# INTERNATIONALE PERSONDATAOVERFØRSLER

## *INTERNATIONAL TRANSFERS OF PERSONAL DATA*

af MAKAR HOLST

*I denne kandidatafhandling undersøges europæiske virksomheders muligheder for at foretage internationale overførsler af persondata i lyset af EU-Domstolens afgørelse i C-362/14 Schrems, hvorved Domstolen kendte Europa-Kommissionens beslutning vedrørende Safe Harbor ugyldig.*
*Indledningsvis behandles det generelle overførselsbegreb, herunder særligt hvad der forstås ved en overførsel, og hvilke krav databeskyttelsesforordningen stiller til internationale overførsler af persondata. Endvidere undersøges den nu ugyldige Safe Harbor-beslutning med henblik på at klarlægge, hvorfor beslutningen blev kendt ugyldig. Herudover analyseres selve Schrems-dommen for at finde ud af, hvad domstolen fandt og på hvilken baggrund samt hvilke direkte og indirekte konsekvenser dommen har haft for mulighederne for at foretage internationale overførsler af persondata til tredjelande.*

*Domstolen bemærkede, at Kommissionen i deres egen vurdering af Safe Harbor-beslutningen og ordningen havde fundet, at Safe Harbor-ordningen tillod offentlige amerikanske myndigheder at tilgå personoplysninger overført på baggrund af ordningen. Udover at kende Safe Harbor-beslutningen ugyldig, udtalte Domstolen sig også om, hvad der kræves af lovgivning, der tillader indgreb i grundlæggende rettigheder efter EU's Charter om grundlæggende rettigheder.*
*Slutteligt diskuteres dommens konsekvenser for de øvrige overførselsgrundlag under databeskyttelsesforordningen, og hvorvidt disse muligheder fortsat er levedygtige post-Schrems.*

## Abstract

In this thesis, the possibilities for European companies to perform international transfers of personal data after the European Court of Justice's invalidation of the European Commission's Safe Harbor Decision are examined.

Firstly, the general notion of transfers is examined, especially what constitutes a transfer, what is required under the General Data Protection Regulation in order to transfer personal data across the world. Additionally, the now invalid Safe Harbor Decision, is examined in order to ascertain, what caused it to be declared invalid. Moreover, the Schrems judgment itself is dissected to establish what the court ruled, on what grounds it did so and what direct and indirect effects the judgment had on the possibilities to transfer personal data to third countries.

In its decision, the Court noted, that the European Commission in their own assessment had found, that the Safe Harbor allowed American authorities to access the personal data transfers under the regime. Consequently, the Court, besides invalidating Safe Harbor, generally noted, what is required of legislation enabling interference with fundamental rights guarantee by the Charter.

Lastly, the judgments impact on the other possibilities under the General Data Protection Regulation to perform international transfers has been discussed, and these possibilities' continued viability is questionable post-Schrems.

# Indholdsfortegnelse

# Forkortelser

| | |
|---|---|
| Chartret | Den Europæiske Unions Charter om grundlæggende rettigheder |
| Domstolen | EU-Domstolen |
| DPC | Data Protection Commissioner |
| EU | Den Europæiske Union |
| EØS | Det Europæiske Økonomiske Samarbejde |
| Gruppen | Artikel 29-gruppen |
| Kommissionen | Europa-Kommissionen |
| NSA | National Security Agency |
| Parlamentet | Europa-Parlamentet |
| TEUF | Traktaten om Den Europæiske Unions Funktionsmåde |

# Terminologi

*"Personoplysninger:* Enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet."[1]

*"Behandling*: Enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring,

[1] Databeskyttelsesforordningens artikel 4(1).

genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse."[2]

"*Dataansvarlig*: En fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; hvis formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret, kan den dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret."[3]

"*Databehandler*: En fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne."[4]

# 1. Introduktion

## 1.1. Indledning og problemformulering

Internettet kender ingen grænser. Information og tjenesteydelser er tilgængelige øjeblikkeligt fra alle verdenshjørner, og virksomheder lader sig ikke længere begrænse af deres geografiske placering, men betragter i højere grad hele verden som deres marked. Den teknologiske udvikling har gjort det muligt for selv små og mellemstore virksomheder at tilbyde deres tjenester til kunder i hele verden. Seneste tal viser, at der i 2014 blev overført femogfyrre gange så meget data på tværs af lande- og kontinentgrænser, som der blev overført i 2005.[5] Behovet for at flytte data rundt i verden vokser så hurtigt, at den eksisterende infrastruktur ikke kan følge med, og store, multinationale selskaber er begyndt at anlægge egne transatlantiske fiberkabler for at imødekomme deres stigende behov for at overføre data på tværs af kontinenter.[6]

En stor del af denne datastrøm indbefatter imidlertid personlige oplysninger; være det sociale mediers overførsler af oplysninger vedrørende deres brugere eller virksomheders overførsler af kundedata. Det er muligt, at disse personoplysninger på tværs af en koncerns selskaber verden over nyder den samme tekniske beskyttelse i form af høje it-sikkerhedsstandarter, men det er usikkert, hvorvidt den retlige beskyttelse af personoplysningerne er tilsvarende identisk på tværs af landegrænserne.

Den retlige beskyttelse af personoplysninger er et retsområde, der de seneste år har været genstand for stor bevågenhed, både på verdensplan og særligt i den Europæiske Union. Især reguleringen af internationale persondataoverførsler har tiltrukket sig stor opmærksomhed, da virksomheder i en stadigt mere globaliseret økonomi har et stort behov for at kunne overføre personoplysninger på tværs af deres egne afdelinger samt udveksle informationer med samarbejdspartnere. I denne forbindelse er den svære øvelse at tilgodese virksomhedernes mulighed for at drive forretning og forblive konkurrencedygtige på et internationalt marked, uden at borgernes fundamentale rettigheder og integritet krænkes.

[2] *Ibid.*, artikel 4(2).
[3] *Ibid.*, artikel 4(7).
[4] *Ibid.*, artikel 4(8).
[5] McKinsey Global Institute: Digital Globalization: The New Era of Global Flows, s. 4.
[6] Cade Metz: Facebook and Microsoft Are Laying a Giant Cable Across the Atlantic.

