Internationale dataoverførsler
– Tredjelandes opnåelse af et tilstrækkeligt beskyttelsesniveau

International data transfers
– The attainment of an adequate level of protection by third countries

af SARA SARMANLU

Formålet med nærværende speciale er at vurdere, hvornår et tredjeland har et tilstrækkeligt beskyttelsesniveau, således at Europa-Kommissionen kan vedtage en tilstrækkelighedsafgørelse for landet i medfør af databeskyttelsesforordningens artikel 45. Vedtages en sådan afgørelse, kan personoplysninger fra EU frit overføres til det pågældende tredjeland, hvorved begge parter nyder væsentlige økonomiske gevinster. Det er derfor af relevans at fastlægge de nærmere krav for opnåelsen af et tilstrækkeligt beskyttelsesniveau.

Med henblik herpå foretages en undersøgelse af det retlige grundlag for tilstrækkelighedsafgørelser, som efterfølges af analyser af de hidtidige tilstrækkelighedsafgørelser samt Schrems II-dommen og endelig en perspektivering til den såkaldte Bruxelles-effekt. Det kan herefter konkluderes, at et tilstrækkeligt beskyttelsesniveau ikke forudsætter et i forhold til EU ækvivalent beskyttelsesniveau, men blot et niveau i tredjelandet, der i det væsentlige svarer til EU's. Det indebærer navnlig krav om tilstedeværelsen af databeskyttelsesregler og -principper i lovgivningen, håndhævelsesmuligheder og tilgængelige retsmidler. Imidlertid vil der af historiske og kulturelle årsager altid være visse forskelle mellem EU's og tredjelandets respektive retssystemer og lovgivning, hvilket dog ikke bør stå i vejen for opnåelsen af en tilstrækkelighedsafgørelse, såfremt de pågældende forskelle ikke medfører et lavere niveau af databeskyttelse. Endelig bemærkes, at tredjelandes tilpasning til EU's krav for at opnå en tilstrækkelighedsafgørelse medfører, at kravene opnår status som de globale standarder.

Indholdsfortegnelse

Abstract

This thesis seeks to examine the requirement in article 45 of the General Data Protection Regulation according to which personal data from the European Union can be transferred to a third country if the European Commission has determined that the country in question has attained an adequate level of protection. It is more specifically the content of the requirement to have an "adequate" level of protection that is to be explored. This is first of all done by analyzing the decisions of the Commission whereby a dozen third countries have thus far been approved as "safe countries" due to their adequate level of protection. It is second of all done by studying the recent Schrems II-decision by the Court of Justice of the European Union.

In doing so, this thesis concludes that the Commission assumes a holistic approach to the examination of the third country in order to ascertain that not only the law of the third country satisfies the EU's requirements, but that the law is also followed in practice. In general, the third country has to present a level of protection that is essentially equivalent to the level of protection established in the EU by the GDPR. Furthermore, the GDPR must always be read in the light of the Charter of Fundamental Rights of the European Union, namely articles 7, 8 and 47. Thus, a violation of these provisions in the charter will simultanously entail the inadequacy of the third country's level of protection.

Finally, this thesis concludes that the adequacy decisions of the Commission gives rise to the so-called "Brussels-effect". This is due to the fact that when third countries are required to live up to the data protection standards single-handedly formulated by the EU, the EU externalises these standards. In other words, the standards gain recognition as the global standards when third countries adapt to them in order to gain approval as a country with an adequate level of protection. Though this adaption to EU-formulated data protection standards by the third countries is voluntary, such adaption is attractive due to the significant financial and commercial advantages linked to it. In other words, the interest in gaining access to the market of the EU is in itself such a substantial reward that it serves as the main motivating force behind the third countries' adaption to the standards set by the EU. As such, the EU uses its market power to set the global standards through the approval of third countries as having "adequate" levels of protection.

1. Introduktion

1.1 Indledning

"At være europæer betyder, at du har ret til at få dine personoplysninger beskyttet af stærk europæisk lovgivning" udtalte daværende Europa-Kommissionsformand Jean-Claude Juncker i sin tale om Unionens tilstand i 2016 og fortsatte, "For privatlivets fred betyder noget i Europa. Det er et spørgsmål om menneskelig værdighed."[1] Junckers fremhævelse af menneskerettighedsaspektet ved databeskyttelse skinner igennem i EU's regulering heraf og udgør en idealistisk aspiration i en tid, hvor personoplysninger bliver behandlet til et hav af forskellige formål og af forskellige aktører. Herunder i forbindelse med overførsler til tredjelande.

[1] Jean-Claude Juncker, Unionens tilstand, s. 10.

I stigende grad opererer europæiske virksomheder nemlig i et miljø, der rækker ud over Unionens grænser, hvilket nødvendiggør overførsler til tredjelande.[2] Tildeles ingen adgang til sådanne internationale dataoverførsler kan EU's virksomheder risikere at halte efter deres globale konkurrenter og Unionen kan lide økonomiske tab, hvilket naturligvis ikke har været hensigten med vedtagelsen af EU's databeskyttelseslovgivning. Idet internationale dataoverførsler således er uundværlige for europæiske virksomheders konkurrencedygtighed, men overførsler til lande, hvor EU's regler ikke finder anvendelse, risikerer at underminere det i EU etablerede høje beskyttelsesniveau, stiller databeskyttelsesforordningens[3] (herefter forordningen) kapitel V krav om tilstedeværelsen af et overførselsgrundlag for, at en international dataoverførsel kan finde sted. Tilstrækkelighedsafgørelser vedtaget af Europa-Kommissionen (herefter Kommissionen) udgør efter forordningens artikel 45 et sådant overførselsgrundlag. Indtil videre er adskillige tredjelandes beskyttelsesniveau blevet godkendt som tilstrækkeligt, senest Japan i 2019 og med udsigt til flere indenfor den nærmeste fremtid, herunder særligt Sydkorea og Latinamerika.[4]

Det er på den baggrund af væsentlig betydning at fastlægge nærmere, hvornår et tredjeland kan forventes at udgøre et sikkert tredjeland med et tilstrækkeligt beskyttelsesniveau, og hvad der ligger bag Kommissions afgørelse heraf. Med henblik herpå foretages nedenfor en kort redegørelse af dette speciales problemformulering, afgrænsning, metode og kilder efterfulgt af en gennemgang af forordningens artikel 45. Dernæst analyseres tilstrækkelighedsafgørelserne truffet i medfør af databeskyttelsesdirektivet[5] (herefter direktivet), som efterfølges af en dyberegående analyse af tilstrækkelighedsafgørelsen vedrørende Japan truffet i medfør af forordningen. En analyse af Schrems II-dommen foretages derefter med en efterfølgende perspektivering til Bruxelles-effekten og endelig en konklusion.

1.2 Problemformulering og afgrænsning

Dette speciale har til formål at vurdere, hvornår et tredjeland besidder et tilstrækkeligt beskyttelsesniveau i medfør af databeskyttelsesforordningens artikel 45.

Da de øvrige overførselsgrundlag i forordningens kapitel V ligger udenfor dette speciales formål, vil de ikke blive redegjort for. Af samme grund vil forordningens artikel 45 som overførselsgrundlag alene blive undersøgt for så vidt angår tredjelande, selvom også internationale organisationer er omfattet af bestemmelsen. Læseren forudsættes i øvrigt at have et vist kendskab til forordningen og dennes begreber. Der vil derfor kun blive redegjort for enkelte begreber vedrørende internationale dataoverførsler i det omfang, det er nødvendigt.

1.3 Metode og kilder

Det centrale regelsæt for nærværende afhandling er databeskyttelsesforordningen, hvis forgænger, databeskyttelsesdirektivet, der desuden vil blive lavet enkelte henvisninger til. Herudover inddrages bestemmelser i Den Europæiske Unions Charter om Grundlæggende Rettigheder[6] (herefter charteret)

[2] Databeskyttelsesforordningen, præambelbetragtning 101.
[3] 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.
[4] Europa-Kommissionen: COM(2017) 7, s. 8.
[5] Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.
[6] Den Europæiske Unions charter om grundlæggende rettigheder, OJ [2000] C 364/1.

i det omfang, det stiller krav til tredjelandes beskyttelsesniveau. Med inddragelse af disse kilder anvendes den retsdogmatiske metode til at beskrive, fortolke og systematisere gældende ret vedrørende internationale dataoverførsler.[7]

Også den komparative metode vil blive anvendt i dette speciale, idet sammenligninger af Kommissionens tilstrækkelighedsafgørelser vil blive foretaget og analyseret for at besvare problemformuleringen.[8] Således vil en stor del af specialet centrere sig om tilstrækkelighedsafgørelserne samt EU-Domstolens (herefter Domstolen) afgørelse i Schrems II-dommen. I den forbindelse inddrages tredjelandenes databeskyttelseslovgivning i det omfang, det er nødvendigt for at redegøre for deres beskyttelsesniveau og klarlægge Kommissionens bevæggrunde for godkendelse.

Endelig inddrages undervejs økonomiske og kulturelle betragtninger som fortolkningsbidrag til den juridiske analyse af tilstrækkelighedskravet i artikel 45.

Af hensyn til den centrale position, som forordningen og charteret indtager i dette speciale, gives nedenfor en kort redegørelse af hver.

1.3.1 Generelt om databeskyttelsesforordningen

Databeskyttelsesforordningen har til formål at sikre et ensartet niveau for databeskyttelse og muliggøre fri udveksling af personoplysninger i Unionen[9] samt at skabe et område med frihed, sikkerhed og retfærdighed.[10] Idet behandling af personoplysninger bør have til formål at tjene menneskeheden, er personoplysninger henhørende EU-borgere genstand for grundig beskyttelse. Beskyttelsen indebærer, at personoplysninger ikke kan behandles uden behandlingsgrundlag eller til ethvert formål. Imidlertid er retten til databeskyttelse ikke en absolut ret – den skal betragtes i lyset af sin funktion i samfundet.[11] Forordningen har nemlig også til formål at bidrage til den internationale samhandel[12] samt skabe økonomiske og sociale fremskridt, herunder i form af en styrkelse af og øget konvergens mellem økonomierne i det indre marked.[13] Ved en forening af de to motiver – beskyttelse af personoplysninger og forfølgelsen af økonomiske interesser – fastsættes i forordningen mulighederne for internationale dataoverførsler, som betinges af tilstedeværelsen af et overførselsgrundlag, der garanterer for beskyttelsen af personoplysningerne. Herom nærmere nedenfor afsnit 2.

1.3.2 Generelt om Den Europæiske Unions Charter om Grundlæggende Rettigheder

Ifølge Traktaten om Den Europæiske Union artikel 6, stk. 1, har charteret "samme juridiske værdi som traktaterne" og dermed status som primær ret. En fortolkning af forordningens bestemmelser skal således til enhver tid ske i lyset af charteret. Hvorvidt et tredjeland har et tilstrækkeligt beskyttelsesniveau skal derfor indeholde en vurdering af, om de grundlæggende rettigheder og frihedsrettigheder, der anerkendes i charteret, er overholdt. Det forudsætter navnlig overholdelsen af den i artikel 7 angivne respekt for privatliv, familieliv, hjem og kommunikation, den i artikel 8 angivne ret til beskyttelse af personoplysninger, der vedrører den pågældende og den i artikel 47 angivne ret til

[7] Jens Evald, Juridisk teori, metode og videnskab, s. 11.

[8] Ibid., s. 183.

[9] Databeskyttelsesforordningen, præambelbetragtning 170.

[10] Ibid., præambelbetragtning 2.

[11] Ibid., præambelbetragtning 4.

[12] Ibid., præambelbetragtning 101.

[13] Ibid., præambelbetragtning 2.

adgang til effektive retsmidler og til en retfærdig rettergang ved en upartisk domstol.[14] Foretages begrænsninger i udøvelsen af disse rettigheder, skal de opfylde kravene angivet i charterets artikel 52, stk. 1, hvilket uddybes nærmere i afsnit 5.4.

2. Internationale dataoverførsler

Alene fra et teknisk perspektiv kan overførsler af personoplysninger ske uden hindringer på tværs af landegrænser. Imidlertid angives i forordningens artikel 44, at internationale dataoverførsler kun kan finde sted, såfremt et af de i kapitel V nævnte overførselsgrundlag foreligger, og såfremt de øvrige bestemmelser i forordningen er opfyldt af den dataansvarlige eller databehandleren. Herved sikres, at det beskyttelsesniveau, som fysiske personer garanteres i medfør af forordningen, ikke undermineres ved overførslen til tredjelandet. Før en gennemgang af den for dette speciale centrale bestemmelse i kapitel V, artikel 45, foretages en redegørelse af begrebet "international dataoverførsel", idet tilstedeværelsen af en sådan overførsel er afgørende for anvendelsen af kapitlets bestemmelser.

2.1 Begrebet "internationale dataoverførsler"

Fra konvention 108,[15] som var det første bindende internationale instrument angående databeskyttelse,[16] til direktivet og endelig til den nugældende forordning er ingen definition af begrebet "internationale dataoverførsler" blevet angivet, selvom de alle tre indeholder bestemmelser om sådanne overførsler. En definition af begrebet kræver derfor en nærmere undersøgelse. Det er klart, at "international dataoverførsel" i hvert fald forudsætter en forståelse af, 1) hvad personoplysninger er, 2) hvornår der foreligger en overførsel, og 3) hvornår overførslen er international.

2.1.1 Personoplysninger

Forordningens artikel 4, nr. 1, definerer personoplysninger som enhver form for information om en identificeret eller identificerbar fysisk person. Med andre ord skal oplysningerne være personhenførbare. Det favner bredt og omfatter blandt andet navn, CPR-nummer, cookies,[17] et fingeraftryk lagret i et chipkort,[18] offentliggørelse af billeder på internettet af genkendelige personer[19] mv.

Er oplysningerne pseudonymiserede, anses de for personoplysninger, hvis de ved brug af supplerende oplysninger kan henføres til en fysisk person. Forordningen finder omvendt ikke anvendelse på anonyme oplysninger, da oplysningerne ikke er personhenførbare. Ved vurderingen af, om en fysisk person er identificerbar ud fra den pågældende oplysning, tages i betragtning alle midler, som med rimelighed kan tænkes anvendt til at identificere personen. Alle objektive forhold inddrages ved afgørelsen af, om midler med rimelighed kan tænkes anvendt, hvilket eksempelvis omfatter omkostningerne og tidsforbruget nødvendigt for identifikation set i forhold til den tilgængelige teknologi.[20]

[14] Ibid., præambelbetragtning 1 og 4.

[15] Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, som i 2018 blev moderniseret under navnet konvention 108+.
Det bemærkes, at Europarådet er et organ separat fra EU, men alle EU's medlemsstater har underskrevet konventionen.

[16] Europarådet, Convention 108 and Protocols.

[17] Bent Ole Gram Mortensen, Dansk Persondataret, s. 35.

[18] Datatilsynets j.nr. 2003-212-0143.

[19] Datatilsynets j.nr. 2002-216-0109

[20] Databeskyttelsesforordningen, præambelbetragtning 26.

2.1.2 Overførsel

Forordningen finder anvendelse på behandling af personoplysninger, "der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register", jf. forordningens artikel 2, stk. 1. Forordningen er således teknologineutral for at undgå en omgåelse af den beskyttelse, som tildeles de registrerede.[21]

Begrebet "behandling" er en samlebetegnelse for forskellige handlinger. Ifølge artikel 4, nr. 2, udgør blandt andet videregivelse og "enhver anden form for overladelse" eksempler på behandling. Sådanne behandlinger udgør samtidig overførsler af personoplysninger. Videregivelse foreligger nemlig, når den dataansvarlige i EU overfører personoplysninger til en dataansvarlig uden for EU. Overladelse foreligger, når den dataansvarlige eller databehandleren overfører personoplysninger til en databehandler udenfor EU.[22] Videregivelsen eller overladelsen kan antage flere former og omfatter eksempelvis digitale overførsler i form af e-mails samt anden ikke-digital behandling såsom den fysiske flytning af en harddisk med personoplysninger til et tredjeland, jf. artikel 2, stk. 1.[23]

2.1.3 Det internationale element

I artikel 3 angives forordningens territoriale anvendelsesområde. Det følger heraf, at anvendelsen af forordningen primært afhænger af, om den dataansvarlige eller databehandleren er etableret i et EU-medlemsland. Men forordningen finder også anvendelse på dataansvarlige og databehandlere, der ikke er etablerede i Unionen, såfremt deres behandlingsaktiviteter angår udbud af varer og tjenester i Unionen eller overvågning af registreredes adfærd i Unionen. Omfattes en dataansvarlig eller databehandler af bestemmelsen og dermed forordningens territoriale anvendelsesområde, foreligger der ikke en international dataoverførsel i kapitel V's forstand, når personoplysninger overføres til dem, selv hvis de befinder sig i et tredjeland. Et land kategoriseres som et tredjeland, såfremt det ikke er medlem af hverken EU eller EØS (Island, Liechtenstein og Norge).[24] Med andre ord foreligger det internationale element ved en international dataoverførsel kun, hvis personoplysningerne overføres til en dataansvarlig eller databehandler i et tredjeland, og disse ikke omfattes af artikel 3 som følge af deres behandlingsaktiviteter.

2.1.4 Sammenfatning

Sammenfattende kan det konkluderes, at en international dataoverførsel foreligger, når der sker en overførsel af oplysninger, der identificerer eller kan identificere en fysisk person, i form af eksempelvis videregivelse eller overladelse til en dataansvarlig eller databehandler, der er etableret i et land, der ikke er medlem af EU eller EØS, og hvis behandling ikke omfattes af forordningens territoriale anvendelsesområde.

