktbestemmelser. I dette speciale tages der udgangspunkt i SCC. De andre bestemmelser i artikel 46 behandles derfor ikke nærmere, jf. afsnit 1.1.

[141] Henstilling 01/2020, punkt 19

4.1.2. Tredje trin

Som tredje trin er det op til dataeksportøren at sætte sig ind i tredjelandets lovgivning og praksis. Dette er for at undersøge, hvorvidt lovgivningen eller praksissen i tredjelandet kan stride imod effektiviteten af de fornødne garantier efter databeskyttelsesforordningens artikel 46. Dataeksportøren bør sikre, at de rettigheder, der tildeles de registrerede efter databeskyttelsesforordningen, faktisk kan håndhæves i praksis og ikke hindres af lovgivningen i tredjelandet. Desuden skal dataeksportøren være opmærksom på, hvorvidt den registrerede har klageadgang i tredjelandet, således den registrerede sikres effektive retsmidler, jf. Charterets artikel 47. Ydermere skal dataeksportøren undersøge, hvorvidt der er lovgivning i tredjelandet, der hjemler adgang til, at tredjelandets offentlige myndigheder kan overvåge de registreredes oplysninger. I det tilfælde vil det være problematisk, såfremt overvågningen overstiger det, der er nødvendigt og proportionelt i et demokratisk samfund, jf. Charterets artikel 52. Databeskyttelsesrådet anfører, at det er op til dataeksportøren selv at vurdere, hvorvidt overvågningen overstiger dette.[142] Dataeksportøren vil dog formentlig sjældent have forudsætninger for at foretage denne vurdering.

Databeskyttelsesrådet har i Henstilling 02/2020 udledt fire europæiske væsentlige garantier, der er baseret på retspraksis fra Domstolen vedrørende Charterets artikel 7, 8, 47 og 52 samt reglerne om databeskyttelse. Når det skal vurderes, hvorvidt et tredjeland sikrer et beskyttelsesniveau, der i det væsentligste svarer til det, der er sikret i Unionen, udgør garantierne et bidrag til denne vurdering. Databeskyttelsesrådet fremhæver, at de væsentlige garantier er som følger: A) Behandlingen skal være baseret på klare, præcise og tilgængelige regler, B) nødvendighed og proportionalitet, hvad angår de legitime mål, der forfølges, skal godtgøres, C) der skal findes en uafhængig tilsynsmekanisme og D) der skal være effektive retsmidler til rådighed for de enkelte personer. I Henstilling 01/2020 henvises dataeksportøren til at finde hjælp i Henstilling 02/2020 til at klarlægge, hvorvidt der er noget i tredjelandets lovgivning, der hindrer de tilsagn, der ydes under overførselsværktøjet i databeskyttelsesforordningens artikel 46.[143]

[142] Henstilling 01/2020, punkt 36
[143] Henstilling 01/2020, punkt 39

Ikke nok med at dataeksportøren skal vurdere, hvorvidt tredjelandets offentligt tilgængelige lovgivning og praksis er i strid med de fornødne garantier, så fremhæver Databeskyttelsesrådet endvidere, at dataeksportøren skal vurdere tredjelandets ikke-offentligt tilgængelige lovgivning og praksis. Dataeksportørens vurdering af, hvorvidt lovgivningen modarbejder de fornødne garantier, vil formentlig være både særdeles kompliceret og omkostningstung, idet dataeksportøren ofte vil være nødsaget til at søge juridisk bistand i tredjelandet for at få et indblik i tredjelandets lovgivning. Vurderingen er kun gjort endnu mere kompliceret af, at dataeksportøren også skal vurdere ikke-offentligt tilgængelig lovgivning, og hvorvidt lovgivning er tvetydig eller mangelfuld. Det er noget nær umuligt for dataeksportøren i Unionen at vurdere, hvorvidt der er tilgængelig og ikke-tilgængelig lovgivning, der hjemler mulighed for, at tredjelandets offentlige myndigheder kan tilgå dataimportørens oplysninger uden dataimportørens viden. Det er desuden også noget nær umuligt for dataeksportøren at vurdere om tredjelandets offentlige myndigheder kan tilgå oplysningerne allerede i kommunikationskanalen, når oplysningerne er på vej til dataimportøren. Det er endvidere bemærkelsesværdigt, at det er dataeksportøren selv, der er ansvarlig for denne vurdering, når det fremgår af Schrems-afgørelserne, at Kommissionen har haft problemer med at foretage selvsamme vurdering af USA's lovgivning. Efter C-362/14, Schrems I forsøgte USA og Kommissionen at afhjælpe manglerne i USA's lovgivning, hvorefter Kommissionen traf en ny tilstrækkelighedsafgørelse. Kommissionen vurderede dermed, at USA's lovgivning sikrede et tilstrækkeligt beskyttelsesniveau, hvilket Domstolen underkendte i C-311/18, Schrems II.

4.1.3. Fjerde trin

Såfremt dataeksportøren finder, at tredjelandets lovgivning hindrer de fornødne garantier, skal dataeksportøren udpege og vedtage supplerende foranstaltninger, der effektivt afhjælper disse hindringer. De supplerende foranstaltninger, der kan iværksættes, opdeles i tre kategorier i henstillingen, som er henholdsvis tekniske, organisatoriske og yderligere kontraktmæssige foranstaltninger.[144]

Databeskyttelsesrådet fremhæver, at der vil være situationer, hvor udelukkende tekniske foranstaltninger vil gøre det muligt for dataeksportøren at forhindre offentlige myndigheder i tredjelande i at få adgang til de overførte personoplysninger. Dette vil især være i forbindelse med tredjelandes

[144] Henstilling 01/2020, punkt 45-47

offentlige myndigheders adgang til at overvåge, hvor yderligere kontraktmæssige og organisatoriske foranstaltninger ikke i sig selv vil være tilstrækkelige. De kontraktmæssige og organisatoriske foranstaltninger kan dog supplere de tekniske foranstaltninger og dermed styrke beskyttelsen af personoplysningerne.[145] Databeskyttelsesrådets eksempler på tekniske, organisatoriske og kontraktmæssige foranstaltninger, vil blive yderligere uddybet i afsnit 4.2. til 4.4.

Såfremt dataeksportøren finder, at der ikke kan implementeres supplerende foranstaltninger, som er effektive til at sikre et beskyttelsesniveau, der i det væsentligste svarer til det i Unionen, fremhæver Databeskyttelsesrådet, at dataeksportøren ikke må overføre personoplysninger til det pågældende tredjeland, ligesom dataeksportøren skal suspendere eller indstille allerede igangværende overførsler. Vælger dataeksportøren alligevel at fortsætte overførslen, skal dataeksportøren underrette den kompetente tilsynsmyndighed, der kan suspendere eller forbyde overførslen samt uddele bøder, såfremt tilsynsmyndigheden ligeledes vurderer, at der ikke kan iværksættes supplerende foranstaltninger.[146]

4.1.4. Femte og sjette trin

Databeskyttelsesrådet anfører i femte trin, at dataeksportøren skal indføre eventuelle formelle tiltag, eksempelvis indhente godkendelse fra tilsynsmyndigheden. Ved anvendelse af SCC, kan supplerende foranstaltninger dog indføres af dataeksportøren uden yderligere godkendelse fra tilsynsmyndighederne. I sjette trin anføres afslutningsvist, at foranstaltningerne og beskyttelsesniveauet i tredjelandet løbende skal vurderes, hvilket følger af princippet om ansvarlighed, som er en vedvarende forpligtelse.[147]

4.2. Tekniske foranstaltninger

Databeskyttelsesrådet opstiller indledningsvist eksempler på effektive tekniske foranstaltninger, som dataeksportøren kan indføre med henblik på at forhindre myndighederne i at få adgang til personoplysninger. Disse myndighedsindgreb kan ske på forskellige måder, herunder ved at tilgå kommunikationslinjer. Ved tilgangen via kommunikationslinjerne kan adgangen være passiv, hvor data blot

[145] Henstilling 01/2020, punkt 48
[146] Henstilling 01/2020, punkt 52-54
[147] Henstilling 01/2020, punkt 56 og 62

kopieres, eller aktiv, hvor myndighederne kan manipulere eller fjerne indhold. Derudover kan de offentlige myndigheder opnå tilgang til de overførte data, ved at myndigheden enten skjult eller ved anmodning udtrækker data fra dataimportøren.[148]

4.2.1. Scenarier, hvor der kan konstateres effektive foranstaltninger

Databeskyttelsesrådets første brugstilfælde omhandler effektiv kryptering, hvor dataimportøren ikke har adgang til ikke-krypteret data. For at sikre at denne beskyttelse er effektiv, påpeger Databeskyttelsesrådet, at krypteringen skal være robust mod modtagerlandets myndigheders tilgængelige ressourcer og tekniske kapaciteter, hvilket må antages at være en vanskelig vurdering. Det er ligeledes centralt for at sikre en effektiv kryptering, at dataimportøren ikke har adgang til krypteringsnøglerne. Dette skyldes især, at krypteringen og beskyttelsen kan blive illusorisk, såfremt tredjelandets myndigheder kan kræve krypteringsnøglerne udleveret. Det er eksempelvis tilfældet i USA, hvor FISA sec. 702 (50 USC § 1881a) forpligter amerikanske dataimportører til at tildele adgang til importerede personoplysninger, hvorunder krypteringsnøgler også kan være omfattet.[149]

Hvis de krypterede data udelukkende passerer gennem et usikkert tredjeland til et sikkert tredjeland, som eksemplet i det tredje brugstilfælde, skal dataeksportøren stadig være opmærksom på det usikre tredjelands lovgivning og offentlige myndigheders tekniske kapaciteter. I dette tilfælde vil transportkrypteringen eller ende-til-ende-kryptering udgøre en effektiv teknisk foranstaltning, såfremt denne form for kryptering giver en effektiv beskyttelse i forhold til de tilgængelige ressourcer myndighederne i det usikre tredjeland har. I dette tilfælde skal nøglerne blandt andet forvaltes pålideligt af dataeksportøren, og være uden for myndighederne i det usikre tredjelands rækkevidde.[150]

Databeskyttelsesrådet anfører endvidere i fjerde brugstilfælde, at det vil være tilstrækkeligt at implementere ende-til-ende-kryptering, og dermed give dataimportøren adgang til ikke-krypteret data i de tilfælde, hvor dataimportøren er underlagt en særlig tavshedspligt, som fritager denne fra at overgive oplysninger til myndighederne i tredjelandet. Dette skyldes, at myndighederne dermed ikke får

[148] Henstilling 01/2020, punkt 75
[149] Henstilling 01/2020, punkt 76 og 79
[150] Henstilling 01/2020, punkt 84

mulighed for at tilgå data, selvom dataimportøren har adgang til krypteringsnøglen. En sådan beskyttet modtager kan eksempelvis være en dataimportør, som leverer lægebehandling eller juridiske tjenesteydelser.[151]

I andet brugstilfælde fremhæver Databeskyttelsesrådet, at når data er effektivt pseudonymiseret, vil det som udgangspunkt ikke være muligt at identificere den registrerede. Databeskyttelsesrådet påpeger, at såfremt der anvendes pseudonymisering, skal dataeksportøren være særlig opmærksom på, at der kan være faktorer ved den registrerede, hvor det ikke vil være muligt at pseudonymisere data således, at den registrerede ikke kan identificeres.[152] Hertil bemærkes, at pseudonymiserede oplysninger, trods de ikke er personhenførbare, stadig betragtes som personoplysninger.[153]

Efter femte brugstilfælde kan det også udgøre en supplerende teknisk foranstaltning, at der sker delt behandling mellem flere parter ved at oplysningerne opdeles, så de ikke hver for sig udgør læsbare data. Herved samler dataeksportøren data fra samarbejdspartnere, og først på dette tidspunkt bliver data læsbare på en sådan måde, at oplysningerne kan henføres tilbage til den registrerede. På den måde vil det dermed være uden betydning, såfremt dataimportøren bliver pålagt at udlevere oplysningerne til en myndighed i tredjelandet. I den pågældende situation skal dataeksportøren dog sikre sig, at der ikke er et samarbejde mellem de offentlige myndigheder i de tredjelande, hvor deloplysningerne overføres til, ligesom dataeksportøren skal sikre sig, at det ikke er muligt for myndigheden i ét tredjeland individuelt at indsamle data fra flere lande.[154] En sådan foranstaltning vil formentlig være uforholdsmæssig dyr og kompliceret for dataeksportøren at undersøge og administrere, ligesom det formentlig ikke vil være praktisk muligt i alle sammenhænge at anvende en sådan løsning, da mange databehandlinger kræver, at der faktisk er adgang til det samlede datasæt.

4.2.2. Scenarier, hvor der ikke kan konstateres effektive foranstaltninger

Der opstilles ligeledes scenarier, hvor Databeskyttelsesrådet ikke kan forestille sig, at der findes effektive tekniske foranstaltninger, der kan sikre et tilstrækkeligt beskyttelsesniveau. I sjette

[151] Henstilling 01/2020, punkt 85
[152] Henstilling 01/2020, punkt 80 og 81
[153] Datatilsynet: Hvad er en personoplysning?
[154] Henstilling 01/2020, punkt 86

brugstilfælde overfører dataeksportøren oplysninger til en cloud-leverandør, således denne, på dataeksportørens anvisninger, kan behandle personoplysninger i et tredjeland. I eksemplet har cloud-leverandøren behov for ikke-krypterede data for at kunne udføre den opgave, som dataeksportøren har tildelt den, ligesom tredjelandets lovgivning giver de offentlige myndigheder mulighed for at tilgå de overførte data ud over, hvad der er nødvendigt og proportionelt i et demokratisk samfund. Her er Databeskyttelsesrådet ikke i stand til at forestille sig, at der på nuværende tidspunkt med det nuværende tekniske niveau, kan være tekniske foranstaltninger, der kan forhindre, at de registreredes rettigheder krænkes.[155] Det vil således ikke være muligt at anvende en cloud-leverandør, der er placeret i USA eller et andet usikkert tredjeland med lignende lovgivning, såfremt cloud-leverandøren har behov for ikke-krypterede data.