I efteråret 2015 afsagde EU-domstolen dom i Schrems-sagen[7], der bl.a. underkendte Safe Harbor-beslutningen, der dannede et særligt grundlag for dataoverførsler mellem amerikanske og europæiske virksomheder. Hermed blev der skabt uklarhed omkring mulighederne for at foretage internationale persondataoverførsler.

Formålet med denne afhandling er at analysere den nuværende retstilstand for så vidt angår internationale persondataoverførsler. Hvilke muligheder har europæiske virksomheder for at overføre personoplysninger på tværs af grænser i lyset af EU-domstolens dom i Schrems v. Data Protection Commissioner? Endvidere vil afhandlingen vurdere dommens betydning for de øvrige, særlige overførselsgrundlag, herunder standardkontrakter og bindende virksomhedsregler. Endeligt vil den nye Privacy Shield-ordning vil blive efterset med udgangspunkt i Schrems-dommens præmisser med henblik på at undersøge, hvorvidt denne ordning opfylder EU-domstolens krav om et beskyttelsesniveau for personoplysninger, "som i det væsentlige svarer til det niveau, der er sikret inden for Unionen."[8]

Afhandlingens opbygning beskrives nærmere nedenfor. I kapitel 2 belyses gældende ret efter Databeskyttelsesforordningen, og hvilke muligheder denne giver for at overføre personoplysninger på tværs af landegrænser. Kapitel 3 beskriver Safe Harbor-beslutningen, som Schrems-dommen kendte ugyldig, herunder baggrunden for Safe Harbor-ordningen og kritikken af den. I kapitel 4 gennemgås Schrems-dommen med en kort redegørelse for afgørelsens faktum efterfulgt af en nærmere analyse af dommens præmisser. I kapitel 5 vil dommens betydning for overførsler efter de særlige overførselsgrundlag blive bedømt, ligesom Privacy Shield-ordningen, der er tænkt som afløser for Safe Harbor-ordningen, vil blive vurderet i lyset af dommen. Afslutningsvis vil der i kapitel 6 blive konkluderet på afhandlingens analyser og vurderinger.

## 1.2. Metode og retskilder

Afhandlingen søger med udgangspunkt i den retsdogmatiske metode at beskrive og systematisere gældende ret vedrørende internationale persondataoverførsler.[9] Dette vil navnlig ske gennem behandling af retskilder af relevans for databeskyttelsesretten. Der gør sig herunder en række særlige retskildemæssige hensyn gældende i relation til denne afhandling. Disse omtales nærmere nedenfor.

Indledningsvist bør det bemærkes, at afhandlingens udgangspunkt er de unionsretlige retskilder, men fokus retter sig særligt mod de databeskyttelsesretlige retskilder, og der gøres ikke rede for Unionens overordnede retskilder, herunder traktatgrundlaget. Traktaten om Den Europæiske Unions Funktionsmåde berøres dog kort.

Databeskyttelsesrettens traditionelle retskilder vil heller ikke blive præsenteret særskilt og beskrevet i detaljer, men inddrages løbende i afhandlingen, da disse er behandlet dybtgående i den juridiske litteratur og formodes således at være læseren bekendt.[10]

Afhandlingen tager sit primære afsæt i Databeskyttelsesforordningen (2016/679), der blev publiceret i EU-tidende den 4. maj 2016 og står til at erstatte Databeskyttelsesdirektivet (95/46/EF). Databeskyttelsesforordningen finder direkte anvendelse i medlemslandene fra den 25. maj 2018.[11] Efter-

[7] Sag C-362/14 Schrems [2015].
[8] Sag C-362/14 Schrems [2015], præmis 73.
[9] Peter Blume: Retssystemet og juridisk metode, s. 40.
[10] Se for eksempel Peter Blume: Databeskyttelsesret, s. 15ff. og Christopher Kuner: European Data Protection Law, s. 18ff. samt Henrik Udsen: It-ret, s. 321ff. for nærmere om databeskyttelsesrettens historiske udvikling og dennes væsentligste retskilder.
[11] European Commission: Reform of EU Data Protection Rules.

som forordningen er vedtaget og allerede fra medio 2018 finder direkte anvendelse i medlemslandene som fundamentet for databeskyttelsesreguleringen, fremstår det naturligt, at afhandlingen tager udgangspunkt i denne. Det er særligt forordningens kapitel V, hvor reglerne om overførsler til tredjelande findes, der er genstand for nærmere undersøgelse i afhandlingen, da det er reglerne i artikel 44-49, der fastslår, i hvilket omfang internationale overførsler af personoplysninger kan ske. Analysen og vurderingen af Safe Harbor-ordningen, Schrems-dommen og dens betydning for de særlige overførselsgrundlag samt den nye Privacy Shield-ordning sker derfor ligeledes med udgangspunkt i disse regler. Det bemærkes, at bestemmelserne om videregivelse af personoplysninger til tredjelande i Databeskyttelsesdirektivet fandtes i artikel 25 og 26 i direktivets kapitel IV. Direktivets artikel 25 svarerede i sit indhold til forordningens artikel 45, mens indholdet af direktivets artikel 26 i forordningen er fordelt på artikel 46, 47 og 49. Eftersom Schrems-dommen er afsagt på baggrund af Databeskyttelsesdirektivet, kan der forekomme henvisninger til artiklerne, som de findes i direktivet, men der forsøges så vidt muligt ligeledes at angive forordningens ditto.

En særlig unionsretlig retskilde af relevans for databeskyttelsesretten, der også inddrages i afhandlingen, er Den Europæiske Unions Charter om grundlæggende rettigheder (herefter Chartret), der fastsætter en række fundamentale rettigheder, heriblandt retten til respekt for privatlivet samt retten til beskyttelse af personoplysninger.

Retspraksis fra EU-Domstolen vil ligeledes blive inddraget i et vist omfang. Det må dog i denne forbindelse konstateres, at de foreliggende afgørelser er afsagt på baggrund af Databeskyttelsesdirektivet og kan således kun belyse gældende ret efter Databeskyttelsesforordningen i det omfang, der ikke er sket en ændring af retstilstanden på det omhandlede område. Dette in mente inddrages foreliggende retspraksis, hvor dette stadig er egnet til at belyse retstilstanden på databeskyttelsesområdet. National retspraksis fra de enkelte medlemsstater medtages ikke henset til afhandlingens fællesskabsretlige udgangspunkt.