2.2 Tilstrækkeligt beskyttelsesniveau

Ifølge forordningens artikel 45, stk. 1, kan overførsel af personoplysninger til et tredjeland finde sted, hvis Kommissionen har fastslået, at det pågældende tredjeland har et tiltrækkeligt beskyttelsesniveau. Såfremt Kommissionen i medfør af bestemmelsens stk. 3 ved en gennemførelsesretsakt fastslår, at tredjelandet har et sådant tilstrækkeligt beskyttelsesniveau, vil en overførsel af personoplysninger til landet ikke kræve specifik godkendelse, uanset den enkelte overførsels nærmere karakter. Herved

[21] Databeskyttelsesforordningen, præambelbetragtnings 15.
[22] Datatilsynet, Vejledning – Overførsel af personoplysninger til tredjelande, s. 5.
[23] Peter Blume, Databeskyttelsesret, s. 259.
[24] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, s. 778.

adskiller dette overførselsgrundlag sig fra de øvrige i kapitel V, da de øvrige overførselsgrundlag forholder sig til en specifik overførsel eller en specifik type overførsel. Artikel 45 udgør derfor det bredeste overførselsgrundlag.[25]

I den gennemførelsesretsakt, hvorved Kommissionen godkender tredjelandets beskyttelsesniveau, fastsættes en mekanisme for regelmæssig revision, som foretages mindst hvert fjerde år, jf. stk. 3. Herved sikres, at EU-borgernes personoplysninger kun overføres til tredjelande, som har et til enhver tid tilstrækkeligt beskyttelsesniveau, uanset at landet allerede tidligere er blevet godkendt. Med henblik herpå overvåger Kommissionen løbende enhver relevant udvikling i tredjelandet for så vidt angår forhold, der kan påvirke tilstrækkelighedsvurderingen, jf. stk. 4. Såfremt det viser sig, at tredjelandet ikke længere har et tilstrækkeligt beskyttelsesniveau, kan Kommissionen ophæve, ændre eller suspendere gennemførelsesretsakten, jf. stk. 5. I en sådan situation er internationale dataoverførsler dog ikke udelukkede, idet de kan foretages efter de øvrige overførselsgrundlag i kapitel V, jf. stk. 7 og præambelbetragtning 107.

Kommissionen foretager sin vurdering af tredjelandets beskyttelsesniveau på grundlag af en række momenter, der oplistes i stk. 2, litra a-c. Der er ikke tale om en udtømmende oplistning, hvilket eksempelvis ses ved, at forordningens præambelbetragtning 105 fastsætter, at Kommissionen også bør høre Det Europæiske Databeskyttelsesråd (herefter Databeskyttelsesrådet) ad, når beskyttelsesniveauet i tredjelandet vurderes, selvom det ikke fremgår af selve artikel 45, stk. 2, litra a-c. Momenterne i denne bestemmelse er dog centrale for forståelsen af et tilstrækkeligt beskyttelsesniveau og gennemgås derfor nærmere nedenfor.

2.2.1 Elementerne i litra a

Ifølge artikel 45, stk. 2, litra a, tager Kommissionen i sin vurdering af beskyttelsesniveauets tilstrækkelighed følgende i betragtning:

> "retsstatsprincippet, respekt for menneskerettighederne og de grundlæggende frihedsrettigheder, relevant lovgivning, både generel og sektorbestemt, herunder vedrørende offentlig sikkerhed, forsvar, statens sikkerhed og strafferet og offentlige myndigheders adgang til personoplysninger, samt gennemførelsen af sådan lovgivning, databeskyttelsesregler, faglige regler og sikkerhedsforanstaltninger, herunder regler for videreoverførsel af personoplysninger til et andet tredjeland eller en anden international organisation, der gælder i dette land (…), retspraksis samt effektive rettigheder for registrerede, som kan håndhæves, og effektiv administrativ og retslig prøvelse for de registrerede, hvis personoplysninger overføres."

Ved tilstrækkelighedsvurderingen skal Kommissionen således tage de grundlæggende værdier, som Unionen bygger på, i betragtning, herunder navnlig menneskerettighederne.[26] Det bemærkes, at det ikke er tilstrækkeligt, at de relevante regler, principper og rettigheder fremgår af tredjelandets lovgivning. Det er afgørende, at datasubjekterne også har mulighed for at håndhæve dem. De nærmere krav til lovgivning og håndhævelse kan dog i praksis være vanskelige, da den nærmere udformning heraf ofte afhænger af tredjelandets retslige kultur, og krav herom har derfor potentiale til at blive opfattet som et uberettiget, udefrakommende indgreb. Som minimum må det dog kunne kræves, at der er rimelig sikkerhed for, at overtrædelser af regler, rettigheder og principper bliver forfulgt og

[25] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, s. 782.

[26] Databeskyttelsesforordningen, præambelbetragtning 104.

håndhævet i tredjelandet, uden at der stilles specifikke krav til midlerne for håndhævelse.[27] Det afgørende er i sidste ende, at tredjelandet har et tilstrækkeligt beskyttelsesniveau – ikke på hvilken måde beskyttelsesniveauet opnås.

2.2.2 Elementerne i litra b

Ved sin vurdering tager Kommissionen ifølge artikel 45, stk. 2, litra b, følgende i betragtning:

> "tilstedeværelse af en eller flere velfungerende uafhængige tilsynsmyndigheder i tredjelandet (…) med ansvar for at sikre og håndhæve, at databeskyttelsesreglerne overholdes, herunder tiltrækkelige håndhævelsesbeføjelser, for at bistå og rådgive de registrerede, når de udøver deres rettigheder, og for samarbejde med tilsynsmyndighederne i medlemsstaterne."

Tilsynsmyndighed, samarbejdsmekanismer med medlemsstaternes databeskyttelsesmyndigheder og tilstedeværelsen af de registreredes effektive rettigheder, som kan håndhæves, herunder ved adgang til administrativ og retslig prøvelse, er således centrale for opnåelsen af et beskyttelsesniveau, der i det væsentlige svarer til EU's.[28] Uden disse vil det være op til den enkelte selv at varetage sin databeskyttelse, og vedkommende vil alene kunne indbringe databeskyttelsesklager for domstolene, hvilket vil medføre en svækkelse af de registreredes databeskyttelse.[29] Som nævnt ovenfor vedrørende litra a kan det dog være problematisk at gribe ind i tredjelandets retslige kultur, hvilket også gælder krav om datatilsyn og den nærmere håndhævelse, og det kan ikke afvises, at andre modeller med et alternativt myndighedsapparat vil kunne sikre effektiv håndhævelse. En helt ens institutionel tilrettelæggelse som tilsynene i EU er derfor ikke påkrævet.[30]

2.2.3 Elementer i litra c

Endelig tager Kommissionen ifølge artikel 45, stk. 2, litra c, følgende i betragtning ved sin vurdering:

> "de internationale forpligtelser, som tredjelandet (…) har påtaget sig, eller andre forpligtelser, der følger af retligt bindende konventioner eller instrumenter og af landets (…) deltagelse i multilaterale eller regionale systemer, navnlig vedrørende beskyttelse af personoplysninger."

Der bør navnlig tages hensyn til, om tredjelandet har tiltrådt konvention 108 og tillægsprotokollen hertil.[31] Konventionen udgør EU's folkeretlige forpligtelse for databeskyttelse, udtrykker grundlæggende principper og tager særligt sigte på dataoverførsler. Derfor tillægges den særlig betydning ved tilstrækkelighedsvurderingen.[32]

3. Tilstrækkelighedsafgørelser i medfør af direktivet

En nærmere fastsættelse af kravene til tredjelandes beskyttelsesniveau forudsætter en analyse af de hidtidige tilstrækkelighedsafgørelser truffet af Kommissionen.

---

[27] Peter Blume, Databeskyttelsesret, s. 266.

[28] Databeskyttelsesforordningen, præambelbetragtning 104.

[29] Peter Blume, Databeskyttelsesret, s. 266.

[30] Peter Blume, Databeskyttelsesret, s. 266-267.

[31] Databeskyttelsesforordningen, præambelbetragtning 105.

[32] Peter Blume, Databeskyttelsesret, s. 59.

Tilstrækkelighedsafgørelserne blev før forordningen truffet i medfør af direktivet. I lighed med forordningen kunne videregivelse af personoplysninger til tredjelande ske, hvis tredjelandets beskyttelsesniveau fandtes at være tilstrækkeligt, jf. direktivets artikel 25. Selvom direktivet ikke oplister momenter i tilstrækkelighedsvurderingen på samme måde som forordningens artikel 45, stk. 2, litra a-c, kan afgørelserne efter direktivet stadig bidrage til fastlæggelsen af, hvorledes Kommissionen vurderer tredjelande, og hvornår tredjelandene har opnået et tilstrækkeligt beskyttelsesniveau. Afgørelserne truffet efter direktivet har altså ikke mistet deres relevans efter forordningens indtræden.

Elleve lande er blevet godkendt som sikre tredjelande i medfør af direktivet. Disse er Schweiz[33], Canada (kun kommercielle organisationer)[34], Argentina[35], Guernsey[36], Isle of Man[37], Jersey[38], Færøerne[39], Andorra[40], Israel[41], Uruguay[42] og New Zealand.[43]

Det er karakteristisk for tilstrækkelighedsafgørelserne truffet i medfør af direktivet, at mange af de angivne betragtninger gentager sig på tværs af afgørelserne. Afgørelserne for de tre britiske besiddelser, Guernsey, Isle of Man og Jersey, er endda strukturelt og indholdsmæssigt fuldstændigt ens. Nedenfor gennemgås de momenter, som nævnes i alle eller flere af afgørelserne. Herefter knyttes nogle bemærkninger til tredjelandenes databeskyttelseslovgivning og afslutningsvist diskuteres visse uoverensstemmelser i tilstrækkelighedsvurderingerne.

3.1 Samtlige forhold af indflydelse

I alle afgørelserne nævnes, at vurderingen skal foretages "på grundlag af samtlige de forhold, der har indflydelse på en videregivelse [af personoplysninger]".[44] Desværre uddybes ikke yderligere, hvad dette nærmere indebærer. Generelt præger det afgørelserne truffet i medfør af direktivet, at de er ordknappe og bidrager beskedent til fastlæggelsen af, hvad der nærmere kræves af et tredjelands beskyttelsesniveau. Af bemærkningen om, at samtlige forhold inddrages, kan det dog udledes, at Kommissionen antager en holistisk tilgang til tilstrækkelighedsvurderingen. Beskyttelsesniveauet skal granskes fra ethvert relevant perspektiv, herunder ved en undersøgelse af indholdet af lovgivningen, håndhævelsen, offentlige myndigheders adgang til oplysningerne, videregivelse til andre tredjelande mv.

3.2 Ønske om ikke at diskriminere

Tredjelandene vil uundgåeligt have forskellige opfattelser af begrebet "databeskyttelse" som følge af deres respektive historiske, kulturelle og retslige baggrund. Derfor angives i alle afgørelserne, at vurderingen af beskyttelsesniveauets tilstrækkelighed skal foretages på en sådan måde, at der ikke vilkårligt eller uberettiget diskrimineres mellem tredjelande, hvor lignende forhold gør sig gældende.[45]

[33] Beslutning 2000/518/EF.
[34] Beslutning 2002/2/EF.
[35] Beslutning 2003/490/EF.
[36] Beslutning 2003/821/EF.
[37] Beslutning 2004/411/EF.
[38] Beslutning 2008/393/EF.
[39] Beslutning 2010/146/EU.
[40] Beslutning 2010/625/EU.
[41] Beslutning 2011/61/EU.
[42] Beslutning 2012/484/EU.
[43] Beslutning 2013/65/EU.
[44] Eksempelvis Beslutning 2000/518/EF, betragtning 3, Beslutning 2003/490/EF, betragtning 3, og Beslutning 2003/821/EF, betragtning 3
[45] Eksempelvis Beslutning 2010/625/EU, betragtning 4, og Beslutning 2012/484/EU, betragtning 4.

Foretages tilstrækkelighedsvurderingen ikke med dette formål in mente, vil det indebære en risiko for diskrimination mellem tredjelande, hvis opfattelse af databeskyttelse stemmer overens med EU's, og tredjelande, hvis opfattelse ikke gør, selvom forskellen i opfattelsen af databeskyttelse ikke nødvendigvis er en afspejling af sidstnævntes beskyttelsesniveau.

3.3 Domstolsprøvelse og tilsynsmyndighed

Alle afgørelserne nævner, at anvendelsen af databeskyttelsesretlige regler skal sikres ved domstolsprøvelse og tilsynsmyndighedens undersøgelses- og interventionsbeføjelser.[46] Om Argentina bemærkes eksempelvis, at landets lovgivning indeholder bestemmelser om etablering af en national kontrolmyndighed, der har undersøgelses- og indgrebsbeføjelser med henblik på at sikre opfyldelse af lovens mål. Ligeledes opfyldes disse mål ved, at lovgivningen hjemler anvendelsen af afskrækkende sanktioner af administrativ og strafferetlig karakter.[47] I enkelte af afgørelserne bemærkes desuden, at den registrerede har mulighed for at gøre erstatningskrav gældende ved domstolene i tilfælde af ulovlig behandling af vedkommendes personoplysninger.[48]

3.4 Artikel 29-gruppen

I alle afgørelserne har Kommissionen lagt vægt på, at artikel 29-gruppen[49] (nu erstattet af Databeskyttelsesrådet) har afgivet en positiv udtalelse om tilstrækkeligheden af landets beskyttelsesniveau.[50] Kun i få tilfælde uddybes det nærmere indhold eller betydningen af udtalelsen. I afgørelsen for Andorra bemærkes, at artikel 29-gruppen i sin udtalelse opfordrer de andorranske myndigheder til løbende at vedtage yderligere bestemmelser, som kan bidrage til at udvide anvendelsen af den andorranske lovgivning til elektroniske individuelle afgørelser, da de ved afgørelsestidspunktet ikke udtrykkeligt er omfattede af andorransk databeskyttelseslovgivning.[51] Vedrørende Israel angiver Kommissionen, at artikel 29-gruppen har afgivet en positiv udtalelse, som dog samtidig tilskynder de israelske myndigheder til at vedtage yderligere bestemmelser for blandt andet eksplicit at fastslå, at proportionalitetsprincippet finder anvendelse ved databehandling i den private sektor.[52] Dette indikerer, at enkelte mangler kan eksistere i tredjelandets databeskyttelseslovgivning, uden at det forhindrer en positiv udtalelse fra artikel 29-gruppen og en efterfølgende godkendelse som sikkert tredjeland fra Kommissionen, dog under forudsætning af eller med forventning om, at manglen udbedres i fremtiden, og den ikke individuelt set er af afgørende betydning for beskyttelsesniveauet.

3.5 Mulighed for suspendering

Det sidste element, som alle afgørelserne har til fælles, er angivelsen af muligheden for suspendering af specifikke dataoverførsler, selvom tredjelandets beskyttelsesniveau er godkendt som tilstrækkeligt. Det vil kunne ske med henblik på at sikre, at de kompetente myndigheder i medlemsstaterne kan beskytte datasubjekterne.[53] Suspendering angives blandt andet at kunne forekomme, hvis de i tredjelandet etablerede beskyttelsesnormer overtrædes, hvis en overførsel af personoplysninger vil kunne

[46] Eksempelvis Beslutning 2013/65/EU, betragtning 11, og Beslutning 2010/146/EU, betragtning 7.
[47] Beslutning 2003/490/EF, betragtning 14.
[48] Eksempelvis Beslutning 2003/490/EF, betragtning 14, og Beslutning 2012/484/EU, betragtning 10.
[49] Etableret i medfør af direktivets artikel 29 som en uafhængig rådgivende arbejdsgruppe.
[50] Eksempelvis Beslutning 2012/484/EU, betragtning 18, og Beslutning 2013/65/EU, betragtning 15.
[51] Beslutning 2010/625/EU, betragtning 14.
[52] Beslutning 2011/61/EU, betragtning 15.
[53] Eksempelvis Beslutning 2010/146/EU, betragtning 8, og Beslutning 2012/484/EU, betragtning 16.

skabe "overhængende risiko for alvorlig skade for de registrerede", og hvis myndighederne ikke forventes at reagere på en overtrædelse.[54] Dermed er en tilstrækkelighedsafgørelse ikke carte blanche til frie dataoverførsler fra EU til tredjelandet, såfremt der i specifikke tilfælde foreligger momenter, der kompromitterer den beskyttelse, som EU har fået indtryk af, at tredjelandet tildeler EU-borgerne.

3.6 Konvention 108

I nogle tilstrækkelighedsafgørelser lægges der vægt på tredjelandets ratifikation af konvention 108.[55] Ratifikation af konventionen er dog ikke en ufravigelig forudsætning for, at landets beskyttelsesniveau anses for tilstrækkeligt. Dette blev allerede antydet ved, at det andet godkendte tredjeland, Argentina, ikke havde ratificeret konventionen, men blev alligevel anset for at have et tilstrækkeligt beskyttelsesniveau.[56] Såfremt andre forsikringer for databeskyttelse findes i tredjelandets lovgivning, er det således ikke i sig selv afgørende, hvorvidt tredjelandet har ratificeret konventionen. Dette lader også til at være blevet bekræftet i afgørelsen for Uruguay. Mens landet ikke havde ratificeret konventionen på afgørelsestidspunktet, lagde Kommissionen vægt på, at landet var part i San José de Costa Rica-pagten (en menneskerettighedskonvention), hvori retten til privatlivets fred anerkendes, og at landet havde accepteret Den Interamerikanske Menneskerettighedsdomstols jurisdiktion. Landet udtrykte således sin respekt for databeskyttelse på andre måder end ved ratifikation af konventionen, hvilket var tilstrækkeligt til at blive godkendt som sikkert tredjeland. Kommissionen bemærkede dog, at Uruguay var blevet opfordret af Europarådet til at tiltræde konventionen, hvilket landet også endte med året efter tilstrækkelighedsafgørelsens vedtagelse. Udsigten til Uruguays ratifikation af konventionen indgik således alligevel i Kommissionens vurdering i et vist omfang.[57]

Ratifikation af konventionen må opsummerende fortolkes som et argument for, at tredjelandets beskyttelsesniveau er tilstrækkeligt, da Kommissionen har lagt vægt på det i flere afgørelser, og ratifikation er blevet nævnt i den senere forordnings præambelbetragtning 105 som et moment i tilstrækkelighedsvurderingen. Ikke desto mindre er ratifikation ikke i sig selv et ufravigeligt krav til tredjelandet.