I syvende brugstilfælde gøres personoplysninger tilgængelige for enheder i tredjelandet, eksempelvis i en koncerns datterselskab placeret i et tredjeland, således data kan bruges til fælles forretningsmæssige formål. Her er det nødvendigt, at dataimportøren har adgang til ikke-krypterede data, førend denne kan levere tjenesteydelser eller behandle data efter eget formål. Hvis offentlige myndigheder i det pågældende tredjeland har beføjelser, der går videre, end hvad der er nødvendigt og proportionelt i et demokratisk samfund, kan Databeskyttelsesrådet ikke forestille sig effektive tekniske foranstaltninger, der kan sikre de registreredes rettigheder. Det vil derfor heller ikke være tilstrækkeligt, at der sker transportkryptering og kryptering af data i hvile, netop fordi myndigheder i det pågældende tredjeland har beføjelser til i vidt omfang at tilgå data.[156]

4.3. Yderligere kontraktmæssige foranstaltninger

SCC indeholder kontraktuelle forpligtelser, der alene gælder for aftaleparterne. For at sikre de fornødne garantier, kan det være nødvendigt for parterne at supplere standardbestemmelserne med yderligere kontraktmæssige foranstaltninger. Endvidere ses de kontraktuelle forpligtelser udvidet i udkastet til nye SCC. Databeskyttelsesrådet fremhæver dog, at når SCC ikke binder myndighederne i tredjelandet, bør parterne kombinere SCC med andre tekniske og organisatoriske foranstaltninger.[157]

[155] Henstilling 01/2020, punkt 88
[156] Henstilling 01/2020, punkt 90 og 91
[157] Henstilling 01/2020, punkt 92

Databeskyttelsesrådet fremkommer med det eksempel, at det kontraktmæssigt kan aftales, at en teknisk foranstaltning, som identificeret i afsnit 4.2., skal anvendes. Det kan endvidere aftales, at der skal være øget gennemsigtighed. Dette sker eksempelvis ved, at dataimportøren forpligter sig til at undersøge, hvorvidt de offentlige myndigheder i tredjelandet har mulighed for at tilgå de overførte oplysninger. Dataimportøren kan således forpligtes til at opregne de love, forskrifter eller lignende, som giver hjemmel hertil samt forpligte sig til at give besked til dataeksportøren, såfremt de får anmodning fra offentlige myndigheder om adgang til de overførte personoplysninger. En anden kontraktmæssig foranstaltning kan være, at dataimportøren erklærer, hvad denne har gjort for at forhindre, at offentlige myndigheder opnår adgang til data, herunder at de ikke bevidst har oprettet bagdøre eller andet, som kan bruges af de offentlige myndigheder til at få adgang til personoplysningerne. I den forbindelse kan dataimportøren forpligtes til at anfægte myndighedernes anmodning om adgang til personoplysninger.[158]

Det kan endvidere aftales, at dataeksportøren udfører yderligere kontroller og inspektioner af dataimportørens behandlingsaktivitet, ligesom dataimportøren skal bidrage hertil og dokumentere behandlingsaktiviteten grundigt. Det kan yderligere aftales, at dataimportøren forpligter sig til omgående at give besked til dataeksportøren ved manglende overholdelse af kontrakten, herunder såfremt der sker ændringer i tredjelandets lovgivning, som forhindrer overholdelse af kontrakten.[159] Afslutningsvist fremhæves, at dataimportøren og dataeksportøren kan forpligte sig til at orientere den registrerede om behandlingen og bistå denne med at udøve sine rettigheder i anledning heraf.[160]

4.4. Organisatoriske foranstaltninger

Databeskyttelsesrådet fremhæver, at der også kan vedtages en række organisatoriske foranstaltninger. Disse kan yde bidrag til, at dataeksportøren bliver bevidst om de risici, der er ved, at tredjelandets myndigheder har mulighed for at få adgang til overførte personoplysninger, samt sikre sammenhæng i beskyttelsen af personoplysninger under hele behandlingsforløbet. Dog vil de organisatoriske

[158] Henstilling 01/2020, punkt 97, 99, 103 og 112
[159] Henstilling 01/2020, punkt 105
[160] Henstilling 01/2020, punkt 118 og 120

foranstaltninger ikke kunne stå alene, men kan anvendes som supplement til de kontraktmæssige og/eller tekniske foranstaltninger for at sikre de fornødne garantier.[161]

Organisatoriske foranstaltninger kan bestå af interne politikker, metoder og standarder, herunder interne ansvars- og rollefordelinger mellem dataeksportøren og dataimportøren. Dette kan eksempelvis ske ved nedsættelse af en særskilt afdeling eller gruppe medarbejdere, som håndterer alle anmodninger fra offentlige myndigheder på en struktureret og ensrettet måde. Det vil være nødvendigt for dataeksportøren og dataimportøren at aftale, hvordan overførslerne skal ske, så disse lever op til princippet om dataminimering, herunder ved at begrænse adgangen til oplysningerne til en begrænset kreds af ansatte. Det kunne ligeledes omfatte særlige uddannelse af det relevante personale, eksempelvis ved anvendelse af bedste praksisser, der har til formål at sikre, at den officielt bedste, anerkendte fremgangsmåde anvendes. Dataeksportøren bør endvidere organisere sig på en sådan måde, at der bliver øget gennemsigtighed og ansvarlighed, herunder at oplysninger om anmodninger som udgangspunkt videregives til den registrerede.[162]

[161] Henstilling 01/2020, punkt 122
[162] Henstilling 01/2020, punkt 124, 125, 127 og 131

5. Udkast til nye SCC

Selvom Domstolen ikke fandt grundlag for at erklære de nugældende SCC ugyldige, har Kommissionen i lyset af udviklingen på området fundet, at der et behov for at udarbejde nye SCC, der skal erstatte de nugældende SCC. Se nærmere om Kommissionens begrundelse herom i afsnit 2.8. Det tyder på, at det i de nugældende SCC ikke har været klart nok for dataeksportøren, der anvender disse som overførselsgrundlag, at dataeksportøren er ansvarlig for at sikre et beskyttelsesniveau, der i det væsentligste svarer til det, der er sikret i Unionen, og at det i den forbindelse kan være nødvendigt at lave supplerende foranstaltninger.

Aftaleteksten i udkastet til nye SCC er opdelt i fire moduler: 1) Dataansvarlig til dataansvarlig, 2) dataansvarlig til databehandler, 3) databehandler til databehandler og 4) databehandler til dataansvarlig. Første modul vil således erstatte SCC af 2001 og SCC af 2004. Andet modul vil erstatte SCC af 2010. Tredje- og fjerde modul er nyskabelser i forhold til de nugældende SCC og giver mulighed for et mere moderniseret og fleksibelt overførselsgrundlag, som er nærmere gennemgået i afsnit 2.8.

Nogle af standardbestemmelserne i udkastet til nye SCC vil være gældende uanset hvilket modul, der anvendes, og derfor uanset hvilken type af overførsel, der foretages. Andre bestemmelser i udkastet til nye SCC varierer i ordlyden alt efter hvilket modul, der anvendes, men er i det væsentlige indholdsmæssigt tilsvarende. I disse standardbestemmelser består ændringen primært i forskellen på henholdsvis den dataansvarlige og databehandlerens forskellige forpligtigelser i forbindelse med en overførsel.

I det nedenstående vil udkastet til nye SCC nærmere analyseres med henblik på at undersøge, hvordan Schrems-afgørelserne har påvirket udformning af disse standardbestemmelser. Derfor vil udelukkende ændringerne som relaterer sig til resultatet i Schrems-afgørelserne blive gennemgået i forbindelse med undersøgelsen af udkastet til nye SCC sammenlignet med de nugældende SCC. Undersøgelsen vil således primært beskæftige sig med de supplerende foranstaltninger, som parterne skal overveje, samt hvilke overvejelser, der skal gøres i forbindelse med vurderingen af tredjelandets lovgivning. Der vil derfor ikke blive foretaget en nærmere analyse af samtlige standardbestemmelser i udkastet.

5.1. Formålet og rækkevidden af SCC

Afsnit 1 i udkastet til nye SCC fastsætter blandt andet formålet og rækkevidden af disse standardbestemmelser. Det fremgår af afsnit 1, standardbestemmelse 1, litra c, at disse bestemmelser fastsætter fornødne garantier, rettigheder for de registrerede, samt effektive retsmidler. Det fremgår ligeledes af bestemmelsen, at disse SCC ikke er til hinder for, at parterne tilføjer yderligere foranstaltninger til deres kontrakt. Det fremgår endvidere af betragtning 3 i udkastet til afgørelsesbeslutningen om nye SCC, at dataansvarlige og databehandlere opfordres til at implementere yderligere foranstaltninger, der supplerer beskyttelsen i SCC. Dette er i overensstemmelse med databeskyttelsesforordningens præambelbetragtning 109, der ligeledes anfører, at dataansvarlige og databehandlere bør tilskyndes til at give yderligere garantier gennem kontraktmæssige forpligtelser, der supplerer beskyttelsen i SCC.

Til sammenligning fastsætter SCC af 2001, SCC af 2004 og SCC af 2010 også, at der er mulighed for at aftale yderligere betingelser til parternes kontrakt. Det fremgår af betragtningerne til SCC af 2001, at dataeksportøren og dataimportøren frit kan tilføje enhver anden kommerciel bestemmelse, hvis de anser det for at have betydning for kontrakten.[163] I SCC af 2004 fremgår det, at bestemmelserne ikke forhindrer parterne i, om nødvendigt, at tilføje supplerende forretningsbestemmelser.[164] Det fremgår ligeledes af SCC af 2010, at parterne ikke er forhindret i at tilføje bestemmelser om forretningsmæssige spørgsmål til deres kontrakt, hvis det er nødvendigt, så længe dette ikke strider mod indholdet i SCC.[165]

Af ordlyden i de nugældende SCC fremgår det derfor i højere grad som en mulighed at aftale yderligere foranstaltninger til parternes kontrakt, hvis parterne finder det hensigtsmæssigt i forretningssammenhæng, og ikke som en opfordring til at sikre de registreredes rettigheder, hvilket er tilfældet i udkastet til nye SCC. Ordlyden af SCC af 2001, SCC af 2004 og SCC af 2010 er således indholdsmæssigt rettet mod parternes kommercielle interesser og ikke mod beskyttelsen af de registreredes rettigheder.

[163] SCC af 2001, betragtning 5
[164] SCC af 2004, bilag "standardkontrakt II", punkt VII
[165] SCC af 2010, bilag "Standardkontraktbestemmelser (registerfører)", standardbestemmelse 10

Tilføjelsen i udkastet til nye SCC om, at parterne opfordres til at implementere yderligere foranstaltninger, der supplerer beskyttelsen i SCC for at sikre de registreredes rettigheder, er i overensstemmelse med Domstolens konklusion i C-311/18, Schrems II. Som nærmere beskrevet i afsnit 3.2.5., anførte Domstolen, at SCC, henset til deres karakter, ikke kan garantere beskyttelse i videre omfang end kontraktretligt, hvorfor det kan være nødvendigt for dataeksportøren og dataimportøren at vedtage supplerende foranstaltninger for at sikre opretholdelsen af et beskyttelsesniveau, der i det væsentligste svarer til det, der er sikret i Unionen.[166]

5.2. Behandlingssikkerhed og supplerende foranstaltninger

Nedenfor vil SCC'ernes krav om behandlingssikkerhed bliver gennemgået. Herefter vil parternes mulighed for at implementere tekniske og organisatoriske foranstaltninger i forbindelse med anvendelsen af SCC, også nærmere analyseres.

5.2.1. De almindelige krav til behandlingssikkerhed

Der er til de tre første moduler i afsnit 2, standardbestemmelse 1 i udkastet til nye SCC indskrevet nogle databeskyttelsesretlige principper, herunder princippet om transparens, nøjagtighed, dataminimering, opbevaringsbegrænsning, samt behandlingssikkerhed, som parterne skal overholde i forbindelse med en overførsel af personoplysninger til et tredjeland.

Særligt afsnittet om behandlingssikkerhed er relevant at analysere yderligere, idet flere af de eksempler, som fremgår af Henstilling 01/2020 om supplerende foranstaltninger, herunder kryptering og pseudonymisering, går igen i udkastet til nye SCC. Kravene til behandlingssikkerheden fremgår af alle fire moduler, og ordlyden afhænger af, hvilket modul der anvendes. Dog består forskellene i modulernes formulering primært af den naturlige forskel, der er på henholdsvis den dataansvarliges og databehandlerens rolle i forbindelse med en overførsel. Ud over dette er kravene til behandlingssikkerheden indholdsmæssigt ens.

Indledningsvist fremgår det af afsnittet om behandlingssikkerhed i udkastet til nye SCC, at der skal implementeres tekniske og organisatoriske foranstaltninger for at sikre et tilstrækkeligt

[166] C-311/18, Schrems II, præmis 133 og 134

beskyttelsesniveau. I denne vurdering skal parterne blandt andet tage risiciene, formålet med behandlingen og konteksten i betragtning, og særligt overveje at anvende kryptering, anonymisering og pseudonymisering ved overførsler. Parterne skal endvidere føre løbende kontrol med sikkerheden. Ligeledes fremgår det, at parterne i tilfælde af et databrud skal iværksætte passende foranstaltninger for at begrænse og modvirke effekten bruddet. Det andet og tredje modul, der omhandler overførsler til databehandlere, fastsætter desuden, at dataeksportøren bør have enerådig besiddelse af de supplerende oplysninger, der gør data personhenførbar, såfremt dette er muligt.