Det skal slutteligt bemærkes, at juridisk litteratur også inddrages. Størstedelen af den juridiske litteratur på området er dog ikke opdateret i relation til Databeskyttelsesforordningen, og det er generelt omdiskuteret, hvilken retskildeværdi juridisk litteratur kan tillægges.[12] Dette kan siges at mindske anvendeligheden heraf. Desuagtet anvendes litteraturen i afhandlingen i det omfang, hvor denne til stadighed er egnet til at bidrage til den grundlæggende forståelse af databeskyttelsesrettens retskilder og kan tjene til at underbygge argumentationen for indholdet af gældende ret på de områder, hvor retskilderne ikke er fyldestgørende.

## 1.3. Afgrænsning

Både i den private sektor og det offentlige eksisterer et behov for at kunne overføre personoplysninger internationalt. Afhandlingen er imidlertid afgrænset til mulighederne for at foretage internationale persondataoverførsler i den private sektor. Dette beror på, at de implicerede private aktører har en stor kommerciel interesse i reglerne for grænseoverskridende persondataoverførsler, ligesom området den seneste årrække har påkaldt sig stor opmærksomhed i den private sektor, både blandt virksomheder og individer, hvilket bl.a. er kommet til udtryk i Schrems-dommen.

Idet afhandlingen primært koncentrerer sig om databeskyttelse inden for den Europæiske Unions område, er fokus således rettet mod de unionsretlige retskilder med hovedfokus på Databeskyttelsesforordningen. Det skal imidlertid nævnes, at databeskyttelsesforordningen i sig selv er et komplekst og omfattende stykke lovgivning, og en dybtgående undersøgelse af forordningen kunne

[12] Peter Blume: Retssystemet og juridisk metode, s. 188.

danne grundlaget for adskillelige afhandlinger. Selvom denne afhandling tager udgangspunkt i databeskyttelsesforordningen som rammen for den unionsretlige databeskyttelsesregulering, falder det uden for afhandlingens fokus at undersøge databeskyttelsesforordningens specifikke nydannelser nærmere.

Længere redegørelser for fundamentale databeskyttelsesretlige grundbegreber er ligeledes undladt. Dette dels af hensyn til afhandlingens omfang, og dels under hensyntagen til, at der findes en legaldefinition af et flertal af begreberne i Databeskyttelsesforordningens artikel 4. Definitionen på de væsentligste, relevante begreber er gengivet ovenfor.

Eftersom afhandlingens fokus er den overordnede databeskyttelse inden for EU, berøres de enkelte medlemslandes lovgivning på området ikke. I mindre grad vil relevant amerikansk lovgivning blive inddraget, hvor det er nødvendigt i forbindelse med omtalen af Safe Harbor-ordningen samt i relation til undersøgelsen af EU-U.S. Privacy Shield-ordningen. En tilbundsgående analyse af amerikansk lovgivning på databeskyttelsesområdet falder dog uden for afhandlingens rammer.

Det bemærkes endvidere, at Schrems-dommen, der må siges at være omdrejningspunktet for denne afhandling, er todelt. Første del angår de nationale tilsynsmyndigheders kompetence til at behandle klager om tredjelandsoverførsler i tilfælde af en tilstrækkelighedsafgørelse truffet af Kommissionen, mens anden del angår gyldigheden af Safe Harbor-ordningen. Alene anden del er relevant for besvarelse af afhandlingens problemformulering, og første del omtales således kun flygtigt.

# 2. Overførsler af personoplysninger

Det anerkendes i Databeskyttelsesforordningen, at internationale dataoverførsler er nødvendige i en globaliseret økonomi og i den moderne digitale verden i øvrigt, jf. præambelbetragtning 101. Hvad forstås der imidlertid ved en overførsel?

I dette kapitel klarlægges først og fremmest, hvad der forstås hvad en overførsel, om der findes et entydigt overførselsbegreb, og om der er elementer, der har en særlig indflydelse på overførselsbegrebet. Herefter drøftes, hvorfor der findes særlige bestemmelser i Databeskyttelsesforordningen, der regulerer overførsler. Slutteligt undersøges det, hvilke muligheder Databeskyttelsesforordningen giver for at foretage overførsler, både inden for EU samt uden for.

## 2.1. Overførselsbegrebet

Der findes ingen definition af begrebet 'overførsel' i Databeskyttelsesforordningen. I Databeskyttelsesdirektivet fandtes ej heller en definition af begrebet.[13] Dette er imidlertid ikke ensbetydende med, at Databeskyttelsesforordningen ikke regulerer overførsler.

En overførsel er grundlæggende en form for behandling.[14] Det er dog uklart, hvad der nærmere skal forstås ved en overførsel. I OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, oprindeligt udstedt den 23. september 1980 og senest revideret den 11. juli 2013, er overførsler, der omtales som "transborder flows of personal data", defineret som "movement of personal data across national borders."[15] Opfattelsen er tilsvarende i Europarådets Konvention nr. 108 af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, hvor overførsler i artikel 12(1), beskrives som "transfers across

[13] Christopher Kuner: Transborder Data Flows and Data Privacy Law, s. 11.
[14] Se hertil Peter Blume: Retlig regulering af internationale persondataoverførsler, s. 21 og Christopher Kuner: European Data Protection Law, s. 159 samt Jan Trzaskowski et al.: Introduction to EU Internet Law, s. 110.
[15] The OECD Privacy Framework, s. 13.

national borders", ligesom overførsler i tillægsprotokollen til konventionen beskrives som overførsel af persondata til en modtager, der er underlagt en fremmed stats jurisdiktion.[16]

Som nævnt ovenfor er selve begrebet 'overførsel' ikke defineret i Databeskyttelsesforordningen, men ikke desto mindre findes bestemmelserne der regulerer overførsler, artikel 44-49, i forordningens kapitel V under overskriften "overførsel af personoplysninger til tredjelande". Ligeledes anvendes begrebet 'overførsel' i præamblen, særligt i betragtning 101-103, i forbindelse med overførsler til tredjelande. Overførsler må i overensstemmelse hermed forstås som overførsel af data på tværs af landegrænser, hvilket er i tråd med forståelsen og anvendelsen af begrebet i konvention nr. 108 samt OECD's retningslinjer.