3.7 Forklaringer og forsikringer

Et sidste fællestræk blandt visse afgørelser er angivelsen af inddragelsen af forklaringer og forsikringer fra tredjelandets regering og myndigheder i Kommissionens vurdering.[58] Eksempelvis har databeskyttelsesmyndighederne i Andorra afgivet forklaringer for fortolkningen af landets lovgivning og forsikret, at lovbestemmelserne anvendes i overensstemmelse med den angivne fortolkning. Kommissionen påpeger, at tilstrækkelighedsafgørelsen tager udgangspunkt i disse forklaringer og forsikringer og tager også forbehold for dem.[59] I afgørelsen vedrørende Uruguay angives mere specifikt, hvad forklaringerne har angået, hvilket blandt andet omfatter en forklaring af, at undtagelserne i lovgivningen, som hjemler videregivelse af oplysninger, ikke kan tolkes til at have bredere anvendelse

[54] Muligheden for suspendering angives for alle afgørelsernes vedkommende i deres artikel 3 – med undtagelse af afgørelsen for New Zealand og Uruguay, hvor det angives i deres artikel 2.

[55] Beslutning 2000/518/EF, betragtning 9, Beslutning 2003/821/EF, betragtning 6, Beslutning 2004/411/EF, betragtning 6, Beslutning 2008/393/EF, betragtning 6, og Beslutning 2010/625/EU, betragtning 9.

[56] For tilstrækkelighedsafgørelser generelt var Canada det andet land, der modtog en sådan afgørelse, der dog kun angår kommercielle organisationer.

[57] Beslutning 2012/484/EU, betragtning 13.

[58] Eksempelvis Beslutning 2003/490/EF, betragtning 15, Beslutning 2010/625/EU, betragtning 11, Beslutning 2011/61/EU, betragtning 11og Beslutning 2012/484/EU, betragtning 11.

[59] Beslutning 2010/625/EU, betragtning 11.

end reglerne i direktivet.[60] Således afklarer myndighederne i Uruguay visse forhold ved landets lovgivning, som ellers kunne have talt imod en godkendelse af landet som sikkert tredjeland.

3.8 Landenes lovgivning

Tredjelandene har hver især deres egen databeskyttelseslovgivning, som indtager en central plads i Kommissionens vurdering. De fleste tredjelande har forfatningsfæstede databeskyttelsesprincipper, som suppleres af databeskyttelseslovgivning,[61] hvilket er en struktur, der minder om reguleringen i EU, hvor grundlæggende rettigheder og principper findes i charteret, mens den nærmere regulering findes i forordningen. Således findes de generelle bestemmelser om databeskyttelse for Argentinas vedkommende i landets forfatning, hvori beskyttelse af personoplysninger udgør en grundlæggelse rettighed, og hvor der opstilles en særlig klageprocedure ved domstolene til beskyttelse af personoplysninger.[62] Disse forfatningsbestemmelser er præciseret i og suppleret af yderligere lovgivning, der blandt andet omhandler de registreredes rettigheder, de dataansvarlige og databehandlernes forpligtelser, tilsynsmyndighed og sanktioner.[63]

Men ikke alle tredjelande følger denne struktur. Både Israel og New Zealand har ingen skriftlig forfatning i traditionel forstand, hvori grundlæggende rettigheder ellers typisk bliver nedfældet. I Israel har visse grundlæggende love forfatningsstatus, og disse suppleres af omfattende retspraksis, idet landet – modsat medlemsstaterne i EU – har et common law-retssystem. I en af disse grundlæggende love med forfatningsstatus ses retten til privatlivets fred fastslået.[64] Herudover er landets databeskyttelseslovgivning i betydeligt omfang inspireret af direktivet.[65] Ligeledes har New Zealand en række love af særlig forfatningsmæssig betydning, som anses for "higher law" i den forstand, at de udgør en del af landets forfatningsmæssige grundlag. Adskillige af disse love er af databeskyttelsesretlig relevans.[66] I modsætning til Israel og flere andre tredjelande er New Zealands øvrige databeskyttelseslovgivning dog ikke inspireret af direktivet, idet landets databeskyttelsesretlige regler blev vedtaget før direktivet.[67]

Godkendelse af et tredjelands beskyttelsesniveau er således ikke betinget af, at landet har nøjagtig samme lovgivningsstruktur som EU. Ligeledes er det ikke et krav, at tredjelandets lovgivning er inspireret af direktivet, selvom det har været tilfældet for flere af tredjelandene.[68] Kommissionen lægger vægt på den faktiske tilstedeværelse af tilstrækkelige garantier og værn for EU-borgernes databeskyttelse fremfor at stille specifikke og formalistiske krav. Herved respekteres også de naturlige forskelle mellem tredjelandenes retslige kultur.

3.9 Behovet for en konsekvent tilgang

Mens ovenstående gennemgang har omhandlet de momenter, der genfindes i alle eller de fleste afgørelser, findes også uoverensstemmelser i vurderingerne af tredjelandene.

---

[60] Beslutning 2012/484/EU, betragtning 11 og 12.

[61] Eksempelvis Beslutning 2010/625/EU, betragtning 6 og 8.

[62] Beslutning 2003/490/EF, betragtning 6-7.

[63] Ibid., betragtning 5 og 8.

[64] Beslutning 2011/61/EU, betragtning 5.

[65] Ibid., betragtning 6-8.

[66] Beslutning 2013/65/EU, betragtning 5-6.

[67] Ibid., betragtning 7.

[68] Eksempelvis Beslutning 2003/821/EF, betragtning 7, beslutning 2004/411/EF, betragtning 7 og 2008/393/EF, betragtning 7.

Til trods for angivelsen i alle tilstrækkelighedsafgørelserne om, at hvert tredjelands opfattelse af databeskyttelse skal tages i betragtning, således at ingen bliver diskrimineret, viser EU's praksis, at de momenter, der bliver lagt til grund for en godkendelse eller ikke-godkendelse, til tider kan være arbitrære eller af tvivlsom relevans. Et eksempel herpå er betydningen af, hvornår tredjelandets databeskyttelseslovgivning er vedtaget. Ved den indledende tilstrækkelighedsvurdering af Tunesien blev tilstrækkeligheden af landets beskyttelsesniveau betvivlet under henvisning til, at landets databeskyttelseslovgivning var ny. Databeskyttelseslovgivningen i Mauretanien fandtes ligeledes at være for ny, og der blev desuden lagt vægt på den begrænsede retspraksis om databeskyttelse. Marokkos databeskyttelseslovgivning trådte i kraft samme år, som landet blev genstand for en indledende tilstrækkelighedsvurdering, som angav, at det var for tidligt at konkludere, hvorvidt beskyttelsesniveauet var tilstrækkeligt eller ej. I modsætning til disse lande blev Canada i 2002 godkendt som sikkert tredjeland, hvilket var to år før landets databeskyttelseslov trådte i kraft.[69] Ligeledes blev Argentina godkendt som sikkert tredjeland, før landets databeskyttelseslovgivning var trådt i kraft.[70] Det er derfor vanskeligt som tredjeland at vide, hvornår ens databeskyttelseslovgivning har eksisteret i tilstrækkelig tid til, at man kan regne med godkendelse, og det rejser bekymringer om forskelsbehandling mellem tredjelandene.

I sin udtalelse vedrørende Monaco – som i dag stadig ikke er et godkendt tredjeland – bemærkede artikel 29-gruppen, at landets tilsynsmyndighed ikke havde tilstrækkelig økonomisk og personel uafhængighed.[71] Af udtalelsen fremgik dog også, at det organ, der foretog den indledende vurdering af Monaco, havde fastsat nogle trin, som landet kunne følge for at imødekomme problemerne ved tilsynets uafhængighed. Monaco fik altså hjælp fra EU til at forbedre sit beskyttelsesniveau uden at have anmodet om det. Det rejser spørgsmålet om, hvor langt EU bør gå for at hjælpe tredjelandet med at opnå et tilstrækkeligt beskyttelsesniveau. Især eftersom ingen sådanne forsøg blev gjort på at hjælpe Quebec, hvis beskyttelsesniveau også blev vurderet af artikel 29-gruppen, på rette vej trods landets anmodninger herom.[72] Sådan hjælp tilsyneladende arbitrært afgivet til den ene men ikke den anden vækker i hvert fald bekymringer om en retfærdig behandling af tredjelandene.

Også kravene til tredjelandets regulering af følsomme personoplysninger fremstår svingende. Både Canada og New Zealand blev begge godkendt som sikre tredjelande, selvom de ikke havde lovregler, som specifikt definerede og regulerede følsomme personoplysninger.[73] I modsætning hertil var en utilstrækkelig regulering af følsomme personoplysninger medvirkende til den manglende godkendelse af Quebec, Marokko og Tunesien. For Tunesiens vedkommende skyldtes det mere specifikt, at landets regulering af følsomme personoplysninger ikke inkluderede en udtrykkelig angivelse af oplysninger om personers seksualitet.[74] De specifikke krav til reguleringen af følsomme personoplysninger forekommer derfor ikke helt klar.

I artikel 29-gruppens udtalelse om New Zealand blev syv mangler ved landets lovgivning påpeget, men deres betydning blev bagatelliseret under henvisning til landets geografiske isolation, størrelsen og karakteren af landets økonomi, og idet man ikke forventede data overført til landet i betydeligt

[69] Jennifer Stoddart m.fl., The European Union's Adequacy Approach, s. 150.
[70] Elisabeth Meddin, The Cost of Ensuring Privacy, s. 1007
[71] Jennifer Stoddart m.fl., The European Union's Adequacy Approach,, s. 147.
[72] Elisabeth Meddin, The Cost of Ensuring Privacy, s. 1007.
[73] Jennifer Stoddart m.fl., The European Union's Adequacy Approach, s. 147.
[74] Ibid., s. 148.

omfang. Det aktualiserer et endnu ubesvaret spørgsmål om, hvorvidt et tredjeland geografisk og økonomisk tættere på EU, hvortil data forventes overført i mere betydeligt omfang, ville have modtaget den samme behandling og godkendelse trods mangler ved landets lovgivning.[75] Med andre ord vækker det tvivl om, hvorvidt tredjelandene skal leve op til forskellige standarder for at opnå EU's godkendelse afhængigt af deres økonomi, geografiske placering og omfanget af forventede dataoverførsler til landet.

3.10 Delkonklusion

Som konstateret ovenfor deler tilstrækkelighedsafgørelserne truffet i medfør af direktivet en del fællestræk, der som følge af deres kortfattethed og manglende uddybninger i beskedent omfang bidrager til en fastlæggelse af, hvad "tilstrækkeligt beskyttelsesniveau" nærmere indebærer. Der har dog dannet sig et mønster for, at Kommissionen anlægger en holistisk tilgang, hvor lovgivning og håndhævelse bliver tillagt stor vægt, og hvor visse andre momenter typisk inddrages, herunder forklaringer og forsikringer afgivet af landets myndigheder, artikel 29-gruppens udtalelse mv. Mange af disse momenter genfindes i forordningens artikel 45, stk. 2, litra a-c, som således er en afspejling og forlængelse af betragtningerne angivet i tilstrækkelighedsafgørelserne truffet i medfør af direktivet. Der eksisterer dog også visse uoverensstemmelser i tilstrækkelighedsvurderingerne, hvilket fremhæver et behov for klarere kommunikation med tredjelandene om, hvad der nærmere kræves af dem. Det er dog i en vis grad allerede adresseret ved forordningen, da artikel 45, stk. 2, litra a-c oplister, hvad Kommissionen lægger vægt på i sin vurdering.

4. Tilstrækkelighedsafgørelsen i medfør af forordningen

Japan er ved gennemførelsesafgørelsen (EU) 2019/419[76] blevet godkendt som et tredjeland med et tilstrækkeligt beskyttelsesniveau efter to års forhandlinger med EU.[77] Udover at være den første (og indtil videre eneste) tilstrækkelighedsafgørelse truffet i medfør af forordningens artikel 45 markerer afgørelsen sig ved at være den første gensidige afgørelse, hvorved både EU og Japan har anerkendt tilstrækkeligheden af den anden parts beskyttelsesniveau. Det bemærkes i øvrigt, at afgørelsen er begrænset til alene at angå overførsel af personoplysninger til erhvervsdrivende i Japan, jf. afgørelsens betragtning 4.

Afgørelsen adskiller sig væsentligt fra de tidligere afgørelser truffet i medfør af direktivet. Mens de tidligere afgørelser har haft en længde på mellem 2-4 sider, har denne afgørelse en længde på 58 sider. På disse sider gennemgår Kommissionen de ved afgørelsen relevante momenter med hidtil uset detaljerighed og grundighed.

Nedenfor gennemgås kort selve grundlaget for Kommissionens tilstrækkelighedsvurdering af Japan, som efterfølges af en analyse af afgørelsen. Idet afgørelsen er truffet i medfør af artikel 45, vil analysen følge strukturen i bestemmelsens stk. 2, litra a-c. Analysen afsluttes med en gennemgang af Databeskyttelsesrådets udtalelse om Japans beskyttelsesniveau, nogle bemærkninger om revisionsmekanismen fastsat i afgørelsen og endelig en kort diskussion om indflydelsen af økonomiske interesser og kulturelle forskelle. Således vil analysen af denne tilstrækkelighedsafgørelse være mere

[75] Ibid., s. 150.

[76] Kommissionens gennemførelsesafgørelse (EU) 2019/419 af 23. januar 2019 i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679 vedrørende Japans tilstrækkelige beskyttelse af personoplysninger i henhold til loven om beskyttelse af personlige oplysninger.

[77] Flora Y. Wang, Cooperative Data Privacy, s. 671.

indgående end den af de tidligere afgørelser, hvilket også skyldes, at denne afgørelse vil sætte en præcedens for fremtidige ansøgninger om tilstrækkelighedsafgørelser samt for revisionen af de tidligere afgørelser.[78]

4.1 Grundlaget for vurderingen

I betragtning 3 angives, at afgørelsen finder sted på grundlag af "en omfattende analyse af det pågældende tredjelands retsorden, både hvad angår de regler, der finder anvendelse på dataimportøren, og de begrænsninger og garantier, der gælder med hensyn til offentlige myndigheders adgang til personoplysninger." Kommissionen skal fastslå, om tredjelandet har et beskyttelsesniveau, som "i det væsentlige svarer" til EU's, og der kræves således ikke "et identisk beskyttelsesniveau. Det betyder navnlig, at de midler, som tredjelandet anvender, kan være forskellige fra de midler, som gennemføres inden for Den Europæiske Union, så længe de i praksis viser sig at være effektive med henblik på at sikre et tilstrækkeligt beskyttelsesniveau. Standarden for tilstrækkelighed er derfor ikke, at EU-reglerne duplikeres punkt for punkt. Testen består snarere i, om det pågældende udenlandske system som helhed sikrer det krævede beskyttelsesniveau gennem kerneindholdet i retten til privatlivets fred og den effektive gennemførelse, overvågning og håndhævelse heraf."

4.2 Momenter, der falder under litra a

Kommissionen inddrager i sin tilstrækkelighedsvurdering en række momenter, som nævnes i artikel 45, stk. 2, litra a, og som gennemgås nedenfor.

4.2.1 Forfatning og lovgivning

Den japanske forfatning tildeler ikke en udtrykkelig ret til privatliv og databeskyttelse. Imidlertid anerkendes i forfatningens artikel 13 respekten for grundlæggende frihedsrettigheder. Her angives, at "[a]lle mennesker respekteres som individer. Deres ret til liv, frihed og stræben efter lykke skal, i det omfang dette ikke griber ind i den offentlige velfærd, være det vigtigste hensyn i lovgivningen og i myndighedernes øvrige anliggender.", jf. betragtning 6-8. Denne bestemmelse, sammenholdt med landets retspraksis, angiver implicit, at fysiske personer har en ret til privatliv og databeskyttelse. Det står i modsætning til den eksplicitte anerkendelse af rettighederne i forordningen og charteret.[79]

Den for tilstrækkelighedsafgørelsen centrale databeskyttelseslov i Japan er Loven om beskyttelse af personlige oplysninger (APPI), som angår erhvervsdrivendes behandling af personoplysninger, jf. betragtning 9 og 10. Beskyttelsen af individers rettigheder og interesser angives som formålet med loven, men også datas evne til at skabe nye industrier samt realisere økonomiske mål anerkendes som væsentlig.[80] Japan lægger således betydelig vægt på den økonomiske gevinst ved data og beskyttelsen heraf, mens angivelsen af retten til privatliv og databeskyttelse i forordningen og charteret viser, at EU særligt betoner menneskerettighedsaspektet af databeskyttelse. Afgørelsen er derfor også udtryk for et møde mellem to forskellige anskuelser af databeskyttelse og formålet hermed, hvilket uddybes nærmere i afsnit 4.7.