I SCC af 2001 fremgår det, at kravene til behandlingssikkerhed er, at der skal træffes tekniske og organisatoriske sikkerhedsforanstaltninger, der svarer til de risici, som behandlingen indebærer. Som eksempel på en risiko benævnes udelukkende ikke-autoriseret indsigt.[167] En lignende ordlyd fremgår af SCC af 2004, hvor det fremgår, at parterne opfordres til at træffe tekniske og organisatoriske foranstaltninger.[168] I SCC af 2004 er der dog uddybet flere mulige risici, der kan være i forbindelse med en behandling. Formuleringen om, at parterne skal træffe tekniske og organisatoriske foranstaltninger, er en nedskrivning af det dagældende databeskyttelsesdirektivs artikel 17, stk. 1, som nu er videreført i databeskyttelsesforordningens artikel 5, litra f.

I SCC af 2010 fremgår det ligeledes, at parterne skal iværksætte tekniske og organisatoriske foranstaltninger. Det fremgår dog af SCC af 2010, modsat SCC af 2001 og SCC af 2004, at dette skal ske, når tredjelandet ikke frembyder et tilstrækkeligt sikkerhedsniveau i form af en tilstrækkelighedsafgørelse.[169] Endvidere skal der ved fastsættelse af tekniske og organisatoriske foranstaltninger tages hensyn til databeskyttelseslovgivningen, det aktuelle tekniske niveau, og omkostningerne ved implementeringen.

Dette kan derfor fortolkes således, at det i de nugældende SCC udelukkende er i SCC af 2010, det fremgår klart, at standardbestemmelserne ikke altid yder tilstrækkelig beskyttelse, men at det kan være nødvendigt at implementere yderligere foranstaltninger for at sikre et tilstrækkeligt beskyttelsesniveau. SCC af 2010 kan dog også fortolkes således, at formuleringen er en mere fyldestgørende

[167] SCC af 2001, tillæg 2, punkt 4
[168] SCC af 2004, bilag A, punkt 4
[169] SCC af 2010, betragtning 12

nedskrivning af databeskyttelsesdirektivets artikel 17, stk. 1, og at det derfor heller ikke i SCC af 2010 klart fremgår, at parterne bør overveje at indføre yderligere supplerende foranstaltninger, netop fordi data føres ud af Unionen. SCC af 2010 erstatter nemlig Kommissionens beslutning af 27. december 2001 (2002/16/EF),[170] hvor dennes betragtning 11 svarer til betragtning 12 i SCC af 2010. Således har det tilsyneladende ikke været et udslag af udviklingen, at databeskyttelsesdirektivets artikel 17 er mere udførligt indført i SCC af 2010, end det var tilfældet i SCC af 2001 og SCC af 2004, netop fordi SCC af 2002 anvendte samme formulering som i SCC af 2010. Af den årsag bør den mere udførlige nedskrivning af direktivets artikel 17, stk. 1 formentlig ikke fortolkes således, at Kommissionen har haft øget fokus på, at netop fordi data føres ud af Unionen, bør der iværksættes yderligere supplerende foranstaltninger.

I udkastet til afgørelsesbeslutningen om nye SCC er det tilføjet og betydeligt mere uddybet end i de nugældende SCC, at der skal implementeres supplerende foranstaltninger, når data skal føres ud af Unionen. Det ses derfor, at denne tilføjelse i udkastet til afgørelsesbeslutningen om nye SCC er resultatet af C-311/18, Schrems II, hvor Domstolen kom med denne konklusion. Se mere herom i afsnit 5.2.2.

5.2.2. Tillæg med tekniske og organisatoriske foranstaltninger

I udkastet til nye SCC tillæg 2, skal parterne anføre kravene til de tekniske og organisatoriske foranstaltninger, som de implementerer. Her oplistes eksempler på mulige foranstaltninger og kravene hertil, som parterne bør overveje at implementere i forbindelse med behandlingssikkerhed. Heriblandt anføres først pseudonymisering og kryptering. Derudover fremgår det, at parterne skal sikre en løbende gennemgang af programmers modstandsdygtighed og integritet, ligesom effektiviteten af de tekniske og organisatoriske foranstaltninger løbende skal testes og evalueres. Ydermere fremhæves, at parterne bør overveje, hvilke foranstaltninger de kan implementere for at sikre data særligt i forbindelse med overførsler og opbevaring. Tillægget i udkastet til nye SCC lægger således op til en detaljeret beskrivelse af foranstaltningerne. Databeskyttelsesrådet har dog hertil udtalt kritik af

[170] Kommissionens beslutning af 27. december 2001 (2002/16/EF). Herefter 'SCC af 2002'

tillæggets generelle karakter, og anfører at det bør tydeliggøres, at kun relevante foranstaltninger skal anføres.[171]

I de nugældende SCC, er det udelukkende i SCC af 2010, der er lavet et tillæg, hvor parterne skal notere de supplerende foranstaltninger, de har implementeret. Dette tillæg er dog ikke så udførligt som i udkastet til nye SCC. Årsagen til det mere udførlige tillæg med mulighed for, at parterne kan notere, hvilke tekniske og organisatoriske foranstaltninger, der skal implementeres, samt kravene hertil, må findes i Domstolens konklusion i C-311/18, Schrems II. Heri konkluderede Domstolen, som beskrevet tidligere, at det er parterne selv, der er ansvarlige for at vurdere, hvorvidt det er nødvendigt at opstille supplerende foranstaltninger i SCC'erne, og i givet fald hvilke, med henblik på at sikre, at beskyttelsesniveauet ikke undermineres.[172]

5.3. Lovgivningen i tredjelandet

Udkastet til nye SCC, afsnit 2, standardbestemmelse 2 omhandler tredjelandets lovgivnings påvirkning af overholdelsen af standardbestemmelserne, og finder ens anvendelse på alle moduler. Fjerde modul indeholder dog den modifikation, at bestemmelsen kun gælder, når en databehandler i Unionen kombinerer personoplysninger modtaget fra dataansvarlige i tredjelandet med personoplysninger indsamlet af databehandleren i Unionen. Bestemmelsen finder således ikke anvendelse, når databehandleren udelukkende behandler personoplysninger modtaget fra dataansvarlige i et tredjeland.

Afsnit 2, standardbestemmelse 2, litra a-f angiver forpligtelser, som parterne skal garantere, når oplysninger skal overføres til tredjelande. Først og fremmest skal parterne garantere, at de ikke har grund til at tro, at lovgivning i tredjelandet forhindrer dataimportøren i at opfylde de forpligtelser, der er angivet i SCC. En væsentlig tilsvarende bestemmelse eksisterer også i de nugældende SCC af 2001,[173] SCC af 2004,[174] og SCC af 2010.[175]

[171] EDPB – EDPS Joint Opinion 2/2021, punkt 131
[172] C-311/18, Schrems II, præmis 134
[173] SCC af 2001, standardbestemmelse 5 a
[174] SCC af 2004, bilag 2, punkt 2 c
[175] SCC af 2010, standardbestemmelse 5 b

Parterne skal endvidere i udkastet til nye SCC garantere, at tredjelandets lovgivning ikke tillader offentlige myndigheder en videre adgang, end hvad der er nødvendigt og proportionelt i et demokratisk samfund.[176] En tilsvarende bestemmelse fremgår ligeledes af de nugældende SCC af 2001[177] og SCC af 2010.[178] Som tidligere beskrevet i afsnit 4.1.2., fremgår en lignende formulering af Henstilling 01/2020, hvorefter parterne skal undersøge, hvorvidt myndighedernes adgang til persondata går videre, end hvad der er nødvendigt og proportionelt i et demokratisk samfund. Som anført i samme afsnit, er det kritisabelt, at parterne selv skal vurdere, hvor grænsen går for, hvad der er nødvendigt og proportionelt i et demokratisk samfund. Garantien for at tredjelandets lovgivning ikke tillader offentlige myndigheder en videre adgang, end hvad der er nødvendigt og proportionelt i et demokratisk samfund, er en løbende forpligtelse, og dataeksportøren skal derfor straks underrettes, såfremt dataimportøren har grund til at tro, at den ikke længere kan leve op til forpligtelserne.[179]

I udkastet til nye SCC er der sammenlignet med de nugældende SCC kommet et øget fokus på, hvad parterne skal undersøge i vurderingen af, hvorvidt lovgivningen i tredjelandet umuliggør overholdelsen af standardbestemmelserne. Det fremgår både af udkastet til afgørelsesbeslutningen om nye SCC og udkastet til nye SCC, at parterne forinden en overførsel af data til et usikkert tredjeland bør tage alle konkrete omstændigheder i betragtning med henblik på at undersøge, hvorvidt der er lovgivning i tredjelandet, der umuliggør, at dataimportøren kan leve op til standardbestemmelserne. De konkrete omstændigheder, der bør tages i betragtning, er alle de supplerende tekniske og organisatoriske foranstaltninger, der kan tænkes iværksat for at gøre det muligt for dataimportøren at overholde standardbestemmelserne til trods for tredjelandets lovgivning. Det fremgår ligeledes af udkastet til afgørelsesbeslutningen om nye SCC, at førend de fornødne garantier er sikret, er det en betingelse, at beskyttelsesniveauet stadig i det væsentligste svarer til det, der er sikret i Unionen. Endvidere skal dataimportøren garantere, at denne har gjort sit bedste for at stille relevante oplysninger til rådighed for dataeksportøren i denne sammenhæng.[180]

[176] Udkastet til nye SCC, afsnit 2, standardbestemmelse 2, punkt a
[177] SCC af 2001, standardbestemmelse 5 b, jf. tillæg 2
[178] SCC af 2010, blandt andet af artikel 4, stk. 1, litra a
[179] Udkast til nye SCC, afsnit 2, standardbestemmelse 2, litra e. Lignende forpligtelse i SCC af 2001, standardbestemmelse 5, litra a, SCC af 2004, bilag "standardkontrakt II" og SCC af 2010, standardbestemmelse 5, litra a og b
[180] Udkast til afgørelsesbeslutning om nye SCC, betragtning 11, 19, 20 og 21 samt udkast til nye SCC, afsnit 2, standardbestemmelse 2, litra b og c

5.4. Myndighedsanmodninger

Det er en overvejende ny bestemmelse, at parterne bør tage hensyn til tredjelandets myndigheders mulighed for adgang til personoplysninger. I udkastet til nye SCC, afsnit 2, standardbestemmelse 3, angives det, at dataimportøren straks skal give dataeksportøren og, hvor muligt, den registrerede besked, såfremt der kommer en anmodning om oplysninger fra en myndighed. Ligeledes skal dataimportøren give besked, hvis denne er blevet opmærksom på, at myndigheden af egen drift har fået adgang til personoplysningerne. Samme forpligtigelse fremgår af den nugældende SCC af 2010, standardbestemmelse 5, litra d. En tilsvarende bestemmelse ses ikke at fremgå udtrykkeligt i SCC af 2001 og SCC af 2004.

I udkastet til nye SCC, afsnit 2, standardbestemmelse 3.1 uddybes yderligere, at i tilfælde af at dataimportøren har forbud mod at give dataeksportøren besked om en myndighedsadgang eller -anmodning, skal dataimportøren kommunikere og dokumentere så meget som denne efter tredjelandets lov har adgang til. Forpligtelsen til at underrette om en myndigheds adgang eller anmodning herom kan dermed blive illusorisk, såfremt der er et sådant forbud i tredjelandets lovgivning. Dette kan være problematisk for den registreredes rettigheder samt dataeksportørens mulighed for at opnå indsigt og vurdering af dataimportørens mulighed for overholdelse af standardbestemmelserne. Dog er et sådant forbud i tredjelandets lovgivning i nogle tilfælde nødvendigt, herunder især i forbindelse med strafferetlig forfølgning.

Det fremgår yderligere af udkastet til nye SCC, afsnit 2, standardbestemmelse 3.2, at dataimportøren skal undersøge legaliteten af de myndighedsanmodninger, den modtager. Dataimportøren skal således udtømme enhver mulighed for at anfægte anmodningen, og derved udlevere så lidt data som muligt. Dette har sammenhæng med princippet om dataminimering, som også gennemgående er blevet et mere fremhævet princip i udkastet til nye SCC. Dataimportøren er desuden forpligtet til at dokumentere, hvad denne har gjort for at anfægte anmodningen. Princippet om dataminimering er naturligvis også gældende i de nugældende SCC, men med den særskilte bestemmelse i udkastet til nye SCC er det blevet særligt understreget, at dataimportøren er forpligtet til at foretage en vidtgående efterprøvelse af anmodningen, og hvorvidt denne er lovlig i forhold til tredjelandets lovgivning.

6. Cases

I dette afsnit vil der foretages en gennemgang af tre cases, som er udarbejdet af Bech-Bruun advokatpartnerselskab i forbindelse med Match-making samarbejdet. Disse cases er baseret på konkrete problemstillinger, som Bech-Bruun advokatpartnerselskab har rådgivet dataeksportører om. Disse cases vil analyseres med henblik på at undersøge, hvorvidt konklusionerne fra Schrems-afgørelserne, samt Henstilling 01/2020 og udkastet til nye SCC faktisk giver virksomheder og myndigheder svar på, hvordan de skal forholde sig, såfremt de ønsker at overføre persondata ud af Unionen.

6.1. Case 1

Den første case er som følger:

> *Virksomhed A, der er etableret i Danmark og foretager kliniske forsøg, overfører kliniske billeder til Virksomhed B, der er etableret i USA, med henblik på analyse af selve de kliniske billeder. Overførslen sker på baggrund af EU-Kommissionens standardkontraktbestemmelser.*

I første case overføres der kliniske billeder til det usikre tredjeland USA. De overførte oplysninger er helbredsoplysninger, jf. databeskyttelsesforordningens artikel 9, stk. 1, idet kliniske billeder er billeder af en persons sygdomstilfælde med henblik på blandt andet forskning og behandling.