### 2.1.1. Lovvalgets betydning for overførselsbegrebet

Efter denne forståelse af begrebet, er det dog stadigvæk uklart, om der foreligger en overførsel, når et andet land end eksportlandet udøver jurisdiktion og håndhæver den lov, der finder anvendelse på personoplysningerne, eller når personoplysningerne underlægges et andet lands lov end eksportlandet. Ifølge Blume er lovvalget afgørende for, om der foreligger en overførsel, da det er de materielle lovregler, der er afgørende for, hvilken beskyttelse af personoplysninger importlandet sikrer.[17] Blume understreger dog samtidig, at jurisdiktion må tillægges en vis betydning i forbindelse med overførselsbegrebet, da databeskyttelsesniveauet som sikres ved de materielle regler forudsætter, at dette niveau håndhæves i praksis.[18] Sondringen mellem jurisdiktion og lovvalg kan i denne henseende synes af underordnet betydning, da importlandet i almindelighed vil have jurisdiktion i forhold til de materielle lovregler, men dette er ikke altid tilfældet.[19] Reglerne om Databeskyttelsesforordningens territoriale anvendelse findes i artikel 3, der er forordningens modstykke til Databeskyttelsesdirektivets bestemmelse om lovvalg i artikel 4. Artikel 3, der ikke undersøges nærmere i denne afhandling, repræsenterer en væsentlig udvidelse af, hvornår europæiske databeskyttelsesregler finder anvendelse og betragtes af visse forfattere som en forordningens mest kontroversielle nydannelser.[20] Såfremt Databeskyttelsesforordningen efter en konkret vurdering finder anvendelse i medfør af artikel 3, vil der ikke være tale om en overførsel i forordningens forstand. Det bør ikke være nødvendigt at efterleve forordningens bestemmelser om overførsel til tredjelande, hvis forordningen alligevel finder direkte anvendelse. Det er herefter op til den dataansvarlige at tage stilling til, om Databeskyttelsesforordningen finder direkte anvendelse på deres behandling af personoplysninger, eller om den pågældende dataansvarlige skal iagttage forordningens bestemmelser om overførsel til tredjelande og sikre sig et særskilt hjemmelsgrundlag for overførslen.[21]

### 2.1.2. Overførselsmetoden

Fastlæggelsen af et entydigt overførselsbegreb bliver endvidere vanskeliggjort af de adskillelige faktiske metoder, hvorpå data kan overføres. En overførsel kan umiddelbart opfattes som en handling, hvor data aktivt føres på tværs af landegrænser, men ikke desto mindre kan der også være tale om en overførsel, når data gøres tilgængelig for modtagere andre steder i verden.

---

[16] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (Treaty No. 181), artikel 2(1).
[17] Peter Blume: Databeskyttelsesret, s. 323. Samme opfattelse Henrik Udsen: It-ret, s. 375.
[18] Peter Blume: International overførsel af personoplysninger, s. 152. Se samme for nærmere om overførselsbegrebet.
[19] Article 29 Working Party: Opinion 8/2010 on applicable law, s. 10.
[20] Dan Jerker B. Svantesson: Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, s. 230.
[21] Christopher Kuner: European Data Protection Law, s. 168.

Først og fremmest er det væsentlig at fastslå, at Databeskyttelsesforordningen finder anvendelse på "behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling", jf. artikel 2(1). Forordningen sigter mod at være teknologineutral, og databeskyttelsen efter forordningen "bør ikke afhænge af de anvendte teknikker".[22] Således er alle former for digital overførsel af data omfattet af forordningen, uanset om der er tale om en bærbar computer eller et flashdrev, der medtages på en udenlandsrejse, om dataoverførslen sker via internettet eller om en medarbejder tilgår virksomhedens intranet fra udlandet.[23]

I Lindqvist-sagen[24] forelå et spørgsmål for Domstolen om, hvorvidt der ved anvendelse af en konkret metode, navnlig tilgængeliggørelse på internettet, forelå en overførsel i Databeskyttelsesdirektivets forstand. Sagen angik en svensk statsborger, der havde tilgængeliggjort en række personoplysninger på en hjemmeside i forbindelse med hendes frivillige virke i en svensk kirke. Et af kernespørgsmålene, der forelå for Domstolen, angik, hvorvidt der foreligger en videregivelse af personoplysninger til et tredjeland, når personoplysninger lægges ud på en internetside, der hostes af en internetvært i EU og er tilgængelig for alle, herunder personer i et tredjeland.[25] Domstolen fandt, at der ikke var tale om en videregivelse af personoplysninger til et tredjeland i denne henseende. Afgørelsen var navnlig baseret på, at personoplysningerne ikke blev automatisk blev sendt til internetbrugere, men brugerne måtte selv tilgå den specifikke side for at få adgang til oplysningerne.[26] Ifølge Domstolen kunne det endvidere ikke antages, at lovgiverne havde til hensigt, at begrebet "videregivelse af personoplysninger til tredjeland" skulle omfatte en sådan situation, hvor personoplysninger blev gjort tilgængelige på en internetside, selvom om disse således blev gjort tilgængelige for personer i tredjelande.[27] Såfremt det antoges, at der forelå en overførsel i et sådant tilfælde, ville Databeskyttelsesdirektivets bestemmelser om videregivelse til tredjelande finde anvendelse på hele internettet.[28] Det er blevet anført, at Domstolens afgørelse i Lindqvist-sagen i høj grad bygger på dels de tekniske mekanismer vedrørende, hvordan personoplysningerne blev tilgået, dels pragmatiske overvejelser, herunder de implikationer, som det modsatte resultat ville haft, navnlig at internettet i praksis ville være blevet underlagt EU-lovgivning.[29]