APPI trådte i kraft i 2003, blev moderniseret i 2015 og er sidenhen blevet ændret i takt med interne udviklinger i landet og forhandlingerne med EU. Ændringerne bestod blandt andet af indførelsen af visse individuelle rettigheder samt oprettelsen af en uafhængig tilsynsmyndighed (PPC) med ansvar

[78] Databeskyttelsesrådet, Udtalelse 28/2018, betragtning 28.
[79] Se eksempelvis databeskyttelsesforordningens præambelbetragtning 2 og 4 samt charterets artikel 7 og 8.
[80] Flora Y. Wang, Cooperative Data Privacy, s. 669.

for tilsyn med og håndhævelse af APPI. Som konsekvens heraf nærmede det japanske databeskyttelsessystem sig EU's, jf. betragtning 9 og 11.

Udover APPI findes også Loven om beskyttelse af personlige oplysninger i administrative organer (APPIHAO), Loven om beskyttelse af personlige oplysninger i inkorporerede agenturer (APPI-IAA) og sektorspecifikke regler, som er inddraget i Kommissionens vurdering, dog i mindre omfang end APPI, jf. betragtning 9 og 93.

4.2.2 Supplerende regler

Trods ændringerne ved APPI, hvorved Japan nærmede sig EU's regulering, foreligger der stadig forskelle mellem de to parters databeskyttelsesregler. Forskellene er søgt udbedret ved tilføjelsen af nogle supplerende regler til APPI, som er vedlagt som bilag I til tilstrækkelighedsafgørelsen. De supplerende regler er blevet vedtaget af tilsynsmyndigheden, PPC, med henblik på at øge beskyttelsen af personoplysninger, er retligt bindende for de japanske erhvervsdrivende og kan håndhæves af både PPC og domstolene på samme måde som de øvrige regler i APPI, jf. betragtning 15. I de supplerende regler angives blandt andet, at oplysninger om seksuel orientering og fagforeningsmæssigt tilhørsforhold fremover behandles som følsomme personoplysninger, hvilket hidtil ikke havde været tilfældet. De supplerende regler fastsætter også, at registreredes rettigheder kan påberåbes for alle personoplysninger, der overføres fra EU, uanset deres opbevaringsperiode, hvorimod den almindelige lovgivning fastsætter, at rettighederne ikke kan påberåbes, hvis personoplysningerne er fastsat til at blive slettet indenfor seks måneder.[81]

De supplerende regler finder alene anvendelse på personoplysninger overført fra EU til Japan og således ikke på andre personoplysninger i Japan, som altså alene reguleres af APPI's almindelige (og mindre strenge) regler. Det betyder, at Japan har et toleddet databeskyttelsessystem.[82] Det rejser spørgsmålet om, hvorvidt et tredjeland kan have et beskyttelsesniveau, der i det væsentlige svarer til EU's og dermed er tilstrækkeligt efter artikel 45, når en del af retsgrundlaget, hvorpå vurderingen af beskyttelsesniveauet foretages, ekskluderer behandlingen af tredjelandets egne borgeres personoplysninger. De supplerende regler etablerer trods alt kun et højere beskyttelsesniveau for EU-borgerne, men ikke for Japans egne borgere eller for andre udenlandske borgere, hvis oplysninger behandles i landet. Spørgsmålet er ikke besvaret i selve afgørelsen, som i stedet efterlader et indtryk af, at tredjelande kan overkomme mangler ved deres databeskyttelseslovgivning og dermed opfylde kravet om et tilstrækkeligt beskyttelsesniveau ved hjælp af lovgivning (eller andre lovgivningsmæssige redskaber som de supplerende regler), der har til formål at etablere et højere beskyttelsesniveau kun for EU-borgerne.[83]

Vurderingen af landets beskyttelsesniveau sker således på grundlag af både APPI og de supplerende regler. Databeskyttelsesrådet udtrykker i sin udtalelse om Japans beskyttelsesniveau glæde over landets indsats for ved hjælp af de supplerende regler at bygge bro over parternes forskellige systemer for databeskyttelse.[84] Imidlertid bemærker Rådet også, at selve den omstændighed, at supplerende regler er nødvendige, er et tegn på, at den eksisterende generelle databeskyttelseslovgivning ikke i sig selv lever op til EU's krav. På den baggrund opfordres Kommissionen til at sikre, at et system for fri overførsel mellem Japan og EU er bæredygtigt, pålideligt og med effektiv praktisk håndhævelse.[85]

[81] Databeskyttelsesrådet, Udtalelse 28/2018, betragtning 9 og afgørelsens betragtning 26.
[82] Flora Y. Wang, Cooperative Data Privacy, s. 687-688.
[83] Graham Greenleaf, Japan: EU Adequacy Discounted, s. 8.
[84] Databeskyttelsesrådet, Udtalelse 28/2018, betragtning 29.
[85] Ibid., betragtning 43.

4.2.3 Principper

I forordningens artikel 5, stk. 1, litra a-f, angives en række grundlæggende principper for databehandling, og alle disse genfindes i APPI. Japansk lovgivning indeholder således et formålsbegrænsningsprincip, et princip om lovlighed, rimelighed og gennemsigtighed, et dataminimeringsprincip, et princip om rigtighed, et princip om opbevaringsbegrænsning og endelig et princip om integritet og fortrolighed, jf. betragtning 39-64. Også forordningens princip om ansvarlighed udtrykt i artikel 5, stk. 2, har sin pendant i APPI, hvorefter den databehandlende erhvervsdrivende skal træffe passende organisatoriske foranstaltninger for at sikre effektiv overholdelse af sine forpligtelser samt dokumentere overholdelsen heraf, jf. betragtning 70-74.

4.2.4 Rettigheder

Databeskyttelsesforordningen tildeler den registrerede en række rettigheder angivet i artikel 15-18 og 20-21, som delvist genfindes i APPI. Den registrerede tildeles i APPI en ret til indsigt, berigtigelse, sletning og indsigelse, jf. betragtning 81.

Retten til indsigelse angår dog kun indsigelser mod videregivelsen af personoplysninger til tredjemand, jf. betragtning 92. Således har den registrerede i modsætning til forordningens artikel 21 ingen ret i APPI til at modsætte sig behandling med henblik på direkte markedsføring. Dog angiver en af de supplerende regler, at den erhvervsdrivende er forpligtet til at behandle de personoplysninger, der modtages fra EU, til det samme formål, som oplysningerne er blevet overført efter, medmindre den registrerede giver sit samtykke til andet anvendelsesformål. Det betyder, at hvis overførslen fra EU er foretaget til andet formål end direkte markedsføring, vil den databehandlende erhvervsdrivende i Japan være afskåret fra at behandle oplysningerne med henblik på direkte markedsføring uden den registreredes samtykke, jf. betragtning 89. Dette illustrerer, at Kommissionen alene kræver, at tredjelandet ikke underminerer det i EU etablerede databeskyttelsesniveau og ikke, at tredjelandets databeskyttelseslovgivning skal følge forordningen ordret, hvis virkningen alligevel er den samme. Det samme illustreres af, at APPI ikke indeholder regler om automatiske afgørelser i modsætning til forordningens artikel 22, men at der findes sektorbestemte regler herom i den japanske lovgivning, jf. betragtning 93.

Der er således ikke et fuldstændigt sammenfald mellem rettighederne tildelt efter forordningen og efter APPI, hvilket må fortolkes som heller ikke at være et krav. Afgørelsen antyder i øvrigt også, at visse rettigheder har større indflydelse for sikringen af et tilstrækkeligt databeskyttelsesniveau end andre. Retten til indsigt, berigtigelse, sletning og indsigelse er nemlig her i sig selv tilstrækkeligt tungtvejende til, at beskyttelsesniveauet opfylder kravene i artikel 45, selvom der ikke er nogen ret til begrænsning eller dataportabilitet, som der ellers er i forordningens artikel 18 og 20.

4.2.5 Følsomme personoplysninger

På samme måde som i forordningen er følsomme personoplysninger underlagt yderligere garantier i APPI, som angiver, at erhvervsdrivende ikke kan erhverve sådanne oplysninger uden den registreredes samtykke, hvortil der kun findes ganske få undtagelser, jf. betragtning 69.

Følsomme personoplysninger defineres i APPI som oplysninger, der vedrører race, tro, social status, sygdomshistorie, straffeattest, skader lidt i forbindelse med en forbrydelse eller andre beskrivelser mv., som i henhold til en kabinetsbekendtgørelse er beskrivelser, der kræver særlig håndtering, jf. betragtning 66. Selvom definitionen ikke ordret er den samme som forordningens artikel 9, er de

indholdsmæssigt stort set ens. Det skyldes, at eksempelvis APPI's "sygdomshistorie" svarer til forordningens "sundhedsoplysninger", at "race" dækker "etnisk oprindelse", og at "tro" dækker både religiøse og politiske overbevisninger, jf. betragtning 66. Ydermere angiver Kommissionen at have tilsikret sig, at den særlige beskyttelse, som følsomme personoplysninger i forordningen er underlagt, er udvidet til alle de i forordningen nævnte kategorier af følsomme personoplysninger. Med henblik herpå er det som nævnt i de supplerende regler til APPI fastsat, at de databehandlende erhvervsdrivende skal behandle oplysninger fra EU vedrørende en fysisk persons seksuelle orientering og fagforeningsmæssigt tilhørsforhold på samme måde som de øvrige følsomme personoplysninger omfattet af APPI, jf. betragtning 68. Udvidelsen af definitionen af følsomme personoplysninger i de supplerende regler og Kommissionens sikring heraf viser, at der er visse elementer ved tredjelandets databeskyttelseslovgivning, som EU ikke kan gå på kompromis med uden at risikere at kompromittere det høje niveau af databeskyttelse, som forordningen har etableret.

4.2.6 Videreoverførsel

Kommissionen angiver overordnet, at beskyttelsesniveauet for personoplysninger overført fra EU til Japan ikke må undermineres ved en videreoverførsel fra Japan til et andet tredjeland. Videreoverførsler bør alene tillades, hvis den efterfølgende modtager i tredjelandet "selv er underlagt regler, der sikrer et beskyttelsesniveau svarende til det, der garanteres i den japanske retsorden", jf. betragtning 75.

APPI indeholder detaljerede regler om muligheden for videreoverførsel, der som udgangspunkt kun kan ske ved den pågældende persons samtykke, der ifølge en af de supplerende regler skal være velinformeret, jf. betragtning 76. Der gælder en række undtagelser hertil efter APPI, jf. betragtning 77, som imidlertid ikke finder anvendelse på personoplysninger overført fra EU. Her kommer det toleddede databeskyttelsessystem beskrevet ovenfor i afsnit 4.2.2 til udtryk. I en af de supplerende regler angives nemlig, at der gælder to undtagelser til reglen om samtykkebaserede videreoverførsler, som kun finder anvendelse på personoplysninger overført fra EU. Den pågældende supplerende regel har til formål at øge beskyttelsen af netop disse oplysninger. Den første undtagelse finder anvendelse, når personoplysningerne sendes til et tredjeland, som PPC har anerkendt som at have et beskyttelsesniveau svarende til det japanske. Den anden undtagelse gælder, når den erhvervsdrivende og modtagende tredjemand "sammen har gennemført foranstaltninger, der sikrer et beskyttelsesniveau svarende til APPI, sammenholdt med de supplerende regler, ved hjælp af en kontrakt, andre former for bindende aftaler eller bindende foranstaltninger inden for en koncern", jf. betragtning 78.

Medmindre en af de to undtagelser finder anvendelse, er samtykke altså det primære overførselsgrundlag i Japan. I den forbindelse bemærkes, at samtykke også udgør et overførselsgrundlag efter forordningen, som dog alene er anvendelig i undtagelsesvise tilfælde, jf. artikel 49, stk. 1, litra a. Det er påfaldende, at et overførselsgrundlag, der i EU alene anvendes undtagelsesvist, udgør det generelle overførselsgrundlag i Japan og derfor også grundlaget for videreoverførsel af EU-borgernes personoplysninger.[86] At samtykkebaserede internationale dataoverførsler har undtagelsens karakter efter forordningen er dog ikke ensbetydende med, at samtykke i sig selv er et "dårligt" eller "mindre sikkert" overførselsgrundlag. Tværtimod kan der argumenteres for, at de registrerede gives bedre kontrol over deres personoplysninger ved et sådant krav om samtykke end ved eksempelvis en generel tilstrækkelighedsafgørelse vedrørende et helt land, som de registrerede som enkeltpersoner ikke har nogen indflydelse på. Kommissionen er tydeligvis kommet til en lignende konklusion, da Japans

[86] Graham Greenleaf, Japan: EU Adequacy Discounted, s. 8.

samtykkebaserede ordning for videreoverførsler (som altså fra japanske erhvervsdrivendes perspektiv udgør internationale dataoverførsler) tilfredsstiller kravene i artikel 45.

4.2.7 Offentlige myndigheders adgang til og brug af personoplysninger

Kommissionen har modtaget en række officielle redegørelser, forsikringer og tilsagn fra Japan "undertegnet på højeste ministerielle og forvaltningsmæssige niveau" vedrørende de japanske myndigheders adgang til og brug af personoplysninger overført fra EU til erhvervsdrivende i Japan på grundlag af tilstrækkelighedsafgørelsen, som findes i afgørelsens bilag II, jf. betragtning 113. Japan har således ved brugen af forsikringer mv. afklaret visse elementer ved lovgivningen, som ellers muligvis kunne have talt imod godkendelse af landets beskyttelsesniveau. Det samme gjorde nogle af de tredjelande, hvis beskyttelsesniveau blev godkendt i medfør af direktivet, jf. nærmere ovenfor afsnit 3.7.

Kommissionen angiver i betragtning 114 overordnet, at offentlige myndigheder skal agere i overensstemmelse med legalitetsprincippet, hvilket indebærer, at adgang til og brug af personoplysninger skal ske i overensstemmelse med loven. I den forbindelse bemærkes, at den japanske forfatning indeholder bestemmelser, der begrænser og sætter rammerne for myndighedernes indsamling af oplysninger. I APPI angives endvidere, at alle personoplysninger skal håndteres i overensstemmelse med princippet om respekt for den enkeltes personlighed. Den nærmere regulering findes i APPIHAO, jf. betragtning 118, som beskriver, hvorledes og i hvilket omfang personoplysninger kan bruges med henblik på retshåndhævelse på det strafferetlige område og af hensyn til national sikkerhed. Der kræves hjemmel til en sådan behandling, der enten kan ske på grundlag af en retskendelse eller en anmodning om frivillig udlevering, jf. betragtning 119 og 120. De nærmere regler herom fremgår af betragtning 119-129, som blandt andet angiver, at højesteretspraksis stiller krav om foretagelse af en proportionalitetstest ved anmodninger om frivillige udleveringer, som skal iagttages af både myndigheden og den databehandlende erhvervsdrivende, jf. betragtning 128 og 129. Som konsekvens af denne proportionalitetstest nægtede den mest populære beskedapplikation i Japan, LINE, i 2017 at imødekomme en anmodning fra efterforskningsmyndighederne om frivillig udlevering, idet begrundelsen for anmodningen var utilstrækkelig, og omfanget af anmodningen var for bred i forhold til efterforskningens formål, jf. afgørelsens fodnote 99.

De japanske regler om myndighedernes adgang til og brug af personoplysninger overført fra EU til Japan svarer ifølge Databeskyttelsesrådet til de vigtigste grundlæggende garantier i EU-lovgivningen og den europæiske menneskerettighedskonvention.[87] På den baggrund og på grundlag af de for Kommissionen tilgængelige oplysninger om den japanske retsorden anses myndighedernes adgang til og brug af personoplysninger som begrænset til det strengt nødvendige for at forfølge tilsigtede legitime mål, og der anses at være effektiv retsbeskyttelse mod sådanne indgreb, jf. betragtning 173.

Når en betydelig del af afgørelsen (betragtning 113-170) dedikeres til spørgsmålet om myndighedernes adgang til og brug af personoplysninger overført fra EU, udtrykker Kommissionen, at et tilstrækkeligt beskyttelsesniveau nødvendigvis skal indeholde et værn mod tredjelandets myndigheder og disses uretmæssige behandling af personoplysninger overført fra EU. Det er en klar konsekvens af EU's betoning af menneskerettighedsaspektet ved databeskyttelse og udspringer af EU's negative erfaringer med myndigheders misbrug af personoplysninger, jf. nærmere afsnit 4.8. Betydningen af dette moment fremgår i øvrigt også af Schrems II-dommen, som netop opstod som følge af tredjelandets – USA's – myndigheders adgang til og brug af personoplysninger fra EU, jf. nærmere nedenfor afsnit 5.

[87] Databeskyttelsesrådet, Udtalelse 28/2018, betragtning 152.

4.3 Momenter, der falder under litra b

Også momenter angivet i artikel 45, stk. 2, litra b, inddrages i vurderingen.

4.3.1 Tilsyn og håndhævelse

Med henblik på at sikre, at det af lovgivningen etablerede beskyttelsesniveau rent faktisk eksisterer i praksis, angiver Kommissionen, at der bør være oprettet en uafhængig tilsynsmyndighed i Japan med beføjelse til at overvåge og sikre, at reglerne overholdes, jf. betragtning 95. Dette er ikke i sig selv overraskende, både fordi tilsynsmyndigheder indtager en central position i EU-databeskyttelsesret, og eftersom krav om tilsyn med undersøgelses- og interventionsbeføjelser allerede er blevet angivet i tidligere tilstrækkelighedsafgørelser.