6-trins-vejledningen i Henstilling 01/2020 vil anvendes med henblik på at undersøge, hvordan en virksomhed, eksempelvis Virksomhed A, konkret skal forholde sig i en sådan situation. Vejledningens første og andet trin er iagttaget af Virksomhed A, idet virksomheden har været opmærksom på, hvilke overførsler denne har ud af Unionen, og hvilket overførselsgrundlag, der benyttes.

6.1.1. Lovgivningen i USA

Som tredje trin er det, som beskrevet i afsnit 4.1.2., op til dataeksportører at sætte sig ind i tredjelandets lovgivning og praksis. I det konkrete tilfælde har Domstolen lavet en del af forarbejdet for dataeksportører, der ønsker at overføre personoplysninger til USA, idet de ved Schrems-afgørelserne har klarlagt den relevante lovgivning i USA på tidspunktet for domsafsigelserne. Det blev her blandt

andet konstateret, at PPD-28 tillader myndighedernes masseindsamling af oplysninger uden identifikator til at målrette indsamlingen, ligesom E.O. 12333 tillader, at der gives adgang til oplysninger, som er undervejs til USA. Se nærmere herom i afsnit 3.2.6.1. Det er Virksomhed A's ansvar at klarlægge, hvorvidt der efterfølgende er fremkommet ny relevant lovgivning på området.

Ved anvendelsen af de nye SCC, såfremt de bliver vedtaget i overensstemmelse med udkastet, er dataeksportører hjulpet yderligere på vej i standardbestemmelse 2. Heri nævnes, at der i vurderingen skal tages stilling til tredjelandets lovgivning såvel som alle relevante oplysninger ved overførslen, herunder hvad parterne skal være særligt opmærksomme på, når de garanterer, at de kan overholde standardbestemmelserne sammenholdt med de supplerende foranstaltninger, der kan iværksættes. Som eksempler på de specifikke omstændigheder, som kan have indflydelse på overførslen, anføres blandt andet konteksten, hyppigheden, varigheden og formålet med behandlingen. De samme krav til vurderingen gør sig gældende for de nugældende SCC, men Kommissionen og Databeskyttelsesrådet yder nu mere vejledning i udkastet til nye SCC og Henstilling 01/2020. Se nærmere herom i afsnit 5.3. Selvom både udkastet til nye SCC samt Henstilling 01/2020 yder vejledning til dataeksportører om, hvilke vurderinger, der skal foretages, før der kan ske overførsel, så er de vurderinger, som Kommissionen og Databeskyttelsesrådet pålægger dataeksportørerne at foretage, yderst vidtgående og komplicerede. Der er desuden ingen hjælp at hente hos Kommissionen og Databeskyttelsesrådet til, hvordan disse vurderinger reelt kan foretages i praksis for at simplificere vurderingerne.

I vurderingen af tredjelandets lovgivning vil det typisk være nødvendigt for dataeksportører at indhente juridisk bistand, eventuelt fra tredjelandet. En sådan bistand vil typisk være meget omkostningsfuld samt tidskrævende, og vælger virksomheden at undersøge reglerne selv, vil der omvendt være en nærliggende risiko for fejlfortolkning af tredjelandets nationale regler. Tredjelandets lovgivning kan være tvetydig eller ikke-offentligt tilgængelig, og undersøgelsen kan således være yderst kompliceret.[181] Dette kom også til udtryk i Domstolens gentagende underkendelse af Kommissionens tilstrækkelighedsafgørelser vedrørende USA. Henset til at det er dataeksportøren, der bærer ansvaret for, at personoplysningerne stadig er sikret et tilstrækkeligt beskyttelsesniveau, er dette en yderst tung byrde for virksomhederne at løfte.

[181] Henstilling 01/2020, punkt 39 og 42

I C-311/18, Schrems II fastslog Domstolen, at en overførsel til USA på baggrund af SCC kan ske, når dataeksportøren implementerer supplerende foranstaltninger, idet USA's lovgivning hjemler vidtgående muligheder for myndighederne til at overvåge. På baggrund af dommen er det ikke usandsynligt, at USA's lovgivning vil ændre sig, idet overførsler til og fra USA ikke blot påvirker virksomheder og myndigheder i Unionen, men også dem i USA, idet overførsler af personoplysninger er essentielle i driften af mange virksomheder, og dermed har væsentlig betydning for den globale økonomi.

6.1.1.1. Særlig lovgivning ved en beskyttet modtager

Ved undersøgelsen af tredjelandets lovgivning er det særligt relevant at være opmærksom på, hvorvidt modtageren kan være omfattet af en særlig beskyttelse i tredjelandets lovgivning. Dette kan være relevant i første case, hvor Virksomhed B beskæftiger sig inden for lægevidenskaben. I Henstilling 01/2020 henviser Databeskyttelsesrådet til, at det vil være særligt relevant at overveje, hvorvidt modtageren er beskyttet, når modtageren leverer lægebehandling eller juridiske tjenesteydelser, idet modtageren i så fald kan være underlagt regler om tavshedspligt, der fritager modtageren for at give myndighederne adgang til oplysningerne.[182]

Der er behov for en dybdegående undersøgelse af USA's lovgivning med henblik på at undersøge, hvorvidt Virksomhed B er omfattet af sådanne regler. Det vil være relevant for de to virksomheder at klarlægge, hvorvidt al beskæftigelse inden for lægebehandling er omfattet af sådanne regler, eller hvorvidt der i USA differentieres mellem hvilket formål og beskyttelsesinteresse, beskæftigelsen har. Der kan eksempelvis være forskel på, hvorvidt behandlingen består i lægepraksis eller kliniske forsøg. Det afhænger derfor udelukkende af den amerikanske lovgivning, hvorvidt Virksomhed B er omfattet særregler, der beskytter mod adgang fra de offentlige myndigheder. Såfremt Virksomhed B er omfattet af sådanne regler, vil vurderingen af, hvilke supplerende foranstaltninger, der skal implementeres, være anderledes.

[182] Henstilling 01/2020, punkt 85

6.1.2. Relevante supplerende foranstaltninger

I fjerde trin i Henstilling 01/2020 skal virksomhederne træffe de supplerende foranstaltninger, der skal afhjælpe hindringer i tredjelandets lovgivning, som nærmere fremgår af afsnit 4.1.3. Nedenfor vil de mest relevante tekniske, organisatoriske og yderligere kontraktmæssige foranstaltninger blive gennemgået med henblik på at undersøge, hvordan virksomhederne i denne case bør forholde sig efter Schrems-afgørelserne.

6.1.2.1. Kryptering

Databeskyttelsesrådets første eksempel på en teknisk foranstaltning er effektiv kryptering. Såfremt Virksomhed B ikke er en særlig beskyttet modtager efter amerikansk lovgivning, vil transportkryptering af personoplysninger eksempelvis ikke kunne implementeres som en effektiv foranstaltning, idet FISA sec. 702 (50 USC § 1881a) muliggør, at amerikanske myndigheder kan kræve, at de amerikanske dataimportører tildeler adgang til importerede personoplysninger, hvor også krypteringsnøglerne kan være omfattet. I et sådant tilfælde, hvor den amerikanske lovgivning hjemler adgang for myndighederne til at tilgå oplysninger i videre omfang, end det er nødvendigt og proportionelt i et demokratisk samfund, vil en kryptering udelukkende være effektiv, hvor dataimportøren ikke har adgang til krypteringsnøglen, og dermed kun har adgang til krypterede data. Det vil dog ikke være muligt i dette tilfælde at afskære Virksomhed B fra at få adgang til ikke-krypterede data, idet billederne skal analyseres, og Virksomhed B har derfor brug for krypteringsnøglen for at kunne foretage sin behandling. Kryptering kan således ikke anvendes som en supplerende foranstaltning, såfremt Virksomhed B ikke er en beskyttet modtager.

Såfremt Virksomhed B er en beskyttet modtager efter amerikansk lovgivning, fremgår det af Databeskyttelsesrådets fjerde brugstilfælde, at et tilstrækkeligt beskyttelsesniveau vil kunne opnås ved at kryptere oplysningerne, således den beskyttede modtager er den eneste, som har adgang til krypteringsnøglen. Dette skyldes, at Virksomhed B i så fald ikke kan pålægges at udlevere krypteringsnøglen til de amerikanske myndigheder. Slutteligt bør Virksomhed A være opmærksom på sjette trin i 6-trins-vejledningen, og dermed løbende vurdere om lovgivningen ændrer sig, således Virksomhed B ikke længere er en beskyttet modtager, samt vurdere om krypteringen fortsat lever op til det aktuelle tekniske niveau.

6.1.2.2. Pseudonymisering

Såfremt Virksomhed B ikke er en beskyttet modtager, skal andre supplerende foranstaltninger implementeres for at sikre et tilstrækkeligt beskyttelsesniveau. Databeskyttelsesrådet foreslår, at der kan ske pseudonymisering af personoplysningerne inden overførsel til USA. Førend en oplysning er pseudonymiseret, er det en betingelse, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat, jf. databeskyttelsesforordningens artikel 4, stk. 1, nr. 5. Databeskyttelsesrådet påpeger hertil, at dataeksportører skal være opmærksomme på, at det ikke må være muligt at udpege en bestemt registreret i en gruppe af registrerede uden brug af yderligere oplysninger.[183] Derfor vil antallet af registrerede i de kliniske forsøg ligeledes kunne have betydning for, hvorvidt pseudonymisering er effektiv.

Det vil først og fremmest afhænge af det kliniske forsøgs karakter, hvorvidt pseudonymisering af de kliniske billeder er mulig. Vurderingsgrundlaget vil eksempelvis kunne afhænge af, hvilken type sygdom, som patienten lider af, og hvad kendetegnene for selve sygdommen er. Anvendelsen af kliniske billeder vil som udgangspunkt kun være relevant, såfremt tilstandens udvikling visuelt kan konstateres og ikke i de tilfælde, hvor udviklingen udelukkende kan mærkes af patienten. Det faktum, at udviklingen skal være visuel gør, at selve sygdommen, som patienten fejler, kan få betydning for, hvorvidt de kliniske billeder er personhenførbare. Såfremt den kliniske analyse sker vedrørende en patient med en sjælden lidelse, som kun en eller få personer har, kan dette betyde, at selve de kliniske billeder og kendetegnene ved sygdommen kan gøre det umuligt for Virksomhed A at pseudonymisere de kliniske billeder.

En anden problemstilling for Virksomhed A er, at det i nogle tilfælde vil være nødvendigt for Virksomhed B at få kendskab til det fulde sygdomsbillede, førend det er muligt at foretage en analyse af de kliniske billeder. Ligeledes vil det i nogle tilfælde også være nødvendigt, at Virksomhed B får kendskab til oplysninger om personen sammen med det kliniske billede, idet dette kan have betydning for forsøgets effekt. Det kan for eksempel være oplysninger om alder, vægt, køn eller lignende, der vil kunne gøre det umuligt at pseudonymisere oplysningerne, således de ikke længere er

[183] Henstilling 01/2020, punkt 80

personhenførbare. I det tilfælde vil det være nødvendigt for Virksomhed A at lave en særskilt vurdering ved hver enkelt patient i forhold til, hvorvidt de nødvendige oplysninger, der ønskes overført, er personhenførbare. Denne vurdering er kompliceret henset til den mængde af faktorer, der indgår. Dels skal Virksomhed A dataminimere, og dermed vurdere, præcis hvilke oplysninger, der er nødvendige for Virksomhed B at komme i besiddelse af, førend de kan lave den kliniske analyse af billederne. Dels skal Virksomhed A også vurdere, hvornår de oplysninger, der er givet, faktisk gør det muligt at henføre billederne og oplysninger til en bestemt person. Derudover er det problematisk for Virksomhed A at anvende pseudonymisering som supplerende foranstaltning, idet denne vurdering ikke kun er kompliceret, men også meget tidskrævende, idet hver enkel overførsel skal vurderes, og vurderingen derfor nemt vil blive meget omkostningstung.

Ydermere vil der være tilfælde, hvor personen vil være genkendelig alene på baggrund af billedets indhold. Det kan eksempelvis være, hvis det kliniske billede er af ansigtet, eller hvis patienten har en genkendelig tatovering eller andet kendetegn, der gør det muligt at identificere patienten alene ud fra billedet. I sådanne tilfælde vil det derfor ikke være muligt for Virksomhed A at pseudonymisere billederne, således de ikke længere er personhenførbare. Vurderingen af hvornår patienten er genkendelig vil også her være problematisk, henset til at Virksomhed A skal vurdere, om eksempelvis en tatovering er så unik, at det vil være muligt, at personen bliver identificerbar. Derudover vil vurderingen skulle ske ved hver enkel overførsel, og dermed vil vurderingen igen blive tidskrævende og omkostningstung.

Der vil således være tilfælde, hvor Virksomhed A vil kunne anvende pseudonymisering som en effektiv supplerende foranstaltning. Der vil dog også være tilfælde, hvor der vil opstå tvivl om, hvorvidt pseudonymisering i et konkret tilfælde vil kunne være mulig. I de tilfælde, hvor pseudonymisering vurderes at kunne yde en effektiv supplerende foranstaltning, bør Virksomhed A og B tilsvarende implementere organisatoriske foranstaltninger, der kan yde bidrag til at sikre sammenhæng i beskyttelsen af personoplysninger under hele behandlingsforløbet. Dette kan eksempelvis være interne ansvars- og rollefordelinger både internt i Virksomhed A, hvor det sikres, at hver enkel overførsel bliver vurderet, ligesom det sikres, at kun de nødvendige data bliver overført til Virksomhed B. Derudover kan den interne ansvars- og rollefordeling også reguleres mellem Virksomhed A og B ved håndtering

af eksempelvis myndighedsanmodninger. Se nærmere om organisatoriske foranstaltninger i afsnit 4.4. De supplerende foranstaltninger skal herefter implementeres og løbende vurderes i overensstemmelse med femte og sjette trin i Henstilling 01/2020.