Enkelte forfattere anfører dog, at ovenstående udgangspunkt om, at tilgængeliggørelse på internettet ikke konstituerer en overførsel, ikke er uden undtagelser. Ifølge Blume kan der være tale om en overførsel, såfremt en internetside er rettet mod bestemte modtagere i andre lande. Vurderingen af, om dette er tilfældet, må ske under hensyntagen til række momenter, fx det anvendte sprog samt informationers karakter.[30] Ligeledes påpeger Kuner, eftersom Lindqvist-sagen angik tilgængeliggørelse på en mindre skala, primært forbeholdt et kirkesamfund i ét medlemsland, at det ikke er utænkeligt, at der kan blive tale om overførsel, såfremt der sker tilgængeliggørelse af en større mængde personoplysninger, herunder særligt om tredjeparter, i et kommercielt øjemed.[31]

---

[22] Databeskyttelsesforordningens præambelbetragtning 15.
[23] Peter Blume: Retlig regulering af internationale persondataoverførsler, s. 27.
[24] Sag C-101/01 Lindqvist [2003].
[25] Sag C-101/01 Lindqvist [2003], præmis 52.
[26] *Ibid.*, præmis 60.
[27] *Ibid.*, præmis 68.
[28] *Ibid.*, præmis 69.
[29] Diane Rowland, Uta Kohl & Andrew Charlesworth: Information Technology Law, s. 370 og Christopher Kuner: Transborder Data Flows and Data Privacy Law, s. 12f. samt European Data Protection Law, s. 81.
[30] Peter Blume: Retlig regulering af internationale persondataoverførsler, s. 25.
[31] Christopher Kuner: European Data Protection Law, s. 83.

## 2.2. Generelt om overførsler

Databeskyttelsesforordningen tilstræber at yde et bestemt beskyttelsesniveau i forbindelse med behandling af personoplysninger. En grundlæggende forudsætning for, at dette beskyttelsesniveau kan sikres er, at der findes regler for overførsel af personoplysninger på tværs af landegrænser. Såfremt der ikke eksisterede regler for overførsel af personoplysninger, ville beskyttelsesniveauet som sikres ved forordningen være illusorisk, da personoplysninger uden videre vil kunne overføres til lande med færre forpligtelser forbundet med behandling af oplysningerne. I dette lys ses reglerne om overførsel af personoplysninger at spille en fundamental rolle for, at beskyttelsesniveauet ikke undermineres.[32] Det er først og fremmest en forudsætning for, at en overførsel kan finde sted, at forordningen overholdes til fulde, jf. artikel 44 samt præambelbetragtning 101. Der skal bl.a. være tale om en lovlig behandling af personoplysningerne efter artikel 6, før en overførsel kan finde sted. Hvis dette ikke var tilfældet, ville personoplysninger kunne indsamles arbitrært, overføres og underkastes behandling efter langt lempeligere regler end forordningen fastsætter. Såfremt det tilstræbte beskyttelsesniveau endvidere skal opretholdes, er det i nogle tilfælde nødvendigt, at yderligere betingelser opfyldes, før en overførsel kan finde sted. Dette gælder navnlig ved overførsel til tredjelande, som reguleres i forordningens kapitel V.

## 2.3. Overførsler inden for EU/EØS

Det fremgår af Databeskyttelsesforordningens artikel 1(3), at den frie udveksling af personoplysninger i EU hverken må indskrænkes eller forbydes af databeskyttelsesretlige grunde. Denne bestemmelse fastslår et af forordningens hovedformål, navnlig at sikre fri overførsel af personoplysninger på tværs af medlemslandene på baggrund af et identisk beskyttelsesniveau på tværs af medlemslandene. Dette var ligeledes Databeskyttelsesdirektivets formål, hvilket nævnes i Databeskyttelsesforordningens præambelbetragtning 3, ligesom det tidligere er blevet fremhævet i Lindqvist-sagen.[33] Databeskyttelsesdirektivets forsøg på at sikre den frie overførsel af personoplysninger stødte imidlertid i praksis på en række hurdles, som hovedsageligt tilskrives forskellene i gennemførelsen og anvendelsen af direktivet i medlemslandenes nationale lovgivning.[34] Det betones på denne baggrund i forordningens præambelbetragtning 10, at et højt beskyttelsesniveau sikres ved ens regler for databeskyttelse, der "anvendes konsekvent og ensartet overalt i Unionen." Databeskyttelsesforordningen sigter netop mod at skabe denne manglende ensartethed. I en erkendelse heraf konkluderes det således i præambelbetragtning 13, at der er behov for en forordning på området for at sikre et uniformt databeskyttelsesniveau på tværs af EU, eftersom forordninger anvendes for at sikre en identisk og samtidig lovgivning i Unionen.[35]

Eftersom de fleste[36] tidligere barriere for den frie overførsel inden for EU bliver nedbrudt med forordningen, må det på den baggrund konkluderes, at der reelt er fri overførsel af personoplysninger på tværs af medlemslandene. Det må forventes, at dette ligeledes vil gælde for EØS-landene, men

[32] Databeskyttelsesforordningens præambelbetragtning 101.
[33] Sag C-101/01 Lindqvist [2003], præmis 96.
[34] Databeskyttelsesforordningens præambelbetragtning 9.
[35] Sag C-34/73 Variola [1973], præmis 15.
[36] Det fremgår af forordningens præambelbetragtning 10, at der stadigt gives medlemslandene et vist albuerum til at indføre specifikke bestemmelser, fx regler for behandling af særlige kategorier af personoplysninger, men denne manøvremargen må antages at medføre mindre diskrepans i medlemslandenes beskyttelsesniveau, end det var tilfældet under Databeskyttelsesdirektivet.

der foreligger for nuværende endnu ingen beslutning fra EØS-komitéen om implementering af forordningen i EØS-landene.[37]

## 2.4. Overførsler til tredjelande

Når det kommer til tredjelande, stiller Databeskyttelsesforordningen sig ganske anderledes, end den frie dataoverførsel, der gælder inden for Unionens grænser. Forskellige lande har forskellige databeskyttelsesretlige regler og beskyttelsesniveauet kan variere i vidt omfang. Med henblik på at forhindre at Databeskyttelsesforordningens beskyttelse udhules ved, at personoplysninger overføres til et andet land, der ikke stiller samme høje krav i forbindelse med behandlingen af disse oplysninger, eksisterer særlige regler i Databeskyttelsesforordningens kapitel V. Disse regler skal iagttages, når personoplysninger ønskes overført til lande, der ikke er omfattet af Databeskyttelsesforordningen. Det følger af navnlig af artikel 44, at bestemmelserne i forordningens kapitel V er fastsat for, at beskyttelsesniveauet, som forordningen sikrer, ikke undermineres. Bestemmelsen tydeliggør herved forordningens udgangspunkt, at overførsler af personoplysninger kun accepteres, hvis importlandet yder et tilstrækkeligt beskyttelsesniveau sammenholdt med det, der ydes af forordningen. I artikel 45-49 findes herefter en række grundlag, som kan danne basis for overførsler til tredjelande.