I Japan er PPC den uafhængige myndighed med ansvar for tilsynet og håndhævelsen af APPI, jf. betragtning 11. Tilsynets uafhængighed er sikret i APPI med en række regler, som fastslår, at kommissionærerne i tilsynet kun kan afskediges med gyldig grund og kun i et begrænset antal tilfælde, de må ikke aktivt engagere sig politisk, skal afholde sig fra anden lønnet beskæftigelse og er underlagt interne regler til forhindring af deltagelse i opgaver i tilfælde af interessekonflikter, jf. betragtning 96. PPC har beføjelse til at anmode erhvervsdrivende om at rapportere eller fremsende dokumenter om deres behandlingsaktiviteter, kan foretage inspektioner, afgive vejledning og rådgivning, vedtage retningslinjer og – i anledning af en klage eller på eget initiativ – afgive henstillinger eller påbud for håndhævelsen af APPI eller andre bindende regler, herunder de supplerende regler, jf. betragtning 97-98. I de supplerende regler angives, at såfremt en erhvervsdrivende behandler personoplysninger overført fra EU, vil PPC altid vil betragte den erhvervsdrivendes undladelse af at handle i overensstemmelse med en henstilling fremsat i medfør af APPI som en "alvorlig overtrædelse, der indebærer en overhængende fare for den enkeltes rettigheder og interesser", og som derfor kræver udstedelse af et bindende pålæg, medmindre der foreligger legitime grunde til undladelsen, jf. betragtning 101. Gennem denne supplerende regel har EU således tilsikret sig et yderligere værn for beskyttelsen EU-borgernes personoplysninger.

4.3.2 Retningslinjer

Om PPC's beføjelse til at vedtage retningslinjer knyttes nogle yderligere bemærkninger. Ifølge betragtning 16 kan retningslinjer vedtages "for at sikre en korrekt og effektiv gennemførelse af de foranstaltninger, som en erhvervsdrivende skal træffe i henhold til databeskyttelsesreglerne". Retningslinjerne udgør en autoritativ fortolkning af APPI og er samtidigt bindende for de erhvervsdrivende, jf. betragtning 16, hvilket viste sig at være en kontroversiel retlig konstruktion i EU's øjne.

Når Databeskyttelsesrådet i sin udtalelse angiver, at retningslinjerne ifølge deres vurdering ikke er juridisk bindende, hvis de udgør en "autoritativ fortolkning" af APPI,[88] er det udtryk for, at retningslinjer i EU traditionelt forstås som ikke-bindende vejledninger, hvis efterlevelse ikke nødvendigvis forventes og ikke kan håndhæves af myndighederne. Retningslinjer har dog en helt særlig status i Japan. Her efterleves retningslinjerne fastsat af PPC frivilligt af de erhvervsdrivende, selvom de teknisk set ikke udgør en del af APPI.[89] Det skyldes landets særlige kultur, hvorefter de erhvervsdrivende i stort omfang efterlever selv "fortolkende" retningslinjer af frygt for at overtræde de sociale normer. Erfaringer og interviews har nemlig vist, at risikoen for at miste offentlighedens tillid som følge af et databrud eller en regelovertrædelse – selv hvis reglen blot findes i retningslinjerne og ikke i den

[88] Databeskyttelsesrådet, Udtalelse 28/2018, betragtning 52.
[89] Flora Y. Wang, Cooperative Data Privacy, s. 676.

egentlige lov – er af enorm betydning for virksomhederne, og det er på den baggrund, at retningslinjerne har vist sig at være effektive og bindende, selvom de ikke udgør en del af APPI.[90] Denne forklaring af retningslinjernes status og funktion synes at være accepteret af Kommissionen, som beskriver dem som at være en integreret del af den retlige ramme og er derfor bindende, jf. betragtning 16. Databeskyttelsesrådet anerkender i øvrigt også i sin udtalelse, at retningslinjerne i praksis som regel efterleves. Ikke desto mindre anmodes PPC om at udlevere yderligere information, som dokumenterer dette og som beviser, at japanske domstole behandler retningslinjerne som en del af APPI ved deres afgørelser, således som PPC har anført.[91] Retningslinjerne vil formodentlig blive et af emnerne ved den snarlige revision, eftersom ikke alle Databeskyttelsesrådets betænkeligheder blev adresseret ved tilstrækkelighedsafgørelsen.[92]

Kontroversen om retningslinjerne viser, at Kommissionen ikke kan få et retvisende billede af Japans beskyttelsesniveau, hvis landets særlige sociale normer og retslige kultur ignoreres, idet det er i kontekst af disse, at retningslinjernes effektivitet kan forstås. Kontroversen om retningslinjerne bekræfter også det i afsnit 2.2.1 og 2.2.2 nævnte om, at alternative udformninger af eksempelvis datatilsyn og lovgivning kan accepteres, så længe der eksisterer databeskyttelsesregler og der sikres en effektiv håndhævelse af reglerne. Midlerne for databeskyttelsen er således underordnede, så længe de formår at sikre det tilstrækkelige beskyttelsesniveau.

4.3.3 Administrativ og retslig prøvelse

Japansk lovgivning giver den registrerede adgang til administrativ og retslig prøvelse samt adgang til skadeserstatning, jf. betragtning 103-112, hvilket også er tilfældet efter forordningen, jf. dennes artikel 77, 78 og 82. Udover at kunne indgive klage til PPC og anlægge sag ved domstolene, har den registrerede også mulighed for at klage direkte til den databehandlende erhvervsdrivende. I et sådant tilfælde har PPC en pligt til at sørge for mægling mellem den erhvervsdrivende og den registrerede, herunder ikke-japanske registrerede, jf. betragtning 104. En registreret har desuden mulighed for at indgive en anmeldelse til anklagemyndigheden eller politiet vedrørende overtrædelser af APPI, som kan føre til strafferetlige sanktioner, jf. betragtning 108.

4.3.4 Sanktioner

Mens EU efterhånden er blevet berygtet for sine store bøder med et maksimum på 10/20 mio. euro eller 2/4% af en virksomheds globale årlige omsætning afhængigt af, hvilken bestemmelse der er overtrådt, jf. artikel 83, fastsættes i APPI et bødeniveau på op til 100.000 eller 500.000 yen (cirka 775 og 3870 euro) afhængigt af, hvilken bestemmelse der er overtrådt. Til gengæld fastsætter APPI mulighed for straf i form af fængsel med arbejde i op til seks måneder eller op til et år afhængigt af den overtrådte bestemmelse, jf. betragtning 108. Der kan her stilles spørgsmålstegn ved, om det i forhold til EU lave bødeniveau rent faktisk er med til at skabe et niveau af databeskyttelse, der i det væsentlige svarer til EU's. Af selve afgørelsen kan dog ikke læses anden konklusion end, at selv et sådant lavt bødeniveau er acceptabelt og lever op til de i artikel 45 udtrykte krav.

4.3.5 Underretning ved sikkerhedsbrud

Til forskel fra forordningens artikel 33 er de databehandlende erhvervsdrivende i Japan ikke pålagt en underretningspligt overfor tilsynsmyndigheden i tilfælde af et brud på datasikkerheden. Der eksisterer i stedet en frivillig ordning, hvorefter tilmeldte selskaber kan forpligte sig til at underrette PPC

[90] Ibid., s. 676.

[91] Databeskyttelsesrådet, Udtalelse 28/2018, betragtning 49 og 54.

[92] Flora Y. Wang, Cooperative Data Privacy, s. 678.

og datasubjekterne (eller offentligheden) om sikkerhedsbrud. Trods den frivillige karakter havde 44 brancheorganisationer i 2017 tilmeldt sig ordningen, hvor den største organisation repræsenterer over 15.400 erhvervsdrivende, jf. betragtning 73. Det illustrerer igen en kulturel og juridisk forskel mellem de to parter, idet der i Japan lægges betydelig vægt på og er tillid til de enkelte erhvervsdrivendes egen frivillige efterlevelse af selv ikke-bindende regler, mens EU foretrækker bindende regler, hvis efterlevelse kan håndhæves ved sanktioner. Hidtil har Japans tilgang vist sig ganske effektiv. Alene i 2018 modtog PPC 1.216 underretninger om sikkerhedsbrud, hvoraf 81.9% af tilfældene var af mindre alvorlig karakter, eksempelvis om afsendelse af dokumenter eller en mail til en forkert modtager.[93]

4.4 Momenter, der falder under litra c

Momenter, der falder under artikel 45, stk. 2, litra c, indgår i begrænset omfang i Kommissionens vurdering.

4.4.1 Internationale forpligtelser

Databeskyttelsesrådet bemærker i sin udtalelse, at Japan har fået tildelt observatørstatus for det rådgivende udvalg om konvention 108+ (moderniseringen af konvention 108).[94] I selve afgørelsen nævnes dog intet om internationale forpligtelser, og Kommissionen har således prioriteret en grundig analyse af landets databeskyttelseslovgivning fremfor at se på landets eventuelle internationale forpligtelser.

4.5 Databeskyttelsesrådets udtalelse

Udtalelse 28/2018 om Japan er allerede blevet inddraget løbende gennem denne analyse af tilstrækkelighedsafgørelsen, men der vil her gøres nogle enkelte yderligere bemærkninger om udtalelsens indhold.

Databeskyttelsesrådet anerkender Japans bestræbelser på at møde EU's databeskyttelseskrav, men identificerer dog adskillige problemområder og behov for præciseringer. Det er blandt andet problematisk, at samtykke i Japan defineres anderledes end i EU herunder særligt, at begrebet i Japan ikke omfatter en fortrydelsesret, hvilket i EU er en vigtig faktor for at sikre den registreredes kontrol over sine personoplysninger.[95] Det er også problematisk, at det japanske klagesystem kan være svært tilgængeligt for personer i EU, idet kontakt hertil sker telefonisk og kun på japansk,[96] og at APPI ikke skelner mellem dataansvarlige og databehandlere, idet loven blot omfatter erhvervsdrivende, som behandler personoplysninger.[97] Ikke alle betænkeligheder er blevet løst på tidspunktet for afgørelsens vedtagelse. Eksempelvis skelnes der fortsat ikke i APPI mellem dataansvarlige og databehandlere, jf. betragtning 35, og en besvarelse af spørgsmålet om et tilbagetrukket samtykke udskydes indtil revisionen, jf. betragtning 181. Andre opfordringer og anbefalinger fra Databeskyttelsesrådet blev dog fulgt, herunder blandt andet opfordringen til vedtagelse af yderligere regler med henblik på at skabe et nemmere klagesystem, jf. betragtning 104. Det er således ikke ethvert problem der forhindrer, at landet anses for at have et tilstrækkeligt beskyttelsesniveau.

[93] Hiroshi Miyashita, EU-Japan Mutual Adequacy Decision, s. 10.
[94] Databeskyttelsesrådet, Udtalelse 28/2018, betragtning 58.
[95] Ibid., betragtning 18.
[96] Ibid., betragtning 19.
[97] Ibid., betragtning 68.

4.6 Revision

Artikel 45, stk. 3, forpligter Kommissionen til at foretage revision af tilstrækkelighedsafgørelser mindst hvert fjerde år. Der er alene tale om en generel tidsramme, som skal tilpasses det enkelte tredjeland afhængigt af landets særlige omstændigheder, som kan tale for et hyppigere revisionsinterval.[98] Japans omstændigheder talte tydeligvis for en forkortelse af revisionsintervallet, idet Databeskyttelsesrådet opfordrede til,[99] og Kommissionen fastsatte, at den første revision skal foretages allerede efter to år, jf. betragtning 181. Årsagen til forkortelsen af revisionsintervallet er, "at det beskyttelsesniveau, som den japanske retsorden sikrer, kan ændre sig", jf. betragtning 180. Mere specifikt skyldes det Databeskyttelsesrådets angivelse af, at det er mere hensigtsmæssigt at foretage den første revision forholdsvist hurtigt og derefter tilpasse revisionsintervallerne til at være længere, hvis det stemmer overens med resultatet i den første revision.[100] Det er her taget i betragtning, at APPI først trådte i kraft i 2017, at PPC blev etableret i 2016, og at der ikke er oplysninger eller beviser for den praktiske anvendelse af de supplerende regler endnu.[101] De supplerende regler blev trods alt vedtaget med henblik på at mindske kløften mellem Japans og EU's lovgivning, og det er tvivlsomt, om en tilstrækkelighedsafgørelse kunne vedtages uden dem. Det er derfor naturligt, at de supplerende regler kommer til at indtage en central position i den kommende revision.

Om revisionen angiver Kommissionen overordnet i betragtning 181, at den "bør omfatte alle aspekter af denne afgørelses funktionsmåde, navnlig anvendelsen af de supplerende regler (med særlig opmærksomhed på den beskyttelse, der gives i tilfælde af videreoverførsler), anvendelsen af reglerne om samtykke, herunder ved tilbagetrukket samtykke, udøvelsen af individuelle rettigheder samt begrænsningerne og garantierne med hensyn til myndighedsadgang (…) Den bør også omfatte effektiviteten af tilsynet og håndhævelsen, både med hensyn til de regler, som finder anvendelse på [erhvervsdrivende, som behandler personoplysninger] og de regler, som finder anvendelse inden for retshåndhævelsen på det strafferetlige område og med hensyn til national sikkerhed." Selvom PPC's retningslinjer ikke specifikt er nævnt, falder de under "håndhævelse" og vil som nævnt i afsnit 4.3.2 højst sandsynligt blive behandlet i revisionen.[102]

Idet Japan har store økonomiske interesser ved at opretholde sin status som sikkert tredjeland, kan det ikke udelukkes, at landet ved revisionen kommer til at vedtage yderligere regler eller korrigere sin nuværende databeskyttelsesret, således at den nærmer sig forordningen i højere grad. En sådan overtagelse af EU's databeskyttelsesregler med henblik på at forblive et sikkert tredjeland i EU's øjne aktualiserer spørgsmålet om den såkaldte Bruxelles-effekt, jf. nærmere nedenfor i afsnit 6. Indtil videre skal det blot bemærkes, at tilstrækkelighedsafgørelser, hvorved et tredjeland godkendes som sikkert for blot et par år senere at blive pålagt yderligere krav kan sætte en uheldig præcedens, hvor tredjelandets egen retslige kultur bliver overtrumfet og erstattet af EU's regler, som måske ikke er lige så velegnede for tredjelandets lokale kultur, men er nødvendige for at forblive et sikkert tredjeland. Det er vanskeligt at konkludere, hvor indgribende revisionen bliver, da den endnu ikke er blevet foretaget. Men fastsættelsen af revisionsintervallet på to år understreger for Japan, at en tilstrækkelighedsafgørelse ikke nødvendigvis betyder, at man er på den sikre side. At være et sikkert tredjeland er tilsyneladende en løbende proces, hvor tredjelandene ikke blot skal vise, at de stadig har det samme beskyttelsesniveau som på afgørelsestidspunktet, men også efter omstændighederne møde andre og flere krav.

[98] Databeskyttelsesrådet, Udtalelse 28/2018, betragtning 55.
[99] Ibid., betragtning 56.
[100] Ibid., betragtning 55.
[101] Ibid., betragtning 55-56.
[102] Flora Y. Wang, Cooperative Data Privacy, s. 678.

4.7 Økonomiske interesser

Selvom databeskyttelsessystemerne i EU og Japan deler visse fællestræk, adskiller deres motivation for databeskyttelse sig fra hinanden. Formålet i EU er hovedsageligt beskyttelsen af retten til privatliv og til databeskyttelse.[103] Mens et økonomisk formål anerkendes som ganske vigtigt, er det dog ikke den primære hensigt.[104] Til sammenligning fremhæves i Japan først og fremmest den økonomiske værdi af data.[105] Eksempelvis udtalte daværende premierminister Shinzo Abe i sin tale ved World Economic Forum, at "The engine for growth, if you think about it, is fueled no longer by gasoline, but more and more by digital data".[106] Det økonomiske incitament bag Japans interesse i en tilstrækkelighedsafgørelse ses også ved, at afgørelsen alene dækker japanske erhvervsdrivende i stedet for at omfatte hele landet generelt, som har været tilfældet for alle de hidtidige tilstrækkelighedsafgørelser truffet i medfør af direktivet med undtagelse af Canada.

Ved overvejelsen af, hvor væsentlig økonomiske interesser har været for vedtagelsen af tilstrækkelighedsafgørelsen kan derfor ikke ignoreres den mulige sammenhæng mellem afgørelsen og frihandelsaftalen med Japan.[107] Tilstrækkelighedsafgørelsen trådte i kraft i den 23. januar 2019. Blot en uges tid senere, den 1. februar, trådte frihandelsaftalen mellem EU og Japan i kraft. Umiddelbart ville det ikke være overraskende, hvis aftalerne var beslægtede. I et memo specifikt vedrørende frihandelsaftalen med Japan angav Kommissionen imidlertid, at "Data protection is a fundamental right in the European Union and is therefore not up for negotiation. Privacy is not a commodity to be traded."[108] Der er da også tale om to helt forskellige aftaler, og det kan derfor ikke stipuleres, at den ene med sikkerhed ikke ville være blevet vedtaget uden den anden, men det er klart, at tilstrækkelighedsafgørelsen er motiveret af både Japans og EU's økonomiske interesser. Det er i forordningen anerkendt, at internationale dataoverførsler er nødvendige for den internationale samhandel,[109] og det er kun naturligt, at EU søger at eliminere handelshindringer. I en pressemeddelelse vedrørende tilstrækkelighedsafgørelsen udtalte EU-kommissær Věra Jourová også, at "Data is the fuel of global economy and this agreement will allow for data to travel safely between us to the benefit of both our citizens and our economies."[110] Denne naturlige og forventelige sammenhæng mellem fjernelsen af handelshindringer ved vedtagelsen af både frihandelsaftaler og tilstrækkelighedsafgørelser kan i øvrigt forventes bekræftet indenfor de næste par år. EU og Sydkorea indgik nemlig en frihandelsaftale i 2015,[111] og Sydkorea er højst sandsynligt det næste land, der bliver genstand for en tilstrækkelighedsafgørelse, idet landets forhandlinger med EU blev afsluttet den 30. marts 2021.[112] Nu afventes blot Kommissionens afgørelse.

---

[103] Databeskyttelsesforordningen, præambelbetragtning 4.

[104] Ibid., præambelbetragtning 6 og 7.

[105] Flora Y. Wang, Cooperative Data Privacy, s. 670.