Såfremt Virksomhed A finder, at det ikke er muligt at pseudonymisere, fordi det kliniske billede fortsat er personhenførbart, er det svært på baggrund af Henstilling 01/2020 at forestille sig, at Virksomhed A kan implementere andre supplerende foranstaltninger, således de kan overføre personoplysninger efter SCC og stadig sikre et beskyttelsesniveau, der i det væsentligste svarer til det, der er sikret i Unionen.

Såfremt Virksomhed B er en beskyttet modtager, vil det ikke være nødvendigt at implementere pseudonymisering som en supplerende foranstaltning, idet det tidligere er konstateret, at kryptering vil være effektiv i et sådant tilfælde. Virksomhed A bør dog alligevel overveje at pseudonymisere oplysninger, jf. princippet om dataminimering.[184]

6.2. Case 2

Den anden case er som følger:

> *Den danske kommune X anvender en digital bibliotekløsning, der er etableret i Danmark, på kommunens folkeskoler. Den digitale bibliotekløsning anvender en cloudtjeneste til hosting af pseudonymiserede personoplysninger om brugerne af bibliotekløsningen. Selve hostingen af de pseudonymiserede personoplysninger sker på en server, der er placeret i Tyskland, men ifølge cloud-leverandørens betingelser kan data, der hostes i cloud-løsningen, i visse tilfælde overføres til underleverandører, der er etableret i USA og Kina. Sådanne overførsler sker på baggrund af EU-Kommissionens standardkontraktbestemmelser.*

[184] Databeskyttelsesforordningens artikel 5, stk. 1, litra c

Når Kommune X anvender en cloud-tjeneste til hosting af pseudonymiserede personoplysninger om brugerne af bibliotekssløsningen, sker der som tidligere beskrevet en overførsel af personoplysninger. Som anført i afsnit 4.1.1., skal dataeksportører i første og andet trin kortlægge deres overførsler og kende deres overførselsgrundlag, hvilket Kommune X har gjort. Selvom hosting-tjenesten befinder sig inden for Unionen, fremgår det, at data i visse tilfælde overføres til underleverandører, der er etableret i USA og Kina, og der sker således en overførsel til tredjelande.

6.2.1. Vurdering af tredjelandenes lovgivning

I tredje trin skal dataeksportører sætte sig ind i tredjelandets lovgivning og praksis. Det fremgår af casen, at data, der hostes i cloud-tjenesten, i visse tilfælde overføres til underleverandører, der er etableret i USA. Ligesom i første case har Domstolen bidraget til Kommune X's vurdering af USA's lovgivning, men kommunen skal stadig foretage en undersøgelse af, hvorvidt der siden C-311/18, Schrems II er kommet ny, relevant lovgivning.

Det fremgår af casen, at data i visse tilfælde også overføres til underleverandører, der er etableret i Kina. Det er derfor nødvendigt for Kommune X at foretage en vurdering af, hvorvidt den kinesiske lovgivning og praksis er i strid med effektiviteten af de fornødne garantier ved SCC, således at de registrerede ikke længere sikres en beskyttelse, der i det væsentligste svarer til den beskyttelse, som er sikret i Unionen. Som det fremgår af bemærkningerne til første case, har Kommissionen og Databeskyttelsesrådet i udkastet til nye SCC samt Henstilling 01/2020 og Henstilling 02/2020 givet yderligere vejledning til, hvad Kommune X bør tage i betragtning, når de skal vurdere Kinas lovgivning og praksis. Henset til, at Domstolen alene har foretaget en vurdering af lovgivningen i USA, vil den vurdering, som Kommune X skal foretage af Kinas lovgivning være endnu dyrere og endnu mere kompliceret, end det er tilfældet ved den vurdering, som Kommune X skal foretage af den eventuelle nytilkomne lovgivning i USA.

6.2.2. Pseudonymisering

Som tidligere anført, kan en supplerende teknisk foranstaltning være pseudonymisering. Databeskyttelsesrådet opstiller i sjette brugstilfælde, der omhandler den situation, hvor der sker overførsel via en cloud-leverandør til et tredjeland, og hvor de offentlige myndigheder har beføjelser, der går videre,

end hvad der er nødvendigt og proportionelt i et demokratisk samfund. I den situation kan Databeskyttelsesrådet ikke forestille sig, at der kan implementeres effektive tekniske foranstaltninger, når cloud-leverandøren har behov for ikke-krypteret data for at udføre den tildelte opgave.[185]

I C-311/18, Schrems II fastslog Domstolen, at FISA sec. 702 giver amerikanske myndigheder adgang til oplysninger i videre omfang, end hvad der er strengt nødvendigt. Se nærmere i afsnit 3.2.6.1. Cloud-leverandører er netop omfattet af FISA sec. 702, idet FISA finder anvendelse, hvis oplysninger er indhentet fra eller med hjælp fra en tjenesteudbyder af elektronisk kommunikation.[186] En tjenesteudbyder af elektronisk kommunikation er blandt andet defineret som en udbyder af fjerndatabehandlingstjenester i henhold til definitionen i 18 USC § 2711.[187] Det fremgår af 18 USC § 2711 (2), at fjerndatabehandlingstjenester defineres som udbud af opbevarings- eller behandlingstjenester til offentligheden ved hjælp af et elektronisk kommunikationssystem. Dermed er cloud-leverandører omfattet af FISA sec. 702, hvor der er hjemlet adgang til, at de offentlige myndigheder i USA har beføjelser, der går videre, end hvad der er nødvendigt og proportionelt i et demokratisk samfund.

Allerede fordi det fremgår af sjette brugstilfælde, at Databeskyttelsesrådet ikke kan forestille sig effektive tekniske foranstaltninger, når myndigheder i tredjelandet har beføjelser, der går videre, end hvad der er nødvendigt og proportionelt i et demokratisk samfund, vil det ikke være tilstrækkeligt, at Kommune X pseudonymiserer personoplysningerne om brugerne af biblioteksløsningerne og hoster dem i en cloud-tjeneste, når der overføres oplysninger til underleverandører i USA.

Kommune X skal derudover undersøge, hvorvidt der også i Kina er hjemlet adgang til, at myndighederne kan få adgang til personoplysninger i videre omfang, end hvad der er nødvendigt og proportionelt i et demokratisk samfund. Først herefter kan de konstatere, hvorvidt det dels er nødvendigt at implementere supplerende foranstaltninger, samt dels hvorvidt pseudonymisering af personoplysningerne i så fald vil være tilstrækkeligt, således de registrerede sikres et beskyttelsesniveau, der i det væsentligste svarer til det, der er sikret i Unionen.

[185] Henstilling 01/2020, punkt 88 og 89
[186] FISA sec. 702 (50 USC § 1881a (h)(2)(a)(iv))
[187] FISA sec. 702 (50 USC § 1881(b)(4))

6.2.3. Kryptering

Kommune X kan ligeledes overveje at implementere kryptering. Det fremgår ikke af casen, hvorvidt hosting-leverandøren har behov for ikke-krypteret data, idet det ikke nærmere fremgår, hvorvidt hosting-leverandøren udelukkende opbevarer data, eller om de også foretager en yderligere behandling af oplysningerne.

Databeskyttelsesrådet uddyber i denne forbindelse, at når lovgivningen går videre, end hvad der er nødvendigt og proportionelt i et demokratisk samfund, og når der anvendes en cloud-leverandør, som kun skal have adgang til krypterede data, er kryptering alene effektiv, såfremt nøglerne forbliver i dataeksportørens kontrol inden for Unionen. Transportkryptering og kryptering af data i hvile vil derfor ikke være tilstrækkeligt ifølge Databeskyttelsesrådet, såfremt dataimportøren er i besiddelse af de kryptografiske nøgler.[188]

Hvis det er nødvendigt, at cloud-leverandøren har adgang til ikke-krypterede data for at leve op til deres kontrakt med dataeksportøren, fremgår det ovenfor i afsnit 6.2.2., at det ikke vil være muligt at implementere tekniske foranstaltninger i forbindelse med overførslen til USA. Det samme gør sig gældende i forhold til Kina, såfremt den kinesiske lovgivning ligeledes indeholder bestemmelser, der går videre end, hvad der er nødvendigt og proportionelt i et demokratisk samfund.

Henning Mortensen, der er medlem af Datatilsynet og er formand i Rådet for Digital Sikkerhed, anfører i denne forbindelse, at sjette brugstilfælde i Henstilling 01/2020 gør cloud-tjenester ulovlige, idet han ikke mener, at der er cloud-tjenester, der fungerer således, at data er krypteret hele vejen fra de forlader terminalen til de ligger i databasen. Henning Mortensen er af den opfattelse, at cloud-tjenester er designet på en sådan måde, at når transportkrypteringen brydes og omsættes til lagring i databasen, vil data typisk være i klar tekst.[189]

Såfremt cloud-leverandøren alene opbevarer data, vil denne formentlig ikke have behov for at kunne tilgå ikke-krypteret data. Som det fremgår af punkt 79 i Henstilling 01/2020, vurderer

[188] Henstilling 01/2020, punkt 79 og 89
[189] Kjærsdam, Flemming: Henning Mortensen om Schrems II: "Særligt problematisk for amerikanske cloudleverandører"

Databeskyttelsesrådet, at kryptering udgør en effektiv supplerende foranstaltning, når der sker datalagring til sikkerhedskopiering og andre formål, som ikke kræver adgang til ikke-krypterede data. Hertil er det en betingelse, at krypteringen er robust set i forhold til det aktuelle tekniske niveau. Til dette bemærker Databeskyttelsesrådet, at dataeksportøren bør sætte sig ind i, hvilke tilgængelige ressourcer og tekniske kapaciteter, som tredjelandets myndigheder har til at foretage en kryptoanalyse. Det er i tilslutning til dette udfordrende for virksomheder og myndigheder, at Databeskyttelsesrådet forventer at hver enkel dataeksportør skal og kan finde oplysninger om tredjelandets myndigheders tekniske kapaciteter for at garantere krypteringens effektivitet.

6.2.4. Afskæring af underleverandører

Det fremgår ikke i hvilke tilfælde overførslerne fra hosting-leverandøren i Tyskland sker til underleverandørerne. Kommune X kan overveje, hvorvidt det er muligt at aftale med hosting-leverandøren, at overførsel af personoplysninger til underleverandører uden for Unionen afskæres, således personoplysningerne holdes i Unionen. Det ses i praksis, at internationale udbydere af cloud-tjenester er begyndt at spekulere i denne løsning. Eksempelvis har Microsoft offentliggjort planer om at etablere deres cloud-tjenester på en sådan måde, at data ikke forlader Unionen.[190]

Såfremt Kommune X's underleverandører modtager oplysningerne fra hosting-leverandøren med henblik på at yde support, ville tredjelandsoverførslen formentlig kunne afskæres ved at supporten varetages i Unionen. Det samme vil formodentlig være tilfældet, såfremt underleverandørerne modtager oplysningerne fra hosting-leverandøren med henblik på at analysere data, hvis det er muligt at finde en underleverandør i Unionen, der vil kunne foretage en tilsvarende analyse. Uanset at det faktisk er muligt at flytte tjenesteydelsen til en databehandler i Unionen i disse tilfælde, vil en sådan ændring for hosting-leverandørens måde at drive forretning på, naturligvis aldrig være uden konsekvenser eller være omkostningsfri.

Der vil dog være situationer, hvor det vil være yderst kompliceret eller ligefrem umuligt for hosting-leverandøren at afskære underleverandørerne i USA og Kina. Såfremt hosting-leverandøren anvender underleverandørerne til at foretage en behandling, hvor underleverandørerne har særlig ekspertise

[190] Microsoft: Answering Europe's Call: Storing and Processing EU Data in the EU

eller er de eneste, der foretager en sådan behandling, vil det være yderst kompliceret eller ligefrem umuligt for hosting-leverandøren at finde en alternativ underleverandør i Unionen.

Det har også i den juriske litteratur været diskuteret, hvorvidt dataeksportører bør ændre deres forretningsmodeller, således de i stedet anvender cloud-tjenester inden for Unionen, og om dette er den korrekte løsning for at undgå problemerne med tredjelandsoverførsler. Henning Mortensen har blandt andet udtalt, at cloud-leverandører kan overveje at ændre forretningsmodel og etablere europæiske cloud-tjenester. Han argumenterer for, at dette løsningsforslag er dyrt, men det dog er billigere, end hvis virksomhederne skal foretage de omfattende analyser af tredjelandets lovgivning samt betale store bøder, hvis deres vurdering er forkert.[191]

Juraprofessor ved Georgetown University Law Center, Anupam Chander, har modsat udtrykt, at ændring af cloud-leverandørers forretningsmodeller, således disse benytter sig af europæiske cloud-leverandører til at udbyde deres cloud-tjenester, ikke er den optimale løsning på problemerne med tredjelandsoverførsler. Først og fremmest påpeger Chander, at den amerikanske masseovervågning ikke i sig selv er afskåret, blot ved at data opbevares i Unionen.[192] Desuden argumenterer Chander for, at der også i Unionen sker en høj grad af overvågning.[193]

Ydermere nævner Chander, at det er et problem at sikre, at data forbliver i Unionen, idet data i nogle tilfælde vil blive dirigeret via USA eller et andet tredjeland via netinfrastrukturen. At undgå dette vil kræve, at det internet, vi kender i dag, vil skulle laves fundamentalt om, således der bliver en ydre grænse for netværket, som følger Schengenområdet.[194]

Chander argumenterer ligeledes for, at det vil skabe sine egne problemer, såfremt der udelukkende anvendes cloud-tjenester inden for Unionen. Først argumenterer Chander for, at denne løsning vil være meget dyr, og derfor umulig for mindre virksomheder at implementere. Derudover argumenterer

[191] Wired Relations: Notat om Schrems II af Henning Mortensen
[192] Chander, Anupam, side 778
[193] Chander, Anupam, side 778 ff.
[194] Chander, Anupam, side 782

Chander for, at dette er i strid med ideen om global samhandel, hvor vigtigheden af den frie udveksling af personoplysninger, er fremhævet i databeskyttelsesforordningens præambelbetragtning 6.