### 2.4.1. Afgørelser om tilstrækkeligheden af beskyttelsesniveauet

Det første af disse grundlag findes i artikel 45, hvorefter overførsler kan finde sted, hvis Kommissionen har fastslået, at tredjelandet sikrer et tilstrækkeligt beskyttelsesniveau. En af Databeskyttelsesforordningens nyskabelser findes i artikel 45, hvorefter Kommissionen, foruden tredjelande, også har mulighed for at fastslå, at et område, en specifik sektor i et tredjeland eller en international organisation sikrer et tilstrækkeligt beskyttelsesniveau.[38] Sådanne afgørelser træffes ligeledes i medfør af artikel 45. Af hensyn til afhandlingens omfang beskrives artikel 45 alene med udgangspunkt i afgørelser om tilstrækkeligheden af et tredjelands beskyttelsesniveau.[39] Kommissionen kan træffe sådanne afgørelser i medfør af artikel 45(3). Hvis der foreligger en sådan afgørelse, kan der ske fri overførsel af personoplysninger til det pågældende tredjeland uden forudgående godkendelse på samme måde, som er tilfældet inden for Unionen.[40]

For nuværende har Kommissionen truffet sådanne afgørelser for 12 lande.[41] Disse afgørelser er truffet i medfør af Databeskyttelsesdirektivet, men det fremgår af Databeskyttelsesforordningens artikel 45(9), at disse afgørelser forbliver gyldige, indtil de ændres, erstattes eller ophæves i medfør af forordningens artikel 45(3) eller 45(5). Kommissionens afgørelse om tilstrækkeligheden af et tredjelands beskyttelsesniveau sker formelt ved en gennemførelsesretsakt, som vedtages efter undersøgelsesproceduren i artikel 93(2). Denne generelle procedure, der reguleres nærmere i forordning nr. 182/2011[42], træder i stedet for artikel 31-udvalget etableret ved Databeskyttelsesdirektivet. Af artikel 70(1)(s) følger det endvidere, at Databeskyttelsesrådet, som oprettes ved forordningen[43] og træder i stedet for den tidligere artikel 29-gruppe, har til opgave at afgive udtalelser til Kommissionen vedrørende beskyttelsesniveauet i et tredjeland, og hvorvidt dette er tilstrækkeligt. Der gjaldt

[37] European Free Trade Association: 32016R0679.
[38] Databeskyttelsesforordningens artikel 45 samt præambelbetragtning 103.
[39] Se nærmere om Databeskyttelsesforordningens nye muligheder for tilstrækkelighedsafgørelser Peter Blume: EU adequacy decisions: the proposed new possibilities.
[40] Databeskyttelsesforordningens artikel 45 samt præambelbetragtning 103.
[41] European Commission: Commission decisions on the adequacy of the protection of personal data in third countries.
[42] Europa-Parlamentets og Rådets Forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser.
[43] Databeskyttelsesforordningens artikel 68(1).

en tilsvarende procedure ved afgørelser om tilstrækkeligheden af beskyttelsesniveauet efter Databeskyttelsesdirektivet, hvor Kommissionen på baggrund af Artikel 29-gruppens udtalelser om beskyttelsesniveauet i det pågældende tredjeland og efter konsultation af Artikel 31-udvalget traf afgørelse.[44]

For så vidt angår momenterne, der skal tages i betragtning ved en afgørelse om tilstrækkeligt beskyttelsesniveau, fremgår disse af artikel 45(2). Vedrørende de første elementer fremgår følgende af artikel 45(2)(a):

"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 eller denne internationale organisation, retspraksis samt effektive rettigheder for registrerede, som kan håndhæves, og effektiv administrativ og retslig prøvelse for de registrerede, hvis personoplysninger overføres."

Der er tale om en lang række momenter, der skal tages i betragtning. I vurderingen skal ikke alene tredjelandets databeskyttelsesretlige regler indgå, men ligeledes landets respekt for menneskerettighederne og de grundlæggende frihedsrettigheder. Dette skal særligt ses i sammenhæng med Databeskyttelsesforordningens præambelbetragtning 1, hvor det fastslås, at databeskyttelse i EU betragtes som en grundlæggende rettighed, jf. herved også Chartrets, artikel 8 samt artikel 16, stk. 1, i TEUF, hvor det fastlås, at enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.

Når det konkret kommer til, hvilke databeskyttelsesretlige regler tredjelandet bør have for, at der er tale om et tilstrækkeligt beskyttelsesniveau, må der skelles til Artikel 29-gruppens synspunkter i et af gruppens tidlige arbejdsdokumenter.[45] Heri identificerer gruppen med udgangspunkt i Databeskyttelsesdirektivet en række kernekriterier, der bør opfyldes af tredjelandets databeskyttelsesretlige regulering, såfremt der skal være tale om et tilstrækkeligt beskyttelsesniveau.[46] Først og fremmest bør tredjelandets regulering indeholde tilsvarende principper for behandling af personoplysninger, som er nævnt i artikel 5. Idet gruppens udtalelse bygger på Databeskyttelsesdirektivet, nævnes princippet om opbevaringsbegrænsning ikke i udtalelsen, da dette princip først er fremkommet med Databeskyttelsesforordningen. Det må dog antages, at tredjelandets databeskyttelsesregulering bør indeholde tilsvarende principper, som nævnt i hele artikel 5, såfremt der skal være tale om et tilstrækkeligt beskyttelsesniveau i forhold til Databeskyttelsesforordningen. Dernæst skal de registrerede ved tredjelandets regulering være sikret en række rettigheder. For det første bør de registrerede have ret til indsigt, sml. herved artikel 15. For det andet bør de registrerede være sikret retten til berigtigelse, jf. artikel 16. Slutteligt bør de registrerede have ret til at gøre indsigelse mod behandlingen af personoplysninger, der vedrører den pågældende, jf. herved artikel 21. Det er i denne henseende værd at bemærke, at Artikel 29-gruppens udtalelse er fra 1998 og er som nævnt baseret på Databeskyttelsesdirektivet. En nutidig vurdering af, om et tredjeland har et tilstrækkeligt beskyttelsesniveau i forhold til Databeskyttelsesforordningen, vil formentlig ske på baggrund af alle momenter, der findes i forordningen, heriblandt fx retten til at blive glemt, jf. artikel 17. Dette støttes bl.a. af præambelbetragtning 104, hvoraf fremgår, at tredjelandet bør garantere, at der sikres et beskyttelsesniveau, som i det væsentlige svarer til det, der sikres i Unionen. Det skal dog understreges, at tilsvarende databeskyttelsesregulering ikke alene er tilstrækkeligt til en positiv vurdering efter arti-