[106] Shinzo Abe, Keynote Speech.

[107] Aftale mellem Den Europæiske Union og Japan om et økonomisk partnerskab, L 330/3.

[108] Kommissionen, Memo on Key Elements of the EU-Japan Economic Partnership Agreement.

[109] Databeskyttelsesforordningen, præambelbetragtning 101.

[110] Kommissionen, pressemeddelelse, The European Union and Japan agreed to create the world's largest area of safe data flows.

[111] Frihandelsaftale mellem Den Europæiske Union og dens medlemsstater på den ene side og Republikken Korea på den anden side, OJ 127.

[112] Fælles udtalelse fra Europa-Kommissionen og den sydkoreanske kommissionsformand.

4.8 Kulturelle forskelle

Kontroversen vedrørende retningslinjerne er blot ét eksempel på, at tredjelandes databeskyttelsesregler kan ikke løsrives fra deres kulturelle og sociale kontekst, som Kommissionen derfor er nødsaget til at tage i betragtning ved sin vurdering. Afgørelsen for Japan er heller ikke den første, hvor dette erkendes. Alle afgørelserne truffet i medfør af direktivet nævnte, at tilstrækkelighedsvurderingen skulle foretages ud fra kriterier, der sikrede, at tredjelandene ikke blev diskrimineret som følge af deres eventuelle forskellige opfattelser af databeskyttelse, jf. nærmere afsnit 3.2.

I tilfældet med retningslinjerne havde uenigheden mellem EU og Japan sine rødder i parternes forskellige forståelser af håndhævelse. EU håndhæver i betydeligt omfang sine regler ved en hard power-tilgang præget af et stærkt reguleringsorgan og sanktioner. Men som ovenstående gennemgang af den frivillige underretningsordning og retningslinjernes særlige status viser, har Japan en helt grundlæggende præference for soft power-redskaber til håndhævelse af regler, hvilket hviler på landets kulturelle betoning af virksomheders omdømme. I Japan følger virksomheder generelt myndighedernes retningslinjer af frygt for at miste samfundets tillid og skade virksomhedens omdømme som følge af en regelovertrædelse, hvilket betragtes som mere betydeligt end betalingen af en bøde. Sker der så endelig en overtrædelse af databeskyttelsesregler, ses endnu et særpræg ved japansk forretningskultur, idet virksomhederne typisk udgiver offentlige undskyldninger, som bliver tillagt betydelig symbolsk værdi. Som konsekvens af disse særlige normer og kulturelle skikke er PPC heller ikke nødsaget til at udstede mange bøder for at sikre overholdelsen af APPI eller andre regler.[113]

Illustrerende for den grundlæggelse forskel på håndhævelse i EU og Japan er Cambridge Analytica-skandalen fra 2018, som omhandlede et konsulentselskab af samme navn, der blev afsløret i ulovligt at have indsamlet personoplysninger fra Facebook-brugere, herunder omkring 100.000 japanere. PPC tildelte Facebook en advarsel og pålagde dem at forbedre deres databeskyttelse samt at kommunikere med de registrerede og slette disses data om nødvendigt. Disse instruktioner var ikke-bindende administrative ordrer, hvilket normalt også er tilstrækkeligt for at få virksomheder til at rette ind, såfremt de kulturelle normer i landet følges. Det ville ideelt set have foranlediget Facebook til at udgive en offentlig undskyldning og erkende deres fejl, men det skete ikke.[114] Af EU, derimod, blev Facebook pålagt en bøde på 500.000 pund.[115] Begge parters tilgang er betinget af deres kulturelle og historiske omstændigheder. EU's strengere tilgang menes at kunne spores tilbage til den massive overvågning og misbrug af personoplysninger under anden verdenskrig og det heraf affødte ønske om at undgå en lignende tilstand igen.[116] Ligeledes er den japanske tilgang formet af landets særlige omstændigheder, kultur og skikke og har længe vist sig at være effektiv, om end advarslen tildelt Facebook dog illustrerer vanskelighederne ved at pådutte disse kulturelle forventninger på udenlandske selskaber. Da det således ikke er muligt at erklære den ene eller den anden tilgang for mest korrekt, er det nødvendigt, at vurderingen af tredjelandets lovgivning, håndhævelse, tilsyn mv. skal ske med respekt for landets særlige omstændigheder og under hensyntagen til deres kontekst.

4.9 Delkonklusion

Kommissionens vurdering af Japans beskyttelsesniveau har i stort omfang været baseret på de i artikel 45, stk. 2, litra a-c, angivne momenter med særligt fokus på lovgivningen, myndigheders adgang til og brug af personoplysninger samt håndhævelsen af reglerne. Vurderingen har desuden taget højde

[113] Flora Y. Wang, Cooperative Data Privacy, s. 680.
[114] Flora Y. Wang, Cooperative Data Privacy, s. 682.
[115] Pressemeddelelse fra det britiske datatilsyn.
[116] Anu Bradford, The Brussels Effect, s. 136.

for Japans retslige kultur og særegenheder for på den måde at få et fyldestgørende billede af beskyttelsesniveauet. På den baggrund har afgørelsen i langt højere grad end de tidligere afgørelser bidraget til en nærmere fastlæggelse af indholdet af kravet "tilstrækkeligt beskyttelsesniveau". Afgørelsen er således et stort skridt henimod at give andre tredjelande den forudsigelighed og gennemsigtighed, som de fleste ønsker, før de begiver sig ud i forhandlinger med EU om opnåelsen af en tilstrækkelighedsafgørelse.

5. Schrems II

Af hensyn til USA's økonomiske og politiske betydning for EU er det væsentligt at kunne overføre personoplysninger til landet uden betydelige hindringer. Mens landet ikke har været genstand for en egentlig tilstrækkelighedsafgørelse efter artikel 45 på samme måde som de hidtil nævnte tredjelande, har Kommissionen og USA ad flere omgange indgået særlige aftaler, som henviser til direktivets artikel 25 (nu forordningens artikel 45) og som tillader frie overførsler fra EU til virksomheder i USA, hvis virksomhederne møder visse krav. Det skete først i form af Safe Harbour-aftalen,[117] som blev fundet ugyldig i Schrems I-dommen.[118] Parterne forsøgte herefter at tage Domstolens kritik i dommen i betragtning ved udarbejdelsen af den anden aftale, Privacy Shield-aftalen,[119] som dog i Schrems II-dommen[120] blev fundet ugyldig.

På den baggrund vil der nedenfor blive redegjort for Privacy Shield-aftalens indhold og Schrems II-dommens baggrund. Da Schrems II-dommen bidrager til fastlæggelsen af indholdet af artikel 45 og det heri indeholdte krav om et tilstrækkeligt beskyttelsesniveau, vil den dernæst blive analyseret. Dette efterfølges af en perspektivering til en nylig fransk dom, hvori præmisserne fra Schrems II-dommen blev anvendt.

5.1 Privacy Shield-aftalen

Privacy Shield-aftalens artikel 1 angiver, at "Med henblik på [artikel 45 i forordningen] sikrer USA et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra EU til foretagender i USA under [Den Europæiske Unions] og USA's værn om privatlivets fred." Værnet om privatlivets fred – på engelsk "privacy shield" – består mere specifikt af principper opstillet af det amerikanske handelsministerium, som fremgår af Privacy Shield-aftalens bilag II. Amerikanske virksomheder kan ved anmeldelse til ministeriet blive sat på en liste over deltagere i Privacy Shield-ordningen, som føres og offentliggøres i overensstemmelse med principperne i aftalen. Personoplysninger fra EU vil herefter frit kunne overføres til virksomheden, jf. Schrems II-dommens præmis 46. Af Privacy Shield-aftalens bilag II fremgår dog også, at virksomhedernes tilslutning til de i aftalen oplistede principper kan være begrænset "til et niveau, der er tilstrækkeligt til at opfylde kravene med hensyn til den nationale sikkerhed, den offentlige interesse eller retshåndhævelsen", jf. præmis 47. De under aftalen certificerede virksomheder, der modtager personoplysninger fra EU, er derfor forpligtede til at se bort fra principperne, hvis de er uforenelige med de nævnte hensyn og interesser. Hensynet til den nationale sikkerhed mv. har således forrang fremfor principperne, der ellers har til formål at værne om

[117] 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 (2000/520/EF)

[118] Sag C-362/14, Maximillian Schrems mod Data Protection Commissioner.

[119] 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.

[120] Sag C-311/18, Data Protection Commissioner mod Facebook Ireland Limited og Maximillian Schrems.

EU-borgernes privatliv og at sikre det tilstrækkelige beskyttelsesniveau, jf. præmis 164. Forfølgelsen af de nævnte hensyn og interesser sker mere specifikt ved de amerikanske myndigheders adgang til personoplysninger og brugen heraf som led i overvågning og efterretning, jf. præmis 165.

5.2 Klagen

Schrems II-dommen udsprang af østrigeren Maximillian Schrems' klage til den irske tilsynsmyndighed over overførslen af hans personoplysninger fra Facebook Ireland til Facebook Inc. i USA på grundlag af Privacy Shield-aftalen, jf. præmis 50 og 51. Han gjorde gældende, at USA ikke sikrede et tilstrækkeligt beskyttelsesniveau med Privacy Shield-aftalen, når amerikanske myndigheder kunne anmode om amerikanske virksomheders data, herunder de fra EU overførte, med henblik på forfølgelsen af de ovenfor beskrevne hensyn og interesser, jf. præmis 52. De pågældende myndigheder er National Security Agency (NSA) og Federal Bureau of Investigation (FBI), som er henholdsvis den nationale sikkerhedstjeneste og den føderale efterforskningsmyndighed. Disse myndigheder kan anmode om adgang til og brug af amerikanske virksomheders data med henblik på overvågning og efterretningsaktiviteter i henhold til artikel 702 i Foreign Intelligence Surveillance Act og Executive Order 12333, jf. præmis 52-55 og 60.

Irlands High Court fremlagde på den baggrund en række præjudicielle spørgsmål for Domstolen med henblik på at fastlægge, om Privacy Shield-aftalen var uforenelig med forordningens artikel 45 sammenholdt med charterets artikel 7, 8 og 47. Sådan uforenelighed ville indebære aftalens ugyldighed. Nedenstående analyse angår derfor for det første spørgsmålet om, hvorvidt rettighederne angivet i charterets artikel 7 og 8 blev respekteret ved Privacy Shield-aftalen. For det andet behandles spørgsmålet om, hvorvidt de effektive retsmidler, der kræves i medfør af charterets artikel 47, var tilgængelige for EU-borgerne i USA. Det bemærkes, at Domstolen besvarer spørgsmålene på grundlag af forordningen og ikke direktivet, selvom Privacy Shield-aftalen blev vedtaget før forordningens ikrafttrædelse, jf. præmis 79. Før gennemgangen af Domstolens besvarelse af de to spørgsmål knyttes nogle korte bemærkninger til de generelle krav indeholdt i forordningens artikel 45.

5.3 Generelt om kravet i forordningens artikel 45

Domstolen angiver, at artikel 45 stiller krav om, at tredjelandet i sin lovgivning eller sine internationale forpligtelser skal sørge for at sikre et beskyttelsesniveau for frihedsrettigheder og grundlæggende rettigheder, der i det væsentlige svarer til det niveau, der er sikret i EU med forordningen og charteret, jf. præmis 94 og 162. Således bekræftes det i afsnit 1.3.2 angivne om, at forordningen til enhver tid skal fortolkes i lyset af charteret.

5.4 Charterets artikel 7 og 8 samt begrænsningen af disse i artikel 52

Det første spørgsmål er som nævnt, hvorvidt Privacy Shield-aftalen respekterer den ved charterets artikel 7 angivne ret til privatliv og den ved artikel 8 angivne ret til beskyttelse af personoplysninger, jf. præmis 169.

Ved de amerikanske myndigheders beskrevne adgang til personoplysninger, herunder de fra EU til USA overførte, med henblik på opbevaring eller brug af dem begrænses personens ret til respekt for privatlivet angivet i artikel 7 og retten til beskyttelse af personoplysninger angivet i artikel 8, jf. præmis 170. Domstolen bemærker, at der foreligger en sådan begrænsning af rettighederne, uanset hvad oplysningerne bruges til efterfølgende, uanset om oplysningerne er følsomme, og uanset om indgrebet medfører eventuelle ubehageligheder for de berørte, jf. præmis 171.

Rettighederne i charteret er imidlertid ikke absolutte, men skal ses i lyset af deres funktion i samfundet og afvejes i forhold til andre grundlæggende rettigheder i overensstemmelse med proportionalitetsprincippet, jf. præmis 172. Begrænsninger i udøvelsen af de grundlæggende rettigheder (herunder de i artikel 7 og 8 angivne) er således mulige, men skal ske under iagttagelse af charterets artikel 52. Domstolen vurderede derfor, om adgangen til og brugen af EU-borgernes personoplysninger, således som dette var tilladt i Privacy Shield-aftalen og amerikansk lovgivning, opfyldte kravene angivet i artikel 52. Bestemmelsen stiller krav om, at enhver sådan begrænsning og rækkevidden heraf skal være fastsat i lovgivningen, som tillader begrænsningen og skal være angivet klart og præcist. Bestemmelsens proportionalitetskrav indebærer, at undtagelser fra og begrænsninger i udøvelsen af rettighederne skal være strengt nødvendige i forhold til formålet, som skal være af almen interesse anerkendt af Unionen eller angå et behov for beskyttelse af andres rettigheder og friheder. Lovgivningen skal desuden opstille mindstekrav for berørte personer, således at disse har tilstrækkelige garantier for at kunne beskytte deres personoplysninger effektivt mod risikoen for misbrug, jf. præmis 174-176. De amerikanske myndigheders mulighed for anvendelse af overvågningsprogrammer er imidlertid ikke begrænset på nogen måde i retsgrundlaget, som heller ikke tildeler ikke-amerikanske borgere nogen garantier for deres rettigheder, jf. præmis 180. Der er adgang til masseindsamling, og omfanget af adgangen til oplysninger som er i transit til USA uden at være underlagt noget retsligt tilsyn er ikke tilstrækkeligt klart og præcist afgrænset, jf. præmis 183. Retsgrundlaget angiver i det hele taget ikke, at overvågningsprogrammerne er begrænset til det strengt nødvendige, jf. præmis 184. Begrænsningerne af rettighederne i charterets artikel 7 og 8 findes derfor ikke at leve op til kravene i charterets artikel 52, jf. præmis 185.

5.5 Charterets artikel 47

Det andet spørgsmål er som nævnt, hvorvidt EU-borgerne har adgang i USA til effektive retsmidler og upartisk domstolsprøvelse i tilfælde af krænkelse af deres rettigheder, således som dette er fastsat i charterets artikel 47, jf. præmis 186.

Selve eksistensen af effektiv domstolsbeskyttelse, som er uafhængig og upartisk og har til formål at sikre overholdelsen af EU-retten, er "uløseligt forbundet med eksistensen af en retsstat", jf. præmis 187. Fastsættes i lovgivningen ingen mulighed for at gøre brug af retsmidler med henblik på at få adgang til, berigtiget eller slettet personoplysninger om den pågældende, opfylder lovgivningen ikke det væsentligste indhold i charterets artikel 47, jf. præmis 187. Vigtigheden af adgangen til effektive retsmidler udtrykkes også i forordningens artikel 45, stk. 2, litra a, hvorefter Kommissionen i sin tilstrækkelighedsvurdering skal tage hensyn til "effektiv administrativ og retslig prøvelse for de registrerede, hvis personoplysninger overføres", hvilket har indtaget en central position i alle hidtidige tilstrækkelighedsafgørelser. Adgangen til effektiv prøvelse ved tredjelandets myndigheder og domstole bliver kun mere væsentlig, når medlemslandenes egne administrative og retslige myndigheder alene har begrænsede muligheder for at behandle klager i tredjelandet over ulovlig behandling af de fra EU overførte personoplysninger, jf. præmis 189.

EU-borgerne har imidlertid ingen effektive retsmidler for behandlingen af deres personoplysninger i USA, da retsgrundlaget for overvågnings- og efterretningsprogrammer – det vil sige artikel 702 i Foreign Intelligence Surveillance Act og Executive Order 12333 – ikke tildeler dem nogen rettigheder overfor de amerikanske myndigheder, der kan håndhæves ved domstolene, jf. præmis 192. I Privacy Shield-aftalen erkender Kommissionen endda selv, at der savnes retsmidler og domstolsbeskyttelse mod indgreb foretaget i forbindelse med efterretningsprogrammer, men vælger alligevel at indgå aftalen med USA, jf. præmis 191. Oprettelsen af ombudsmandsordningen – indført efter Domstolens kritik af Safe Harbour-aftalens mangel på effektive retsmidler i Schrems I-dommen – afhjælper ikke

disse mangler ved domstolsbeskyttelsen for de, hvis personoplysninger overføres til USA, jf. præmis 190. Det gælder uanset Kommissionens egen angivelse i Privacy Shield-aftalen om, at ordningen opfylder kravene i charterets artikel 47, jf. præmis 193. For selvom ombudsmanden er uafhængig af efterretningstjenesterne, udpeges han af udenrigsministeren, udgør en del af det amerikanske udenrigsministerium, og der er ingen garantier mod nedlæggelse af ombudsmandsfunktionen eller tilbagekaldelse af udpegningen af ham, hvilket kaster tvivl over hans uafhængighed fra den udøvende magt, jf. præmis 195. Der er desuden ingen regler i Privacy Shield-aftalen, som sikrer ombudsmandens beføjelse til at træffe bindende afgørelser overfor efterretningstjenesterne, jf. præmis 196. Amerikansk lovgivning tildeler derfor ikke EU-borgere de efter charterets artikel 47 sikrede effektive retsmidler og adgang til en upartisk domstol, jf. præmis 197.