Chander påpeger, at datalokalisering muligvis vil underminere cybersikkerheden, ligesom risikoen for databrud vil blive større. Dette skyldes, at firmaerne pålægges at oprette cloud-leverandører i Unionen eller ændre allerede eksisterende cloud-tjenester, hvilket vil pålægge den samme udbyder at have flere forskellige, lokale versioner og kontorer. Risikoen for hackerangreb vil dermed øges og ligeledes besværliggøre uddannelse og sikkerhedsprotokoller.[195]

Chander fremhæver afslutningsvist, at trods datalokalisering kan skabe indtjening i Unionen på grund af de virksomheder, som skal etableres der, så resulterer datalokaliseringen typisk i et tilsvarende tab for de andre lokale virksomheder i Unionen, som anvender tjenesten, og nu må benytte en dyrere og måske dårligere løsning, end der kunne tilbydes i et tredjeland.[196]

Chander fremkommer derfor med en række kritikpunkter og problematikker ved udelukkende at placere cloud-leverandører og data inden for Unionen. Det bør dog bemærkes, at Chander er amerikaner, og kan have et mere kritisk perspektiv på databeskyttelsesreglerne i Unionen. Datalokalisering kan i nogle tilfælde tænkes at være løsningen, men Chanders kritikpunkter er dog stadig værd at bemærke, idet datalokalisering vil skabe nye problemer og udfordringer, ligesom det vil underminere databeskyttelsesforordningens formål om at fremme fri udveksling af personoplysninger.

Selv hvis Kommune X finder en cloud-leverandør, som udelukkende hoster oplysningerne på servere i Unionen, og der dermed ikke sker en overførsel til tredjelande, skal kommunen stadig være opmærksom på selskabskonstruktionen, herunder hvorvidt databehandleren er en del af en koncern, hvor moderselskabet er etableret i et tredjeland, og der potentielt kan være risiko for adgang fra tredjelandets myndigheder. Det blev fastslået i en dom vedrørende Amazon Web Services afsagt den 12. marts 2021 af den øverste forvaltningsdomstol i Frankrig, som vedrørte en europæisk e-sundhedsplatform, der indgik en aftale med det franske sundhedsministerium. Sundhedsplatformen anvendte

[195] Chander, Anupam, side 783 f.
[196] Chander, Anupam, side 784

en hosting-leverandør i Luxemborg, som var datterselskab af det amerikanske selskab Amazon Web Services Inc. Forvaltningsdomstolen konstaterede, at dette ikke var en overførsel af oplysninger til tredjelande, men at der potentielt var risiko for amerikanske myndigheders adgang til oplysninger i medfør af FISA sec. 702 og E.O. 12333. Forvaltningsdomstolen bemærkede, at der var sket kryptering af data, og krypteringsnøglen udelukkende befandt sig ved en tredjepart i Frankrig. Som en yderligere kontraktmæssig foranstaltning havde hosting-leverandøren garanteret, at denne ville udfordre enhver generel anmodning om adgang fra en myndighed, ligesom data automatisk blev slettet efter tre måneder med yderligere mulighed for manuel sletning. Det blev derfor fastslået, at dette tilsammen udgjorde effektive supplerende foranstaltninger, som sikrede et tilstrækkeligt beskyttelsesniveau.

6.3. Case 3

Den tredje case er som følger:

> *I den globale koncern Z Group, der har selskaber i Danmark, USA, UK, Schweiz og Thailand, opbevares oplysninger om alle koncernens medarbejdere i et HR-system, der hostes hos koncernens moderselskab, Virksomhed Q, der er etableret i Danmark. HR-medarbejdere i alle koncernens selskaber har adgang til at tilgå personoplysninger om medarbejdere i deres eget selskab i HR-systemet.*

Det fremgår af casen, at Virksomhed Q i Danmark opbevarer oplysninger om alle koncernens medarbejdere i et HR-system. Det antages derfor, at Virksomhed Q er dataansvarlig for behandling af oplysninger om egne medarbejdere, men omvendt er databehandler for de indsamlede oplysninger fra koncernens øvrige selskaber. Først bør det fastlægges, hvorvidt denne situation falder inden for det territoriale anvendelsesområde af databeskyttelsesforordningen.

6.3.1. Det territoriale anvendelsesområde

Det fremgår af databeskyttelsesforordningens artikel 4, stk. 1, nr. 2, at en behandling omfatter enhver aktivitet eller række af aktiviteter, som personoplysninger eller en samling af personoplysninger gøres til genstand for. Som eksempler på dette opremses blandt andet registrering, opbevaring og

overladelse. Dermed behandler Virksomhed Q oplysninger om medarbejderne i Danmark, USA, UK, Schweiz og Thailand, allerede fordi de opbevarer oplysninger om disse medarbejdere. Selvom indsamlingen af personoplysninger til dels finder sted i lande uden for Unionen, så udføres behandlingen af personoplysningerne af databehandleren, der er etableret i Danmark. Det er uden betydning for vurdering af om databeskyttelsesforordningen finder anvendelse, hvilken nationalitet den registrerede har, eller hvor denne har bopæl.[197] Det afgørende er hvor og hvordan behandlingen foretages.

Det har i den sammenhæng betydning, hvordan Z Groups HR-system er opbygget. Såfremt Z Groups HR-system er opbygget på en sådan måde, at personoplysningerne har hver sin database, således oplysningerne, der er indsamlet fra hvert enkelt land, er adskilt, kan der stilles spørgsmålstegn ved, hvorvidt data stadig er underlagt en sådan behandling, at databeskyttelsesforordningen finder anvendelse. Selskaberne i USA, UK, Schweiz og Thailand er ikke omfattet af databeskyttelsesforordningens artikel 3, stk. 1, idet behandlingen ikke udføres for en dataansvarlig eller databehandler i Unionen. De nævnte selskaber er heller ikke omfattet af databeskyttelsesforordningens artikel 3, stk. 2, idet behandlingen ikke omhandler registrerede, der befinder sig i Unionen. De nævnte selskaber er derfor ikke omfattet af databeskyttelsesforordningens territoriale anvendelsesområde. Virksomhed Q er som databehandler for koncernens andre medarbejdere, end dem i Danmark, heller ikke omfattet af databeskyttelsesforordningens artikel 3, stk. 1 og 2, idet behandlingen ikke udføres af en dataansvarlig, der er etableret i Unionen, og idet behandlingen ikke foretages vedrørende registrerede i Unionen. Virksomhed Q's behandling af oplysninger om egne medarbejdere vil være omfattet af databeskyttelsesforordningens anvendelsesområde, men når data er adskilt, vil oplysningerne om de danske medarbejdere ikke føres ud af Unionen, og der foreligger dermed ikke tredjelandsoverførsel.

Såfremt Z Groups HR-system omvendt er opbygget på en sådan måde, at personoplysningerne fra både Danmark og de øvrige lande sammenblandes i en samlet database, skal Virksomhed Q opfylde kravene til sikker overførsel af personoplysninger til tredjelande, såfremt der er risiko for, at myndighederne i et af tredjelandene kan få adgang til oplysninger om registrerede i Unionen. Virksomhed Q vil i en sådan situation skulle foretage en undersøgelse af de relevante tredjelandes lovgivning, samt implementere passende supplerende foranstaltninger for at sikre et tilstrækkeligt beskyttelsesniveau.

[197] Databeskyttelsesforordningens præambelbetragtning 14

6.3.2. Konsekvens af, at data adskilles

Måden, hvorpå Z Group indretter HR-systemet, har således væsentlig betydning for, hvilke foranstaltninger, der skal iagttages. Såfremt koncernen vælger at organisere sig på en sådan måde, at deres databaser rent teknisk er adskilt, således tredjelandenes myndigheder aldrig ville kunne få adgang til andre oplysninger end om medarbejderne i det konkrete tredjeland, behøver koncernen ikke foretage en dybdegående vurdering af tredjelandenes lovgivning. Koncernen behøver dermed ikke at implementere supplerende foranstaltninger for at sikre, at de registrerede i Unionen sikres et beskyttelsesniveau, der i det væsentligste svarer til det, der er sikret i Unionen, netop fordi der ikke er risiko for at oplysninger om registrerede i Unionen overføres til tredjelande.

Det fremgår af Databeskyttelsesrådets retningslinjer 3/2018 om det territoriale anvendelsesområde for databeskyttelsesforordningen (artikel 3), at i situationen, hvor databehandleren, der er etableret i Unionen, ikke falder ind under det territoriale anvendelsesområde, vil databehandleren alligevel være underlagt nogle af bestemmelserne i databeskyttelsesforordningen. Databehandleren har derfor stadig pligt til at iagttage databeskyttelsesforordningens regler vedrørende de almindelige pligter til en databehandler, herunder eksempelvis at behandling kun må ske ved instruks, behandlingen skal være reguleret ved kontrakt og opfylde kravene til behandlingssikkerhed.[198]

6.3.3. Konsekvens af risikoen for, at data sammenblandes

Såfremt Z Group ikke organiserer sig på en sådan måde, at deres databaser er adskilt, og der dermed er risiko for sammenblanding af data indsamlet uden for Unionen med data indsamlet i Unionen, skal koncernen orientere sig i 6-trins-vejledningen med henblik på at sikre et tilstrækkeligt beskyttelsesniveau. Overførslerne, som koncernen foretager, er allerede klarlagt, og første trin i 6-trins-vejledningen er dermed gennemført.

I andet trin i 6-trins-vejledningen, skal overførselsgrundlaget identificeres. Det fremgår ikke af casen, hvilket overførselsgrundlag koncernen anvender. Hvad angår Schweiz, har Kommissionen den 26. juli 2000 vedtaget en tilstrækkelighedsafgørelse i medfør af databeskyttelsesforordningens artikel

[198] EDPB, Retningslinjer 3/2018, s. 13

45.[199] Det er derfor kun nødvendigt at være opmærksom på, hvorvidt tilstrækkelighedsafgørelsen trækkes tilbage eller kendes ugyldig, som beskrevet i afsnit 2.7. og 4.1.1. UK og Kommissionen har i forbindelse med Brexit indgået en aftale om en overgangsperiode indtil udgangen af juni 2021, hvor personoplysninger fortsat kan overføres til UK, som var de stadig medlem af Unionen.[200] Det forventes dog, at Kommissionen vil træffe en tilstrækkelighedsafgørelse vedrørende UK, idet processen angående en tilstrækkelighedsafgørelse er igangsat.[201] USA og Thailand er usikre tredjelande, og Virksomhed Q bør derfor identificere overførselsgrundlaget til disse.

Såfremt Virksomhed Q ønsker at anvende SCC som overførselsgrundlag til USA og Thailand, er der i udkastet til nye SCC åbent for den mulighed at anvende disse ved en overførsel fra en databehandler til en dataansvarlig. Dette er ikke en mulighed i de nugældende SCC. Såfremt udkastet til nye SCC vedtages, skal Virksomhed Q iagttage afsnit 2, standardbestemmelse 1. Her skal Virksomhed Q garantere, at den vil behandle oplysninger efter instruks fra de dataansvarlige, ligesom parterne skal iagttage princippet om behandlingssikkerhed, samt dokumentere overholdelse af bestemmelserne.

Det fremgår af afsnit 2, standardbestemmelse 2 og 3, der omhandler tredjelandets lovgivning og myndighedsanmodninger, at disse finder anvendelse, når data indsamlet fra et tredjeland sammenblandes med oplysninger indsamlet i Unionen. Virksomhed Q skal i så fald, som tidligere beskrevet, foretage den dybdegående analyse af begge de usikre tredjelandes lovgivning med henblik på at konstatere, i hvilken grad myndighederne i disse tredjelande har mulighed for at tilgå de overførte oplysninger. Som det tidligere er beskrevet i afsnit 6.1.1. og 6.2.1., har Domstolen i C-311/18, Schrems II vurderet USA's lovgivning, og Virksomhed Q skal således kun iagttage ny relevant lovgivning efter domsafsigelsen i deres undersøgelse. Omvendt skal Virksomhed Q lave en komplet undersøgelse af lovgivningen i Thailand.

Dernæst skal Virksomhed Q undersøge, hvorvidt det er muligt at implementere supplerende foranstaltninger for at sikre et tilstrækkeligt beskyttelsesniveau. Som beskrevet i afsnit 4.2.2. vedrørende syvende brugstilfælde i Henstilling 01/2020, kan Databeskyttelsesrådet ikke forestille sig effektive,

[199] Kommissionens beslutning af 26. juli 2000 (2000/518/EF)
[200] Datatilsynet: Brexit og overførsler af personoplysninger
[201] Udkast til tilstrækkelighedsafgørelse vedrørende UK

supplerende foranstaltninger, når data sammenblandes og overføres i HR-sammenhæng i en koncern fra en databehandler i Unionen til en dataansvarlig i et tredjeland, samtidig med at tredjelandets lovgivning går videre, end hvad der nødvendigt og proportionelt i et demokratisk samfund.[202] Som det tidligere er konkluderet i C-311/18, Schrems II, går de amerikanske myndigheders beføjelser videre end det, der nødvendigt og proportionelt i et demokratisk samfund, og de kan dermed få adgang til de sammenblandede oplysninger. Ved overførsel af oplysningerne til Thailand, skal virksomheden foretage en vurdering af lovgivningen med henblik på at finde ud af, hvorvidt det ligeledes udgør samme problem. Når der, som det er tilfældet i USA, er risiko for, at myndighederne kan få adgang til de sammenblandende oplysninger, vil det således ikke være muligt at iagttage supplerende foranstaltninger.

Såfremt koncernens HR-system opbevarer alle oplysningerne samlet i Virksomhed Q, vil den eneste logiske foranstaltning for koncernen være, at de indretter deres system anderledes, således der ikke længere er risiko for at oplysningerne sammenblandes og tredjelandets myndigheder kan tilgå oplysninger om andre personer end dem, der er indsamlet i det pågældende tredjeland.