[44] Peter Blume: Databeskyttelsesret, s. 333.
[45] Article 29 Working Party: Transfers of personal data to third countries.
[46] *Ibid.*, s. 5.

kel 45(1), da der er tale om en helhedsvurdering, jf. herved præambelbetragtning 104 samt artikel 45(2)(a).

I artikel 45(2)(a) fremhæves endvidere særligt, at der skal lægges vægt på, hvorvidt tredjelandet har regler, der regulerer videreoverførsel af personoplysninger til andre tredjelande. Dette er særligt vigtigt, da manglen på sådanne regler indebærer en risiko for, at hele beskyttelsesniveauet som forordningen fordrer undermineres ved at personoplysningerne uden videre vil kunne overføres til lande, der ikke sikrer et tilstrækkeligt beskyttelsesniveau.[47]

Bestemmelsen lægger ligeledes vægt på, at disse regler skal kunne håndhæves for at forhindre, at der bliver tale om et illusorisk beskyttelsesniveau. Hertil fremgår det af artikel 45(2)(b), at der tillige skal lægges vægt på, hvorvidt tredjelandet har en uafhængig tilsynsmyndighed, der sikrer at beskyttelsesreglerne overholdes. Dette blev ligeledes fremhæves af Artikel 29-gruppen i deres udtalelse.[48] Det er værd at bemærke, at kravene til procedure og håndhævelse ikke er nærmere præciseret, hverken af Artikel 29-gruppen eller i Databeskyttelsesforordningen, men må ikke desto mindre tillægges vægt, såfremt der ikke skal blive tale om et proforma beskyttelsesniveau.

Det skal endeligt tages i betragtning, hvilke internationale forpligtelser vedrørende beskyttelse af personoplysninger tredjelandet har påtaget sig, jf. artikel 45(1)(c). Tredjelandets tiltrædelse af Europarådets Konvention nr. 108 af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger og tillægsprotokollen hertil taler i retning af et tilstrækkeligt beskyttelsesniveau.[49]

Eftersom databeskyttelsesreguleringen ikke er en konstant størrelse, men konstant undergår forandring, fastlås det i artikel 45(3), at Kommissionens tilstrækkelighedsafgørelse skal revideres mindst hvert fjerde år. Eventuelle udviklinger i tredjelandet tages herunder i betragtning.[50] Dette sikrer, at vurderingen af tredjelandets beskyttelsesniveau konstant er tidssvarende og forhindrer, at der sker overførsler såfremt landet grundet lovændringer ikke længere opretholder et tilstrækkeligt beskyttelsesniveau. Bestemmelsen i artikel 45(4), hvorefter Kommissionen løbende overvåger udviklingen i det pågældende tredjeland, skal ses i sammenhæng hermed.

### 2.4.2. Overførsler omfattet af fornødne garantier

I mangel på en tilstrækkelighedsafgørelse efter artikel 45, stk. 3, indtræder spørgsmålet, i hvilket omfang der i så fald kan overføres personoplysninger til tredjelande. Svaret herpå findes i artikel 46, der regulerer en række særlige ordninger, der fungerer som overførselsgrundlag, samt artikel 49, hvorefter overførsel i særlige situationer undtagelsesvist kan ske.

Artikel 46 giver overordnet set adgang til at foretage overførsler, hvis dataeksportøren "har givet de fornødne garantier, og på betingelse af at rettigheder, som kan håndhæves, og effektive retsmidler for registrerede er tilgængelige." Af bestemmelsens stk. 2 og 3, fremgår mere specifikt, hvorledes disse fornødne garantier kan sikres. Der skelnes mellem garantier, som ikke kræver specifik godkendelse fra den kompetente tilsynsmyndighed, jf. stk. 2, og garantier, som kræver godkendelse, jf. stk. 3. Nedenfor omtales de mest anvendte af de såkaldte særlige overførselsgrundlag. Under henvisning til afhandlingens afgrænsning, skal det herunder kort bemærkes, at overførselsgrundlaget for overførsler mellem offentlige myndigheder som findes i artikel 46(2)(a), ikke omtales nærmere.

---

[47] Peter Blume: Retlig regulering af internationale persondataoverførsler, s. 88.
[48] Article 29 Working Party: Transfers of personal data to third countries, s. 7.
[49] Databeskyttelsesforordningens præambelbetragtning 105.
[50] *Ibid.*, præambelbetragtning 106.

#### 2.4.2.1. Bindende virksomhedsregler

Artikel 46(2)(b) nævner bindende virksomhedsregler som en måde, hvorpå et særligt overførselsgrundlag kan tilvejebringes. Ved bindende virksomhedsregler forstås et sæt retligt bindende regler på koncernniveau, som fastsætter principper og procedurer for databehandling på tværs af koncernen samt tildeler de registrerede en række rettigheder, der kan håndhæves.[51] Der findes ikke et standard sæt bindende virksomhedsregler, og der skal udarbejdes individuelle regler for den enkelte koncern tilpasset herefter. Det betyder samtidigt, at alene koncerner af en vis størrelse vil anse bindende virksomhedsregler som et egnet overførselsgrundlag henset til det ikke ubetydelige ressourceforbrug forbundet med udarbejdelsen af et sæt virksomhedsregler.[52]

Efter artikel 47 forelægges det udarbejdede sæt bindende virksomhedsregler for den kompetente tilsynsmyndighed til godkendelse. Godkendelsen er, jf. artikel 47(1)(a) til (c), betinget af, at de bindende virksomhedsregler er retligt bindende for alle koncernens virksomheder, således at de registrerede kan håndhæve de rettigheder, virksomhedsreglerne tillægger dem, ligesom virksomhedsreglerne indholdsmæssigt skal opfylde de mindstekrav, der følger af artikel 47(2).