På grundlag af besvarelsen af de to ovenstående spørgsmål fandt Domstolen, at Privacy Shield-aftalen var uforenelig med forordningens artikel 45 sammenholdt med charterets artikel 7, 8 og 47, jf. præmis 199. Således medfører et tredjelands manglende overholdelse af de nævnte bestemmelser i charteret, at tredjelandets beskyttelsesniveau ikke er tilstrækkeligt i medfør af forordningens artikel 45.

5.6 Status efter Schrems II-dommen

Den 12. marts 2021 anvendte den øverste forvaltningsdomstol i Frankrig, Conseil d'État, de i Schrems II-dommen udtrykte præmisser til at afgøre, om der i en bestemt sag forelå tilstrækkelige sikkerhedsforanstaltninger mod en risiko for udlevering af EU-borgerens personoplysninger til amerikanske myndigheder.[121] Baggrunden for sagen var en aftale mellem det franske sundhedsministerium og virksomheden Doctolib, hvorefter sidstnævnte fik til opgave at administrere booking af vaccinationer mod COVID-19. Doctolib gjorde brug af AWS Sarl som hostingleverandør, det vil sige til opbevaring af data. AWS Sarl er etableret i Luxembourg, men er datterselskab til amerikanske Amazon Web Services Inc. Flere fagforeninger krævede aftalen mellem ministeriet og Doctolib suspenderet, idet de anså anvendelsen af et datterselskab til en amerikansk virksomhed for at udgøre en risiko for de amerikanske myndigheders adgang til franske borgeres personoplysninger.[122]

Conseil d'État udtalte, at alene AWS Sarl's opbevaring (hosting) af personoplysninger ikke udgjorde en international dataoverførsel, idet de pågældende data blev opbevaret på servere i Tyskland og Frankrig. Imidlertid anerkendtes den af fagforeningerne udtrykte risiko for amerikanske myndigheders anmodninger om adgang til personoplysningerne med henblik på overvågning og efterretning under henvisning til artikel 702 i Foreign Intelligence Surveillance Act eller Executive Order 12333, hvilket også var tilfældet i Schrems II-dommen. I overensstemmelse med Schrems II-dommen afhang en mulig suspendering af aftalen mellem Doctolib og AWS Sarl af, om parterne havde etableret tilstrækkelige sikkerhedsforanstaltninger til beskyttelse af de opbevarede personoplysninger.[123] I denne forbindelse noterede Conseil d'État sig, at vurderingen af beskyttelsesniveauets tilstrækkelighed, som er etableret af den dataansvarlige og databehandleren, særligt inddrager de i artikel 45, stk. 2 nævnte momenter, således som dette er blevet udtrykt i Schrems II-dommen.[124] Både tekniske og juridiske sikkerhedsforanstaltninger fandtes at være etableret i aftalen mellem Doctolib og AWS Sarl. Det omfattede kryptering af de opbevarede data, hvis krypteringsnøgle blev betroet til en tredjepart i Frankrig. Ydermere fastsatte parterne i deres aftale en procedure, der skulle følges, hvis udenlandske myndigheder anmodede om adgang til data. På denne måde sikrede Doctolib sig, at AWS Sarl ville gøre

[121] Conseil d'État, pressemeddelelse.
[122] Bird & Bird, Fransk domstol anvender Schrems II præmisser.
[123] Conseil d'État, pressemeddelelse.
[124] Conseil d'État, CE – 450163, præmis 5, som angiver følgende: *A cet effet, l'évaluation du niveau de protection assuré doit, notamment, prendre en considération (…) [les éléments] énoncés à l'article 45, paragraphe 2, du règlement.*

modstand mod adgangsanmodninger fra amerikanske myndigheder. Endelig bemærkede Conseil d'État, at de opbevarede personoplysninger automatisk blev slettet senest efter tre måneder. Under henvisning til disse sikkerhedsforanstaltninger fandt Conseil d'État, at beskyttelsen af personoplysninger opbevaret af AWS Sarl var tilstrækkelig. Fagforeningernes anmodning om suspendering blev derfor afvist.[125] Således bidrager Doctolib-sagen til en fastlæggelse af, hvornår der foreligger de tilstrækkelige sikkerhedsforanstaltninger efter artikel 45, stk. 2, litra a-c, som Schrems II-dommen stillede krav om.

5.7 Delkonklusion

I Schrems II-dommen anerkender Domstolen vigtigheden af at styrke de økonomiske og handelsmæssige relationer til USA.[126] Forfølgelsen af disse naturlige og berettigede økonomiske interesser må dog ikke ske på bekostning af EU-borgernes rettigheder. Begrænser tredjelandet udøvelsen af rettighederne angivet i charteret uden tilstrækkelig begrundelse herfor og uden at tildele EU-borgerne effektive retsmidler, kan landet ikke anses for at have ydet tilstrækkelig beskyttelse af borgerne i medfør af forordningens artikel 45. Med henvisning til Schrems II-dommens præmisser viser Doctolib-sagen endvidere, at virksomheder i EU skal inddrage de i artikel 45, stk. 2, litra a-c angivne momenter ved sin etablering af sikkerhedsforanstaltninger, når der samarbejdes med virksomheder, der som følge af deres virksomhedsstruktur kan blive genstand for udenlandske myndigheders anmodninger om udlevering af EU-borgeres personoplysninger.

6. Bruxelles-effekten

Tilstrækkelighedsafgørelserne og Schrems II-dommen indskriver sig i en større tendens, hvor EU gennem en eksternalisering af sin lovgivning formår at sætte de globale standarder. Denne tendens kendes undertiden som Bruxelles-effekten. Nærmere bestemt dækker begrebet over det fænomen, hvor EU som følge af sin størrelse og markedsposition kan vedtage lovgivning for det indre marked, som tredjelande – uden at være forpligtede hertil – tilpasser sig med henblik på at nyde de økonomiske fordele, som sådan tilpasning udløser. Når ikke kun EU, men også tredjelande således handler efter de samme regler, bliver reglerne den globale standard.[127]

I 90'erne var Bruxelles-effekten mere eller mindre et utilsigtet biprodukt af EU's regulering af det indre marked.[128] Særligt siden 00'erne er EU dog blevet sin evne til at forme de globale lovgivningsmæssige standarder mere bevidst, og aspirationen om at sætte standarden for resten af verden er blevet mere udtalt.[129] Det gælder ikke mindst på databeskyttelsesområdet. Et års tid før vedtagelsen af databeskyttelsesforordningen udtalte EU-kommissær Věra Jourová således, at "we [EU] want to set the global standard".[130] Tidligere vicepræsident af Kommissionen Viviane Reding udtalte desuden, at "Europe must act decisively to establish a robust data protection framework that can be the gold standard for the world".[131] Databeskyttelse er således et af de klareste eksempler på EU's globale aspirationer og dermed Bruxelles-effekten. På den baggrund gøres nedenfor nogle generelle bemærkninger om tilstrækkelighedsafgørelsers forhold til Bruxelles-effekten, som efterfølges af en overvejelse af motivationen for tilpasning til EU's standarder samt en diskussion af de mod EU rettede

[125] Bird & Bird, Fransk domstol anvender Schrems II præmisser.
[126] Se eksempelvis Sag C-311/18, Schrems II, præmis 8.
[127] Anu Bradford, The Brussels Effect, s. 1-2.
[128] Ibid., s. 7 og 19.
[129] Ibid., s. 21.
[130] Ibid., s. 22.
[131] Viviane Reding, Speech: A data protection compact for Europe

anklager om retsimperialisme. Endelig perspektiveres til Japans opnåelse af tilstrækkelighedsafgørelsen.

6.1 Effekten på databeskyttelsesområdet

EU udøver sin globale indflydelse på databeskyttelsesområdet blandt andet gennem tilstrækkelighedsafgørelser, hvor tredjelandene specifikt anmoder om at blive anset for "tilstrækkelige" i EU's øjne. Selve præmissen for en tilstrækkelighedsafgørelse indeholder derfor et element af en eksternalisering af EU's standarder for databeskyttelse, da bedømmelsen af tredjelandet sker efter standarder, som tredjelandet ikke selv har haft nogen indflydelse på. Mens tredjelandets databeskyttelsesregler ikke forventes at være identiske med reglerne i forordningen, forventes de i det væsentlige at svare til de i EU,[132] hvilket altså forudsætter en tilpasning af tredjelandets regler til EU's.

Som nævnt har adskillige godkendte tredjelande vedtaget databeskyttelseslovgivning, der i vid udstrækning er inspireret af EU's. Da eksempelvis Argentina gav sig i kast med at opnå en tilstrækkelighedsafgørelse fra EU, valgte landet i 2000 at udforme sin databeskyttelseslovgivning efter den spanske databeskyttelseslov og opnåede efterfølgende godkendelse som sikkert tredjeland. Efter EU's vedtagelse af forordningen i 2016 nedsatte landet desuden en arbejdsgruppe for at undersøge, hvorledes landets lovgivning eventuelt skulle ændres for i fremtiden (efter ikrafttrædelsen af forordningen) at opretholde sin status som godkendt tredjeland.[133] Også afgørelsen vedrørende Japan kom først efter årelange forhandlinger, hvor landet gradvist tilpassede sig EU's krav. Databeskyttelsesloven i det næste land i rækken til at blive et godkendt tredjeland, Sydkorea, har ifølge landets indenrigsministerium 90% eller større lighed med lovgivningen i EU. Hovedproblemet, der har stået i vejen for en tilstrækkelighedsafgørelse, er manglen på en uafhængig tilsynsmyndighed i landet, hvilket Sydkorea har arbejdet på at ændre, så det stemmer overens med EU's krav.[134]

Indtil videre har omkring 120 tredjelande vedtaget databeskyttelseslovgivning, hvoraf de fleste i større eller mindre omfang har ladet sig inspirere af EU's databeskyttelseslovgivning, ofte med en aspiration om at blive det næste godkendte tredjeland.[135] Der kan herefter ikke være nogen tvivl om EU's succes med at sætte den globale standard for databeskyttelse, herunder ved hjælp af tilstrækkelighedsafgørelser.

6.2 Belønning ved tilpasning

I forhandlingerne for at få en tilstrækkelighedsafgørelse gjorde Japan adskillige indrømmelser for at leve op til EU's standarder. Opnåelsen af en tilstrækkelighedsafgørelse afhænger således i høj grad af tredjelandets villighed til at importere de af EU definerede databeskyttelsesregler og -principper. Det var netop også USA's uvillighed til at gøre større indrømmelser, der gav dødsstødet til Privacy Shield-aftalen. Havde USA accepteret at tilpasse sig flere af EU's krav, navnlig bestemmelserne i charteret, hvis overholdelse Domstolen trods alt allerede i Schrems I-dommen udtrykte betydningen af, var aftalen sandsynligvis gyldig og stadig i kraft i dag.[136]

Når tilstrækkelighedsafgørelser således afhænger af villigheden til at tilpasse sig EU, kan tredjelandet føle sig trængt op i en krog. Det skyldes, at tredjelande, som accepterer at indordne sig EU's databeskyttelsesstandarder, bliver belønnet med en godkendelse som sikkert tredjeland og adgang til EU's

[132] Sag C-311/18, Schrems II, præmis 94.
[133] Anu Bradford, The Brussels Effect, s. 150.
[134] Ibid., s. 151.
[135] Ibid., s. 148.
[136] Sag C-362/14, Schrems I, præmis 34.

marked, mens tredjelande, som ikke gør det, oplever hindringer for dataoverførsler og vanskeligere adgang til EU's marked.[137] Det er ikke svært at forestille sig, at sidstnævnte type tredjelande føler sig pressede til at efterkomme EU's krav for at få en tilstrækkelighedsafgørelse, selvom de ikke nødvendigvis ellers ville have gjort det. Det er trods alt ikke givet, at Japan eksempelvis ville have udvidet definitionen af "følsomme personoplysninger" til også at omfatte oplysninger om seksuel orientering og fagforeningsmæssigt tilhørsforhold, hvis landet ikke ønskede en tilstrækkelighedsafgørelse. Adgangen til EU's marked udgør således et væsentligt middel for at få tredjelande til at tilpasse sig EU's standarder og dermed aktivere Bruxelles-effekten.

6.3 EU som moderne imperialist

Ved eksternaliseringen af sine databeskyttelsesstandarder formår EU at forme tredjelandenes lovgivningsmæssige identitet.[138] Bruxelles-effekten er på den baggrund blevet kritiseret for at udgøre moderne lovgivningsrettet imperialisme. For ved vedtagelsen af EU's databeskyttelseslovgivning og den efterfølgende eksport heraf, herunder som led i opnåelsen af en tilstrækkelighedsafgørelse, undermineres tredjelandenes lovgivningsmæssige suverænitet.[139] Derudover risikerer landets borgere at opleve en form for "hvidvaskning af politik", hvor kilden til landets lovgivning findes andre steder end i landet selv.[140] Forbrugerne, virksomhederne og regeringen i tredjelandet ønsker måske andre regler end de i EU, men ser sig nødsaget til at importere dem for at få adgang til EU's marked.[141] Det er desuden væsentligt at holde sig for øje, at import af EU's regler ikke nødvendigvis er en anerkendelse fra tredjelandene om, at reglerne rent faktisk er de "bedste" eller "mest korrekte". De er i stedet udtryk for tredjelandenes behov for at få adgang til EU's marked.

Hvorvidt kritikken af EU som moderne imperialist holder vand er naturligvis diskutabel. EU tvinger trods alt ikke tredjelandene til at importere forordningens regler og principper.[142] Der er tale om et i tredjelandet opstået ønske om at tilpasse sig EU's standarder. Tilpasningen består desuden heller ikke i overtagelsen af alle forordningens regler og principper ord for ord, og der tages højde for forskelligheder i retslig kultur og normer. Dette kom eksempelvis til udtryk ved, at Israels og New Zealands mangel på en forfatning i traditionel forstand ikke stod i vejen for, at landene blev anset for sikre tredjelande. Tilstrækkelighedsafgørelser bør og er ofte præget af lange forhandlinger for at finde smidige løsninger på forskellene mellem EU og tredjelandet, hvilket vedtagelsen af de supplerende regler til APPI også er et eksempel på. Her viste EU sin villighed til at møde tredjelandet, Japan, midtvejs, og opfattelsen af EU som enevældig global lovgiver holder derfor ikke fuldt ud. EU er villig til at respektere det enkelte tredjelands tilgang til og regulering af databeskyttelse, så længe det i EU etablerede databeskyttelsesniveau ikke kompromitteres ved overførslen af personoplysninger til landet. Hvis tredjelandene selv nærer et ønske om at få adgang til og være aktive på EU's marked, er det således ikke urimeligt at kræve disses efterlevelse af de på markedet gældende regler.

6.4 Bruxelles-effekten og Japan

Et sted mellem at lægge sig fladt ned og efterkomme alle EU's krav eller udvise samme ubøjelighed som USA – som end ikke anmoder om en reel tilstrækkelighedsvurdering efter artikel 45, da resultatet er tydeligt for alle parter på forhånd – har Japan banet vejen for en ny model for tredjelande, der ønsker en tilstrækkelighedsafgørelse uden at gøre flere indrømmelser end højst nødvendigt.

[137] Christopher Kuner, EU Law Beyond EU Borders, s. 133.
[138] Anu Bradford, The Brussels Effect, s. 248.
[139] Ibid., s. 247.
[140] Ibid., s. 250.
[141] Ibid., s. 247.
[142] Ibid., s. 248.

Japan har antaget en "reaktiv" tilgang overfor EU, hvorved landet reagerer på de enkelte krav, som EU fremlægger i parternes forhandlinger og kun tilpasser sig disse krav. Det står i modsætning til den "proaktive" tilgang, som en del af de tidligere godkendte tredjelande antog, herunder eksempelvis Argentina, som importerede store dele af Spaniens databeskyttelseslovgivning direkte med henblik på godkendelse som sikkert tredjeland, jf. nærmere ovenfor i afsnit 6.1. Japans reaktive tilgang kommer også til udtryk ved det i afsnit 4.2.2 beskrevne toleddede databeskyttelsessystem, hvorefter de supplerende regler til APPI kun finder anvendelse på personoplysninger overført fra EU til Japan. Tilstrækkelighedsafgørelsen var som nævnt fra Japans side hovedsageligt motiveret af den økonomiske gevinst ved godkendelsen som sikkert tredjeland fremfor et ønske blandt den japanske befolkning om strengere databeskyttelse. Tilpasningen til EU's krav, herunder i form af de supplerende regler, blev derfor begrænset til det nødvendige for at opnå de økonomiske fordele. Det vil sige, at EU's succes med at fastsætte de globale databeskyttelsesstandarder – altså Bruxelles-effekten – har sine grænser. Tredjelande vil trods alt kun være motiverede til at tilpasse sig EU's krav i det omfang, de opnår økonomiske fordele herved, og opnåelsen af de økonomiske fordele nødvendiggør ikke, som Japan har erfaret, en tilpasning til alle EU's krav.[143]

Bruxelles-effekten lader sig dog stadig mærke ved eksempelvis, at den kulturelle særegenhed, som retningslinjerne udgør i Japan, forventes at blive behandlet ved den fremtidige revision.[144] Når retningslinjerne har fungeret i Japan og endda er mere eller mindre lige så effektive som bøder i EU, men EU alligevel anser dem for betænkelige og eventuelt utilstrækkelige, er det svært ikke at anerkende eksistensen af et retsimperialistisk anstrøg i EU's tilstrækkelighedsafgørelser. Udsigten til muligvis at overtage endnu flere af EU's regler og principper vækker da også bekymringer i Japan. Her har eksperter udtrykt tvivl om foreneligheden mellem EU's regler og traditioner og Japans kultur og normer. Der er tale om tvivl af en sådan størrelse, at det, uanset de ganske sandsynlige ændringer af især APPI for at imødekomme EU's krav ved revisionen, næppe kan forestilles, at landet ender med at vedtage databeskyttelseslovgivning, der læner sig betydeligt tættere op ad forordningen end allerede er tilfældet. Med andre ord forventer japanerne ikke selv at indordne sig de standarder, som EU har sat, mere end allerhøjst nødvendigt for at opretholde landets status som godkendt tredjeland.