6.4. Sammenfatning af cases

Som det fremgår af de tre cases ovenfor, befinder dataeksportører, der ønsker at overføre personoplysninger til usikre tredjelande, sig i en vanskelig situation efter C-311/18, Schrems II. I den forbindelse er der givet mulige løsningsforslag i de tre konkrete cases, men disse tre cases omfatter langt fra alle de mulige problemstillinger, som dataeksportører kan møde. Det bemærkes yderligere, at en egentlig løsning på de fremkomne problemstillinger vil kræve yderligere information om den konkrete overførsel, tredjelandenes lovgivning og omstændighederne i øvrigt.

Som tidligere beskrevet fremgår det af tredje trin i Henstilling 01/2020 samt i afsnit 2, standardbestemmelse 2 i udkastet til nye SCC, at der skal foretages en vurdering af både tredjelandets lovgivning og alle relevante oplysninger ved overførslen sammenholdt med de supplerende foranstaltninger, der kan implementeres, når dataeksportører ønsker at overføre personoplysninger til tredjelande. Som det

[202] Henstilling 01/2020, punkt 90 og 91

dog fremgår af tredje case, kan der være konkrete situationer, hvor det ikke klart fremgår, hvorvidt dataeksportører faktisk foretager en behandling, der er omfattet af databeskyttelsesforordningens territoriale anvendelsesområde.

Såfremt behandlingen er omfattet af databeskyttelsesforordningens anvendelsesområde, skal der som beskrevet foretages en vurdering af både tredjelandets lovgivning og alle relevante oplysninger ved overførslen sammenholdt med de supplerende foranstaltninger, der kan implementeres. Det blev konkluderet i afsnit 6.1.1., at denne vurdering er yderst kompliceret, især henset til dataeksportører også skal tage stilling til den del af tredjelandets lovgivning, der er tvetydig og ikke-offentligt tilgængelig.[203] Vurderingens kompleksitet kommer yderligere til udtryk, idet Domstolen to gange har været nødsaget til at underkende Kommissionens tilstrækkelighedsafgørelser vedrørende USA. Denne vurdering bliver kun mere kompliceret, hvis der sker overførsler til flere lande som i tredje case.

Det er ligeledes problematisk, at det er dataeksportøren selv, der skal foretage vurderingen af tredjelandets lovgivning. Henset til, at der skal ske individuelle vurderinger i hver enkel virksomhed og myndighed om hvert enkelt land, der sker overførsel til, er der en høj risiko for, at vurderingen heraf bliver forskelligartet, hvilket unægtelig vil skabe disharmoni i databeskyttelsesreguleringen i Unionen. Ydermere skal de forskellige nationale tilsyn efterprøve vurderingerne i tilfælde af klager, og også her kan der være en risiko for, at tilsynenes efterprøvelser og beslutninger vil være forskellige på grund af de ufyldestgørende retningslinjer. Til trods for at tilsynene har mulighed for at anmode Databeskyttelsesrådet om en udtalelse efter databeskyttelsesforordningens artikel 64, stk. 2, synes det dog urealistisk at forvente, at Databeskyttelsesrådet vil kunne give en udtalelse i alle tilfælde. Dataeksportørens og tilsynets vurderinger kan derfor stadig resultere i en uensartet retsanvendelse.

Selvom der i Henstilling 01/2020 gives vejledning til, hvilke supplerende foranstaltninger virksomheder og myndigheder med fordel kan overveje at implementere, så er der stadig udfordringer i forbindelse hermed. Ikke nok med at dataeksportører skal foretage en kompliceret undersøgelse af tredjelandets lovgivning, så skal de også foretage en omfattende vurdering af tredjelandets tekniske kapaciteter. Eksempelvis fremgår det af anden case, at det er en betingelse, at krypteringen er robust set

[203] Henstilling 01/2020, punkt 39 og 42

i forhold til tredjelandets aktuelle tekniske niveau, og at dataeksportøren derfor bør sætte sig ind i, hvilke tilgængelige ressourcer og tekniske kapaciteter, tredjelandets myndigheder har til rådighed til at foretage en kryptoanalyse. Det er desuden beskrevet i første case, at selvom pseudonymisering er anbefalet som et muligt løsningsforslag, vil muligheden for at anvende pseudonymiseringen blandt andet afhænge af det konkrete billede, samt hvilke oplysninger modtageren har behov for i forbindelse med de kliniske forsøg.

På baggrund af Henstilling 01/2020 er det desuden problematisk i fremtiden at anvende cloud-tjenester placeret uden for Unionen, eksempelvis som i anden case, idet det er en betingelse, at data i så fald skal være fuldkommen krypteret. Henning Mortensen fremhæver, at cloud-tjenester ikke fungerer således, at data er krypteret hele vejen fra de forlader terminalen, til de ligger i databasen. Det udgør et stort praktisk problem, såfremt det ikke længere er muligt at anvende cloud-tjenester, idet disse er et meget udbredt redskab for virksomheder og myndigheder, ligesom de fleste cloud-tjenester i dag er placeret helt eller delvist uden for Unionen. Det vil i visse tilfælde være muligt at afskære underleverandører uden for Unionen, men dette er heller ikke i alle tilfælde hensigtsmæssigt. Anupam Chander argumenterer i denne forbindelse blandt andet for, at datalokalisering ikke vil afskære amerikansk masseovervågning, og at det samtidig vil underminere cyber-sikkerheden. Det skyldes eksempelvis, at udbydere pålægges at oprette lokale versioner og ændre allerede eksisterende cloud-tjenester, hvilket vil gøre dem mere udsatte for hacker-angreb. Desuden kan selv anvendelse af cloud-leverandører etableret i Unionen vise sig at være problematisk, såfremt cloud-leverandøren har et moderselskab i et tredjeland, hvor lovgivningen forpligter moderselskabet til at udlevere oplysninger, jf. den tidligere omtalte dom vedrørende Amazon Web Services i afsnit 6.2.4.

Der er således behov for at den, der ønsker at overføre personoplysninger til tredjelande, har dybdegående indsigt i tredjelandets lovgivning og tekniske kapaciteter, samt den konkrete behandlingssituation. Selv hvis dataeksportøren vælger at indhente ekstern juridisk bistand til den omfattende vurdering, fordi dataeksportøren ikke selv har kompetencen hertil, vil dette kræve, at den, der skal yde bistand, får dybdegående indsigt i både tredjelandets lovgivning og til den konkrete overførsel samt alle øvrige, relevante omstændigheder. Vurderingen er således yderst kompliceret og omkostningstung, uanset om dataeksportøren foretager vurderingen selv eller indhenter ekstern juridisk bistand.

7. Konklusion

Domstolen konkluderede både i C-362/14, Schrems I og C-311/18, Schrems II, at det skal godtgøres, hvorvidt tredjelandet sikrer et tilstrækkeligt beskyttelsesniveau, forinden der foretages en overførsel til tredjelandet. Hertil blev det konkluderet, at dette er sikret, når niveauet i det væsentligste svarer til det i Unionen. Som tidligere anført blev begge tilstrækkelighedsafgørelser vedrørende USA underkendt, hvorimod Domstolen ikke erklærede de nugældende SCC generelt ugyldige i C-311/18, Schrems II.

Først og fremmest skal dataeksportøren vurdere, hvad det 'væsentlige samme beskyttelsesniveau' indebærer. Det er således op til en virksomhed eller myndighed at vurdere, hvornår det kan tillades, at beskyttelsesniveauet i et vist omfang viger fra beskyttelsesniveauet i Unionen, og hvornår variationen bliver for vidtgående. Den pågældende formulering efterlader virksomheder og myndigheder i uklarhed, da det i enhver situation vil komme an på en konkret vurdering og fortolkning af, hvorvidt det 'væsentlige samme beskyttelsesniveau' er til stede. I Henstilling 02/2020 udledte Databeskyttelsesrådet fire europæiske væsentlige garantier på baggrund af retspraksis fra Domstolen vedrørende Charterets artikel 7, 8, 47 og 52. Disse udgør et bidrag til vurderingen af, hvornår tredjelandet sikrer et beskyttelsesniveau, der i det væsentligste svarer til det i Unionen. Heraf fremgår det blandt andet, at der skal sikres en uafhængig tilsynsmekanisme og stilles effektive retsmidler til rådighed for de enkelte personer. Domstolen konkluderede i C-311/18, Schrems II, at begge disse væsentlige garantier ikke var sikret, herunder heller ikke ved oprettelse af en ombudsmand. Det fremgår yderligere af garantierne i Henstilling 02/2020, at behandlingen skal være baseret på klare, præcise og tilgængelige regler, og må ligeledes ikke gå videre, end hvad der er nødvendigt og proportionelt. Det er således op til dataeksportøren at vurdere, hvorvidt myndighederne i tredjelandet har beføjelser, der går videre, end hvad der er nødvendigt og proportionelt. Det er desuden uddybet både i de nugældende SCC og i udkastet til nye SCC, at parterne skal garantere, at tredjelandets lovgivning ikke tillader offentlige myndigheder en videre adgang, end hvad der er nødvendigt og proportionelt. Henstilling 02/2020 uddyber således momenter i vurderingen, men yder ikke bidrag til, hvad virksomheder og myndigheder konkret skal foretage sig for at kompensere for tredjelandets lovgivning.

Det fremgår af tredje trin i Henstilling 01/2020, samt uddybet i udkastet til nye SCC, afsnit 2, standardbestemmelse 2, modsat de nugældende SCC, at dataeksportøren skal foretage en vurdering af lovgivning og praksis i tredjelandet, og vurdere om der er noget i lovgivningen, der strider mod effektiviteten af de fornødne garantier. Det må antages at være særligt kompliceret at foretage denne vurdering henset til, at vurderingen endda skal foretages i et retssystem, dataeksportøren ikke har et indgående kendskab til. Vurderingen bliver kun yderligere kompliceret, når også ikke-tilgængelig lovgivning og praksis skal vurderes. I første case kan netop dette udgøre et problem, da det her skal vurderes, om der er særlovgivning i tredjelandet, som gør, at modtageren er særligt beskyttet, og dermed ikke er omfattet af tredjelandets myndigheders vidtgående beføjelser.

Det må således konkluderes, at det er et betydeligt ansvar, som dataeksportøren pålægges, især henset til at dataeksportøren kan pålægges sanktioner, såfremt deres vurdering af tredjelandets lovgivning er forkert. Vurderingens kompleksitet synliggøres yderligere ved, at Kommissionens tilstrækkelighedsafgørelser vedrørende USA to gange er blevet underkendt. Dette sætter spørgsmålstegn ved, hvorvidt andre tilstrækkelighedsafgørelser med tiden også vil blive underkendt, fordi der ikke er lavet en tilstrækkelig vurdering af tredjelandets lovgivning. Derudover må virksomheders og myndigheders omkostninger ved at foretage en sådan vurdering være betydelige, uanset om dataeksportøren indhenter juridisk bistand eller selv foretager undersøgelsen. Der er desuden ikke udarbejdet vurderinger af tredjelandenes lovgivning af Kommissionen, Databeskyttelsesrådet eller andre organer, hvilket kunne bidrage til sikring af en fyldestgørende undersøgelse heraf. Dette bevirker derfor, at der er betydelig risiko for, at de enkelte virksomheders og myndigheders undersøgelse vil resultere i forskellige vurderinger af det samme tredjeland. Dette modarbejder derfor harmoniseringen af databeskyttelsesreguleringen i Unionen. Der er desuden risiko for, at de nationale tilsynsmyndigheder vil vurdere tredjelandenes lovgivning forskelligt, hvilket kan resultere i en uensartet retsanvendelse.

Den komplekse vurdering af tredjelandes lovgivning illustreres særligt i tredje case, som er gennemgået i afsnit 6.3. Heraf fremgår det, at det vil være nødvendigt først at vurdere, hvorvidt en behandling er omfattet af databeskyttelsesforordningens anvendelsesområde, når databehandleren i Unionen kun opbevarer personoplysninger fra tredjelande. Det er her afgørende, hvordan behandlingen sker, herunder om data er adskilt eller sammenblandet. Såfremt data er sammenblandet, er dataeksportøren

forpligtet til at vurdere lovgivningen i alle de tredjelande, der overføres oplysninger til. I en behandlingskonstruktion som i casen, bliver det endvidere muligt at anvende SCC som overførselsgrundlag, såfremt udkastet til nye SCC træder i kraft, hvilket ikke er tilfældet med de nugældende SCC.

Domstolen konkluderede i C-311/18, Schrems II, at når tredjelandets lovgivning ikke i sig selv sikrer den væsentlige samme beskyttelse som i Unionen, er dataeksportøren ansvarlig for at opstille supplerende foranstaltninger, således den væsentlige samme beskyttelse sikres. I dommen blev det dog ikke nærmere uddybet, hvilke supplerende foranstaltninger, der skal implementeres. I Henstilling 01/2020 opfordres dataeksportøren og dataimportøren til at implementere supplerende tekniske, organisatoriske og yderligere kontraktmæssige foranstaltninger, ligesom der opstilles brugstilfælde med eksempler på vurderinger af forskellige behandlingssituationer. I udkastet til nye SCC henvises til de samme supplerende foranstaltninger.

Databeskyttelsesrådet foreslår pseudonymisering som en teknisk foranstaltning. Det blev dog konstateret i første case, at pseudonymisering ikke i alle tilfælde vil være mulig. I den konkrete case kan det efter omstændighederne være nødvendigt at foretage en særskilt vurdering af hver enkel overførsel i forhold til, hvorvidt de overførte oplysninger er personhenførbare. Effektiv pseudonymisering vil eksempelvis ikke kunne lade sig gøre, hvis der er kendetegn ved sygdommen eller personen, der umuliggør dette, eller såfremt der er behov for så mange supplerende oplysninger til at opfylde den pågældende kontrakt, at oplysningerne er personhenførbare. Såfremt der skal foretages en særskilt vurdering ved hver enkel overførsel, vil foranstaltningen blive omkostningstung, ligesom det er kompliceret at vurdere, hvorvidt pseudonymisering i hvert enkelt tilfælde er tilstrækkelig.

I Henstilling 01/2020 foreslås ligeledes implementering af kryptering. Såfremt der skal ske en overførsel til et tredjeland, hvor myndighederne har beføjelser, der går videre, end hvad der er nødvendigt og proportionelt i et demokratisk samfund, blev det i henstillingen konkluderet, at kryptering udelukkende er effektiv, når dataimportøren ikke har adgang til krypteringsnøglen, og dermed kun har adgang til krypterede oplysninger. I første case var kryptering således ikke en mulighed, idet dataimportørens behandling nødvendiggjorde adgang til ikke-krypteret data.

Databeskyttelsesrådet fastsætter desuden, at der er betydelige problemer ved anvendelse af cloud-tjenester i forbindelse med en tredjelandsoverførsel. Databeskyttelsesrådet konkluderer, at anvendelsen af en cloud-tjeneste udelukkende vil kunne ske, såfremt data krypteres, og såfremt nøglerne forbliver i dataeksportørens kontrol inden for Unionen. Ved anvendelse af en cloud-tjeneste er det en betingelse, at krypteringen er robust set i forhold til det aktuelle tekniske niveau. Dataeksportøren skal i den forbindelse vurdere, hvilke tilgængelige ressourcer og tekniske kapaciteter tredjelandets myndigheder har til at foretage en kryptoanalyse, hvilket er yderst kompliceret for hver enkel virksomhed og myndighed at vurdere. Efter denne konklusion udtalte Henning Mortensen, at cloud-tjenester dermed vil være ulovlige, idet data reelt ikke er krypteret hele vejen fra det forlader terminalen til det lander i databasen.

I relation til anden case er et muligt løsningsforslag, at koncernen afskærer overførsler til underleverandører i tredjelande og dermed udelukkende anvender cloud-tjenester i Unionen. Afskæringen vil dog i nogle tilfælde skabe sine egne udfordringer eller være umulig. Det vil eksempelvis kunne være skadeligt for datasikkerheden og samhandlen, ligesom underleverandøren kan have særlig ekspertise. Samlet set er det således svært at forestille sig, at internationale cloud-tjenester i den nærmeste fremtid kan leve op til databeskyttelsesreglerne på trods af, at cloud-tjenester anvendes i større udstrækning.

På baggrund af dette må det konkluderes, at dataeksportører, der ønsker at overføre personoplysninger til usikre tredjelande, befinder sig i en yderst vanskelig situation, når de skal vurdere, hvordan de bør indrette sig efter C-311/18, Schrems II. Først og fremmest skal parterne bruge enorme ressourcer på at undersøge både tilgængelig og ikke-tilgængelig lovgivning i tredjelande. Derudover skal de også vurdere, hvilke supplerende foranstaltninger, der kan afhjælpe problemerne ved tredjelandenes lovgivning, således de fornødne garantier sikres. Denne vurdering skal endda ske under hensyntagen til tredjelandets myndigheders tekniske kapaciteter. Henstilling 01/2020 og udkastet til nye SCC forsøger at afhjælpe den vanskelige situation, som parterne befinder sig i efter C-311/18, Schrems II. På baggrund af overvejelserne fremhævet i forbindelse med de tre cases må det dog konstateres, at parterne i virkeligheden ikke megen hjælp har modtaget henset til at vurderingen af, hvorvidt en supplerende foranstaltning er tilstrækkelig, vil afhænge konkret af den specifikke lovgivning i tredjelandet, den specifikke overførsel samt den specifikke dataeksportørs og dataimportørs indretning.

Litteraturliste

1. Lovgrundlag

- Den Europæiske Unions charter om grundlæggende rettigheder, 2010/C 83/02, 30. marts 2010.
  Forkortes: ***Charteret.***
- Europa-Parlamentets og Rådets Direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. (Historisk).
  Forkortes: ***Databeskyttelsesdirektivet.***
- 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).
  Forkortes: ***Databeskyttelsesforordningen.***
- Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger af 28. januar 1981. Danmark ratificerede denne ved BKI nr. 59 af 16/05/1991.
- Konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder af 4. november 1950. Danmark ratificerede denne ved BKI nr. 20 af 11/06/1953.
  Forkortes: ***EMRK.***
- Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. Lov nr. 502 af 23/05/2018.
  Forkortes: ***Databeskyttelsesloven.***
- Traktaten om Den Europæiske Union af 7. februar 1992.
  Forkortes: ***TEU.***
- Traktaten om Den Europæiske Unions funktionsområde af 1. december 2009.
  Forkortes: ***TEUF.***
- Traktaten om oprettelse af Det Europæiske Fællesskab af 25. marts 1957. (Historisk).

- Lov om behandling af personoplysninger. Lov nr. 429 af 31/05/2000. (Historisk).
  Forkortes: ***Persondataloven.***

2. Forarbejder

- Betænkning nr. 1565 om databeskyttelsesforordningen (2016/679) – og de retlige rammer for dansk lovgivning, Justitsministeriet, del I.
  Forkortes: ***Betænkning nr. 1565/2017.***
- Forklaringer til (*) chartret om grundlæggende rettigheder (2007/c 303/02).

3. Europa-Kommissionens beslutninger og afgørelser

- Kommissionens beslutning af 26. juli 2000 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af safe harbor-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium (2000/520/EF). (Historisk).
  Forkortes: ***Safe Harbour.***
- Kommissionens beslutning af 26. juli 2000 i henhold til Europa-Parlamentets og Rådets direktiv 45/46/EF vedrørende tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Schweiz (2000/518/EF).
- Kommissionens beslutning af 15. juni 2001 (2001/497/EF) om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til direktiv 95/46/EF.
  Forkortes: ***SCC af 2001.***
- Kommissionens beslutning af 27. december 2001 (2002/16/EF) om standardkontraktbestemmelser for overførsel af personoplysninger til registerførere etableret i tredjelande i henhold til direktiv 95/46/EF. (Historisk)
  Forkortes: ***SCC af 2002.***

- Kommissionens beslutning af 27. december 2004 (2004/915/EF) om ændring af beslutning 2001/497/EF for at indføre en alternativ standardkontrakt om overførsel af personoplysninger til tredjelande.
  Forkortes: ***SCC af 2004.***
- Kommissionens afgørelse af 5. februar 2010 (2010/87/EU) om standardkontraktbestemmelser for videregivelse af personoplysninger til registerførere etableret i tredjelande i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF.
  Forkortes: ***SCC af 2010.***
- 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. (Historisk)
  Forkortes: ***Privacy Shield.***
- 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.
- Kommissionens meddelelse KOM(2013) 846 endelig af 27. november 2013: ”Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet: Genopbygning af tilliden til datastrømmene mellem EU og USA”.
- Kommissionens meddelelse KOM(2013) 847 endelig af 27. november 2013: ”Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om, hvordan safe harbor-ordningen fungerer for så vidt angår EU-borgere og virksomhederne i EU”.

4. Kommissionens udkast til afgørelser

- Commission implementing decision of XXX pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. Udgivet 19. februar 2021.
  Forkortes: ***Udkast til tilstrækkelighedsafgørelse vedrørende UK***

- Annex to the commission implementing decision 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. Udgivet 12. november 2020.
  Forkortes: ***Udkast til nye SCC.***
- Commission implementing decision (EU) .../… of XXX 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. Udgivet 12. november 2020.
  Forkortes: ***Udkast til afgørelsesbeslutning om nye SCC.***

5. Afgørelser

- Sag 6/64, Costa mod ENEL, af 15. juli 1964.
- C-92/09 og C-93/09, De forenede sager C-92/09 og C-93/09 Volker og Markus Schecke og Eifert, af 9. november 2010.
- C-468/10, ASNEF, af 24. november 2011.
- C-291/12, Schwarz, af 17. oktober 2013.
- C-293/12, Digital Rights Ireland, af 8. april 2014.
- C-362/14, Schrems I, af 6. oktober 2015.
- C-203/15 og C-698/15, De forenede sager C-203/15, Tele2 Sverige og C-698/15, Watson m.fl. af 21. december 2016.
- C-311/18, Schrems II, af 16. juli 2020.
- DT j.nr. 2007-214-0004, af 10. maj 2007.

6. Henstillinger

- Article 29 Data Protection Working Party Opinion 4/2007 on the concept of personal data. Vedtaget 20. juni 2007.
- Datatilsynet: Vejledning: Overførsel af personoplysninger til tredjelande. Opdateret juni 2019.

- EDPB: Anbefaling 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger. Vedtaget 10. november 2020.
  Forkortes: ***Henstilling 02/2020.***
- EDPB: Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger. Vedtaget til offentlig høring 10. november 2020.
  Forkortes: ***Henstilling 01/2020.***
- EDPB: Retningslinjer 3/2018 om det territoriale anvendelsesområde for databeskyttelsesforordningen (artikel 3). Vedtaget 12. november 2019.

7. Generaladvokatens forslag til afgørelser

- Forslag til afgørelse fra generaladvokat Y. Bot, fremsat den 23. september 2015 (1), Sag C-362/14, Maximillian Schrems mod Data Protection Commissioner.
- Forslag til afgørelse fra generaladvokat H. Saugmandsgaard Øe, fremsat den 19. december 2019 (1), Sag C-311/18, Data Protection Commissioner mod Facebook Ireland Limited og Maximillian Schrems.

8. Bøger

- Blume, Peter: Den nye persondataret, 2. udgave, Jurist- og Økonomforbundets Forlag, 2018.
- European Union Agency for Fundamental Rights, m.fl.: Handbook on European data protection law, 2018 edition.
  (https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition).
- Evald, Jens: At tænke juridisk, 5. udgave, Djøf Forlag, 2019.
- Munk-Hansen, Carsten: Retsvidenskabsteori, 2. udgave, Djøf Forlag, 2018.
- Neergaard, Ulla, m.fl.: EU-ret, 8. udgave, Karnov Group, 2020.
- Nielsen, Kristian Korfits m.fl.: Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udgave, Jurist- og Økonomforbundets Forlag, 2020.

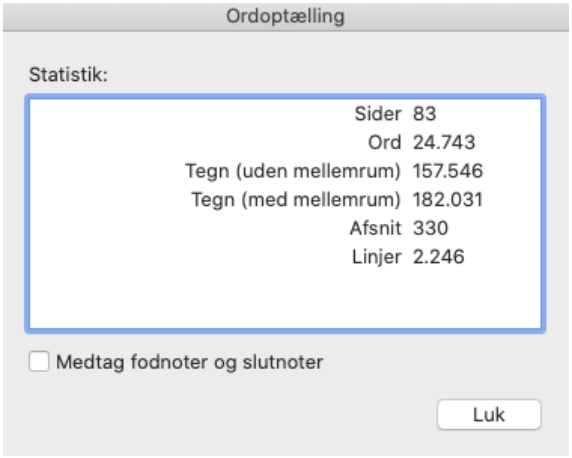
- Rytter, Jens Elo: Individets grundlæggende rettigheder, 3. udgave, Karnov Group, 2019.
- Storgaard, Louise Halleskov, m.fl.: Folkeret og menneskerettigheder, 1. udgave, Karnov Group, 2019.

9. Hjemmesider og artikler

- Chander, Anupam: Is Data Localization a Solution for Schrems II?, Journal of International Economic Law. Udgivet 25. september 2020. (https://academic.oup.com/jiel/article-abstract/23/3/771/5909035?redirectedFrom=fulltext). Senest tilgået 8. maj 2021.
- Datatilsynet: Brexit og overførsel af personoplysninger. (https://www.datatilsynet.dk/internationalt/brexit). Senest tilgået 16. april 2021.
- Datatilsynet: Hvad er en personoplysning? (https://www.datatilsynet.dk/databeskyttelse/hvad-er-personoplysninger). Senest tilgået 22. april 2021.
- EDPB - 41st Plenary session: EDPB adopts recommendations on supplementary measures following Schrems II. Udgivet 11. november 2020. (https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_da). Senest tilgået 7. april 2021.
- EDPB: EDPB - 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. Udgivet 23. juli 2020. (https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf). Senest tilgået 8. maj 2021.
- Europa-Parlamentet, Faktabladet om Den Europæiske Union: EU-retten - kilder og rækkevidde. (https://www.europarl.europa.eu/factsheets/da/sheet/6/eu-retten-kilder-og-rækkevidde). Senest tilgået 11. marts 2021.

- Europa-Parlamentet, Faktabladet om Den Europæiske Unionen: Beskyttelse af de grundlæggende rettigheder i EU. (https://www.europarl.europa.eu/factsheets/da/sheet/146/beskyttelse-af-de-grundl%C3%A6ggende-rettigheder-i-eu). Senest tilgået 11. marts 2021.
- Kjærsdam, Flemming: Henning Mortensen om Schrems II: "Særligt problematisk for amerikanske cloudleverandører". Udgivet 24. februar 2021. (https://itchefer.dk/article/henning-mortensen-om-schrems-ii-saerligt-problematisk-amerikanske-cloudleverandoerer). Senest tilgået 22. april 2021.
- Microsoft: Answering Europe's Call: Storing and Processing EU Data in the EU. Udgivet 6. maj 2021. (https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/). Senest tilgået 7. maj 2021.
- Wired Relations: Notat om Schrems II af Henning Mortensen. Udgivet 12. november 2020. (https://wiredrelations.com/alt-hvad-du-skal-vide-om-schrems-ii/). Senest tilgået 16. april 2021.

Antal anslag



Antal anslag er inkl. mellemrum. Anslag omfatter al brødtekst, undtagen forside, titelblad, abstract, indholdsfortegnelse, litteraturliste samt fodnoter.