Opsummerende kan det anføres, at tilstrækkelighedsafgørelser er et effektivt redskab for opnåelsen af EU's aspiration om at sætte de globale standarder for databeskyttelse, men har dog sine grænser. Så selvom effekten indimellem italesættes som en ustoppelig kraft, som tredjelandene er nødsaget til at acceptere ved at indordne sig EU's krav, viser afgørelsen for Japan, at tredjelande kan vælge et kompromis, hvor de økonomiske fordele ved en tilstrækkelighedsafgørelse opnås uden at tilpasse sig EU's standarder mere end højst nødvendigt.

7. Konklusion

Når Jean-Claude Juncker beskriver retten til databeskyttelse som at være uløseligt forbundet med selve det at være borger af EU,[145] indebærer det ikke, at retten er urørlig. For selvom retten til databeskyttelse er genstand for gennemgribende regulering i databeskyttelsesforordningen, hvis gennemslagskraft i stort omfang afhænger af, at forordningens pligtsubjekter ikke omgår deres pligter ved at overføre personoplysninger udenfor Unionen, hvor forordningens regler ikke finder anvendelse, er

[143] Flora Y. Wang, Cooperative Data Privacy, s. 688-689.
[144] Kommissionens gennemførelsesafgørelse (EU) 2019/419, betragtning 181, og Flora Y. Wang, Cooperative Data Privacy, s. 678.
[145] Jean-Claude Juncker, Unionens tilstand, s. 10.

sådanne internationale dataoverførsler en nødvendighed i nutidens digitale tidsalder. På den baggrund kan internationale dataoverførsler ske til tredjelande, hvis beskyttelsesniveau er blevet godkendt som tilstrækkeligt af Kommissionen i medfør af forordningens artikel 45, og dette speciale har haft til formål at vurdere, hvornår et sådant tilstrækkeligt beskyttelsesniveau foreligger.

Det kunne i den forbindelse konstateres, at Kommissionens tilstrækkelighedsafgørelser truffet efter både direktivet og forordningen antager en holistisk tilgang til vurderingen af tredjelandets beskyttelsesniveau. Særligt tredjelandets lovgivning – som eksempelvis i Japans tilfælde omfattede forfatningen, den almindelige lovgivning, de supplerende regler og retningslinjerne – indtager en central position i Kommissionens vurdering, men kan ikke i sig selv være altafgørende. Den egentlige håndhævelse af reglerne og de for de registrerede tilgængelige retsmidler udgør yderst vigtige momenter i vurderingen, da der ikke kan foreligge et tilstrækkeligt beskyttelsesniveau i et tredjeland, hvis lovgivning på papiret ikke efterleves i praksis. Mens de nævnte momenter klart har indtaget hovedrollerne i tilstrækkelighedsafgørelserne, inddrager Kommissionen også andre, supplerende momenter i sin vurdering i det omfang, det kan belyse beskyttelsesniveauet, eksempelvis eventuelle internationale forpligtelser og Databeskyttelsesrådets udtalelse.

Det kan ikke påstås, at de uoverensstemmelser, der gjorde sig gældende ved EU's praksis under direktivets tid, er helt afklarede i dag. Men med oplistningen i forordningens artikel 45, stk. 2, litra a-c af de ved tilstrækkelighedsvurderingen relevante momenter er der dog taget et stort skridt henimod øget forudsigelighed og gennemsigtighed ved processen for opnåelse af en tilstrækkelighedsafgørelse. Hertil bidrager også tilstrækkelighedsafgørelsen for Japan, som i langt højere grad end de tidligere afgørelser giver et indtryk af, hvad Kommissionen lægger vægt på ved sin vurdering. Dette er til fordel for såvel tredjelandene som for EU, da tredjelandene naturligvis vil være mere tilbøjelige til at udsætte sig for lange forhandlinger med EU, hvis de kender de overordnede krav til deres beskyttelsesniveau på forhånd og kan se, hvorledes Japan har båret sig gennem sine forhandlinger med EU. Afgørelsen for Japan udgør endvidere et eksempel på foreneligheden mellem to parter, hvis retslige kultur og sociale normer adskiller sig betydeligt fra hinanden. Dette illustrerer tilstrækkelighedsvurderingens elasticitet og Kommissionens vilje til at møde tredjelandet halvvejs for at åbne vejen for frie dataoverførsler mellem dem og således nyde de økonomiske fordele, der er forbundet hermed for begge parter. Domstolens fund af Privacy Shield-aftalen som ugyldig viser dog, at der er grænser for, hvor langt EU kan strække sig. For selvom artikel 45 ikke pålægger tredjelande et ækvivalenskrav, men blot et krav om, at der foreligger et beskyttelsesniveau, der i det væsentlige svarer til EU's, viser Schrems II-dommen, at dette krav kun opfyldt, hvis de grundlæggende rettigheder og frihedsrettigheder angivet i charteret er respekteret.

Endelig kan det konkluderes, at den "noget for noget"-tilgang, som Japan antog i sine forhandlinger med EU, hvor landet ikke tilpassede sig EU's krav mere end nødvendigt, og hvor afgørelsen tog form af en gensidig anerkendelse af hver parts tilstrækkelige beskyttelsesniveau, tjener som eksempel for andre tredjelande. For mens EU er blevet anklaget for at pådutte tredjelande sine databeskyttelsesstandarder gennem tilstrækkelighedsafgørelserne, har afgørelsen for Japan vist, at en tilpasning til EU's standarder kan være begrænset til det absolut nødvendige. Det vil sige, at der er grænser for Bruxelles-effekten. Generelt må det dog erkendes, at eftersom en tilstrækkelighedsafgørelse – samt de heri liggende økonomiske fordele – forudsætter, at tredjelandets beskyttelsesniveau i det væsentlige svarer til EU's, er tredjelandene nødt til at indordne sig EU's standarder i et vist omfang. Gør tredjelandene det, hvilket mange har gjort, opnår EU's databeskyttelsesregler efterhånden status af den globale standard og bekræfter dermed teorien om Bruxelles-effekten. Med Sydkorea som det

formentlig næste godkendte tredjeland samt en række andre lande i kø er det ikke svært at forestille sig, at Bruxelles-effekten på databeskyttelsesområdet vil tage til i styrke i de næste år.

8. Litteraturliste

Lovgivning

- Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (citeret: Konvention 108).
- Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (citeret: Databeskyttelsesdirektivet).
- Den Europæiske Unions charter om grundlæggende rettigheder, OJ [2000] C 364/1.
- Traktaten om Den Europæiske Union, OJ C 326, konsolideret i 2016.
- Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (citeret: Databeskyttelsesforordningen).
- Europarådets Konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger af 18. maj 2018 (citeret: Konvention 108+).

Domme

- Domstolens dom af 6. oktober 2015, Sag C-362/14, Maximillian Schrems mod Data Protection Commissioner, ECLI:EU:C:2015:650.
- Domstolens dom af 16. juli 2020, Sag C-311/18, Data Protection Commissioner mod Facebook Ireland Limited og Maximillian Schrems, ECLI:EU:C:2020:559.
- Conseil d'États dom af 12. marts 2021, CE – 450163, tilgængelig på https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2021-03-12/450163 [kun fransk] (sidst besøgt 23/05/2021).

Kommissionens beslutninger

- 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) (citeret: Beslutning 2000/518/EF).
- 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 harbour-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium (2000/520/EF) (citeret: Safe Harbour-aftalen).
- Kommissionens beslutning af 20. december 2001 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse af personoplysninger, der opnås ved hjælp af Canadas lov om beskyttelse af personoplysninger og elektroniske dokumenter (Canadian Personal Information Protection and Electronic Documents Act) (2002/2/EF) (citeret: Beslutning 2002/2/EF).
- Kommissionens beslutning af 30. juni 2003 i henhold til Europa-Parlamentets of Rådets direktiv 95/46/EF om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Argentina (2003/490/EF) (citeret: Beslutning 2003/490/EF).
- Kommissionens beslutning af 21. november 2003 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Guernsey (2003/821/EF) (citeret: Beslutning 2003/821/EF).

- Kommissionens beslutning af 28. april 2004 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Isle of Man (2004/411/EF) (citeret: Beslutning 2004/411/EF).
- Kommissionens beslutning af 8. maj 2008 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger på Jersey i henhold til Europa-Parlamentets og Rådets direktiv 96/46/EF (2008/393/EF) (citeret: Beslutning 2008/393/EF).
- Kommissionens afgørelse af 5. marts 2010 om tilstrækkeligheden af det beskyttelsesniveau, der sikres ved den færøske lov om behandling af personoplysninger, jf. Europa-Parlamentets og Rådets direktiv 95/46/EF (2010/146/EU) (citeret: Beslutning 2010/146/EU).
- Kommissionens afgørelse af 19. oktober 2010 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Andorra i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF (2010/625/EU) (citeret: Beslutning 2010/625/EU).
- Kommissionens afgørelse af 31. januar 2011 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om, hvorvidt staten Israel yder en tilstrækkelig beskyttelse af personoplysninger i forbindelse med automatisk behandling af personoplysninger (2011/61/EU) (citeret: Beslutning 2011/61/EU).
- Kommissionens gennemførelsesafgørelse af 21. august 2012 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om, hvorvidt Den Østlige Republik Uruguay yder en tilstrækkelig beskyttelse af personoplysninger i forbindelse med automatisk behandling af personoplysninger (2012/484/EU) (citeret: Beslutning 2012/484/EU).
- 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 (citeret: Privacy Shield-aftalen).
- Kommissionens gennemførelsesafgørelse (EU) 2019/419 af 23. januar 2019 i henhold til Europa-Parlamentets of Rådets forordning (EU) 2016/679 vedrørende Japans tilstrækkelige beskyttelse af personoplysninger i henhold til loven om beskyttelse af personlige oplysninger (citeret: Beslutning (EU) 2019/419).
- Kommissionens gennemførelsesafgørelse af 19. december 2021 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om, hvorvidt New Zealand yder tilstrækkelig beskyttelse af personoplysninger (2013/65/EU) (citeret: Beslutning 2013/65/EU).

Handelsaftaler

- Frihandelsaftale mellem Den Europæiske Union og dens medlemsstater på den ene side og Republikken Korea på den anden side, OJ L127, permanent i kraft siden 2015, tilgængelig på https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:22011A0514(01)&from=DA (sidst besøgt 23/05/2021).
- Aftale mellem Den Europæiske Union og Japan om et økonomisk partnerskab, L 330/3, 2019, tilgængelig på http://publications.europa.eu/resource/cellar/d40c8f20-09a4-11e9-81b4-01aa75ed71a1.0003.01/DOC_1 (sidst besøgt 23/05/2021).

Kommissionens meddelelser

- Europa-Kommissionen, Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om udveksling og beskyttelse af personoplysninger i en globaliseret verden, (COM(2017) 7 final), 10/02/2017, tilgængelig på https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52017DC0007&from=DA (sidst besøgt 23/05/2021) (citeret: Europa-Kommissionen: COM(2017) 7).

Bøger

- Blume, Peter, Databeskyttelsesret, 5. udgave, Jurist- og Økonomforbundets Forlag, 2018.
- Bradford, Anu, The Brussels Effect, Oxford Scholarship Online, 2019.
- Evald, Jens, Juridisk teori, metode og videnskab, 2. udgave, Djøf Forlag, 2020.
- Gram Mortensen, Bent Ole, Dansk Persondataret, 1. udgave, Ex Tuto Publishing A/S, 2020.
- Korfits Nielsen, Kristian og Lotterup, Anders, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udgave, Jurist- og Økonomforbundets Forlag, 2020.
- Kuner, Christopher, EU Law Beyond EU Borders: the extraterritorial reach of EU law, 1. udgave, Oxford University Press, 2019 (citeret: Christopher Kuner, EU Law Beyond EU Borders).

Artikler og tidsskrifter

- Greenleaf, Graham, Japan: EU Adequacy Discounted, 155 Privacy Laws & Business International Report 8, 2018, tilgængelig på https://poseidon01.ssrn.com/delivery.php?ID=180 (sidst besøgt: 23/05/2021).
- Meddin, Elisabeth, The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and XVII of the General Agreement on Trade in Services, American University International Law Review, vol. 35, nr. 4, s. 997-1036, 2020, tilgængelig på https://tinyurl.com/sdvrdz5s (sidst besøgt 23/05/2021) (citeret: Elisabeth Meddin, The Cost of Ensuring Privacy).
- Miyashita, Hiroshi, EU-Japan Mutual Adequacy Decision, Blog Droit Européen, 2020, tilgængelig på https://blogdroiteuropeen.files.wordpress.com/2020/06/miyashita-redo.pdf (sidst besøgt 23/05/2021).
- Stoddart, Jennifer, Chan, Benny, Joly, Yann, The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research, Journal of Law, Medicine and Ethics, vol. 44, nr. 1, s. 143-155, 2016, tilgængelig på https://www.researchgate.net/publication/318927320_The_European_Union%27s_Adequacy_Approach_to_Privacy_and_International_Data_Sharing_in_Health_Research (sidst besøgt 23/05/2021) (citeret: Jennifer Stoddart m.fl., The European Union's Adequacy Approach).
- Wang, Flora Y., Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement, Harvard Journal of Law and Technology, vol. 33, 2020, tilgængelig på https://jolt.law.harvard.edu/assets/articlePDFs/v33/33HarvJLTech661.pdf (sidst besøgt: 23/05/2021) (citeret: Flora Y. Wang, Cooperative Data Privacy).

Materiale fra Datatilsynet

- Datatilsynets journalnummer 2003-212-0143.
- Datatilsynets journalnummer 2002-216-0109.
- Datatilsynet, Vejledning – Overførsel af personoplysninger til tredjelande, juni 2019, tilgængelig på https://www.datatilsynet.dk/Media/8/9/Overførsel%20af%20personoplysninger%20til%20tredjelande.pdf (sidst besøgt 23/05/2021).

Materiale fra Databeskyttelsesrådet

- Det Europæiske Databeskyttelsesråd, Udtalelse 28/2018 vedrørende Kommissionens udkast til gennemførelsesafgørelse om tilstrækkelig beskyttelse af personoplysninger i Japan, 5. december 2018, tilgængelig på https://edpb.europa.eu/sites/default/files/files/file1/2018-12-05-opinion_2018-28_art.70_ja_da.pdf (sidst besøgt 23/05/2021) (citeret: Databeskyttelsesrådet, Udtalelse 28/2018).

Websteder

- Europa-Kommissionen, Unionens tilstand 2016 af Jean-Claude Juncker, formand for Europa-Kommissionen, 2016, tilgængelig på https://op.europa.eu/da/publication-detail/-/publication/c9ff4ff6-9a81-11e6-9bca-01aa75ed71a1 (sidst besøgt 23/05/2021) (citeret: Jean-Claude Juncker, Unionens tilstand).
- Memo fra Europa-Kommissionen, Key Elements of the EU-Japan Economic Partnership Agreement, 2018, tilgængelig på https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3326 (sidst besøgt 23/05/2021) (citeret: Kommissionen, Memo on Key Elements of the EU-Japan Economic Partnership Agreement).
- Pressemeddelelse fra Europa-Kommissionen, The European Union and Japan agreed to create the world's largest area of safe data flows, 2018, tilgængelig på https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4501 (sidst besøgt 23/05/2021).
- Abe, Shinzo, Toward a New Era of "Hope-Driven Economy": the Prime Minister's Keynote Speeach at the World Economic Forum Annual Meeting, 2019, tilgængelig på http://japan.kantei.go.jp/98_abe/statement/201901/_00003.html (sidst besøgt 23/05/2021) (citeret: Shinzo Abe, Keynote Speech).
- Pressemeddelelse fra det britiske datatilsyn, ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information, 2018, tilgængelig på https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/ (sidst besøgt 23/05/2021) (citeret: Pressemeddelelse fra det britiske datatilsyn).
- Fælles udtalelse fra Europa-Kommissionen og den sydkoreanske kommissionsformand, Joint Statement by Commissioner Reynders and Yoon Jong In, Chairperson of the Personal Information Protection Commission of the Republic of Korea, 2021, tilgængelig på https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1506 (sidst besøgt 23/05/2021) (citeret: Fælles udtalelse fra Europa-Kommissionen og den sydkoreanske kommissionsformand).
- Tale, vicepræsident af Europa-Kommissionen Viviane Reding, Speech: A data protection compact for Europe, 2014, tilgængelig på https://ec.europa.eu/commission/presscorner/detail/da/SPEECH_14_62 (sidst besøgt 23/05/2021).
- Europarådet, Convention 108 and Protocols, tilgængelig på https://www.coe.int/en/web/data-protection/convention108-and-protocol (sidst besøgt 23/05/2021).
- Katja Djurhuus, Bird & Bird, Fransk domstol anvender Schrems II præmisser på vaccinationsplatform: Brugen af AWS var ikke i strid med GDPR, 2021, tilgængelig på https://www.twobirds.com/da/news/articles/2021/denmark/conseil-d'etat---schrems-ii (sidst besøgt 23/05/2021) (citeret: Bird & Bird, Fransk domstol anvender Schrems II præmisser).
- Conseil d'État, The urgent applications judge does not suspend the partnership between the Ministry of Health and Doctolib for the management of COVID-19 vaccination appointments, 2021, tilgængelig på https://tinyurl.com/35tbkze4 (sidst besøgt 23/05/2021) (citeret: Conseil d'État, pressemeddelelse).