Når et sæt bindende virksomhedsregler foreligger, kan der herefter ske fri overførsel af personoplysninger på tværs af koncernens virksomheder, uanset om disse geografisk er placeret inden for eller uden for EU.

#### 2.4.2.2. Kontraktbestemmelser

En yderlige måde, hvorpå sådanne fornødne garantier kan sikres, er ved en indgåelse af en kontrakt mellem dataeksportøren og –importøren, der tjener som grundlag for overførslen. Efter artikel 46(2)(c) og (d), kan der enten gøres brug af standardkontraktbestemmelser udarbejdet af Kommissionen selv eller kontraktbestemmelser udarbejdet af en tilsynsmyndighed og efterfølgende godkendt af Kommissionen. Kommissionen har til dato vedtaget tre standardkontrakter.[53] I artikel 46(5) fastslås det udtrykkeligt, at disse Kommissionsafgørelser fortsat er i kraft indtil de ændres, erstattes eller ophæves i henhold til artikel 46(2). Anvendelse af disse standardkontrakter kan ske uden forudgående tilladelse fra den kompetente tilsynsmyndighed. Det står derudover dataeksportøren og –importøren frit for selv at udfærdige en kontrakt, der kan tjene som grundlag for tredjelandsoverførslen, men i sådanne tilfælde skal kontrakten godkendes af den kompetente tilsynsmyndighed, jf. artikel 46(3).

Kommissionen godkendte i 2001 den første standardkontrakt, der angår overførsler mellem to dataansvarlige.[54] Kontrakten indgås mellem dataeksportøren og –importøren, som efter kontrakten afgiver et tredjepartsløfte, hvorved den registrerede gives håndhævelsesmuligheder i tilfælde af parternes misligholdelse af deres forpligtelser. Ligeledes tildeles eksportlandets tilsynsmyndighed ved kontrakten en række beføjelser. Endeligt garanterer kontrahenterne, at deres behandling af personoplysningerne vil ske i overensstemmelse gældende regler, hvilket for dataeksportøren er bestemmelserne i Databeskyttelsesforordningen og for dataimportøren er de obligatoriske databeskyttelsesprincipper, der findes som tillæg til kontrakten. I 2004 vedtog Kommissionen endnu en standardkontrakt[55] til brug for overførsler mellem to dataansvarlige som følge af bemærkninger til

[51] Christopher Kuner: European Data Protection Law, s. 219.
[52] Peter Blume: Retlig regulering af internationale persondataoverførsler, s. 138.
[53] Beslutningerne 2001/497/EF, 2004/915/EF og 2010/87/EU.
[54] Beslutning 2001/497/EF.
[55] Beslutning 2004/915/EF.

2001-kontrakten.[56] Kontrakternes væsentligste forskel ligger i ansvarsfordelingen mellem kontraktparterne, hvor der efter 2001-kontrakten gælder et solidarisk ansvar for skade påført den registrerede, jf. kontraktens standardbestemmelse 6 samt Kommissionsbeslutningens præambelbetragtning 19, mens hver part efter 2004-kontrakten ifalder ansvar ved misligholdelse af deres egne forpligtelser.[57] Den tredje standardkontrakt angår overførsler til fra dataansvarlig til databehandler, og den nyeste udgave heraf blev godkendt i 2010.[58]

Når disse standardkontraktbestemmelser omtales som standardkontraker sker det i lyset af, at kontrahenterne kan anvende den eksisterende kontraktstruktur som fremgår af Kommissionsbeslutningerne, ligesom standardkontraktbestemmelserne kan medtages i en bredere kontekst.[59] Standartkontraktbestemmelserne kan således også indgå i en større kontrakt mellem kontrahenterne, hvor også andre kontraktbestemmelser fremgår.[60]

#### 2.4.2.3. Adfærdskodeks og certificering

Endeligt fremgår det af artikel 46(2), at der kan ske overførsel til tredjelande, såfremt der gives et bindende tilsagn, der kan håndhæves, til et godkendt adfærdskodeks eller en godkendt certificeringsmekanisme i medfør af artikel 40 og 42 henholdsvis. Der er tale om forskellige former for frivillig selvregulering, der imidlertid tillægges den betydning, at en overholdelse heraf er med til at skabe en formodning for, at forordningens bestemmelser overholdes, jf. herved bl.a. artikel 24(3) og 28(5).

Af artikel 40(2), fremgår det, at repræsentanter for kategorier af dataansvarlige og databehandlere kan udarbejde adfærdskodekser, ligesom det fremgår hvilke elementer, kodekset kan indeholde. Adfærdskodekser har til formål at "fremme en effektiv anvendelse af denne forordning under hensyntagen til de specifikke typer af behandling, der foretages i visse sektorer."[61] Efter artikel 40(5) forelægges et udkast til adfærdskodeks til godkendelse hos den kompetente tilsynsmyndighed, og såfremt kodekset vedrører flere medlemslande, forelægger den kompetente tilsynsmyndighed udkastet for Databeskyttelsesrådet, jf. artikel 40(7). Finder Databeskyttelsesrådet, at adfærdskodekset er i overensstemmelse med forordningen, afgiver rådet en udtalelse til Kommissionen, som herefter ved en gennemførelsesretsakt kan bestemme, at adfærdskodekset er generelt gyldigt i Unionen, jf. artikel 40(9).

Certificering og mærkning er en yderligere måde for dataansvarlige og databehandlere at skabe transparens omkring disses behandling af personoplysninger og vise, at behandlingen sker i overensstemmelse med forordningen.[62] Fremgangsmåden for certificering er nærmere fastlagt i forordningens artikel 42 og 43. Særligt fremgår det af artikel 42(2), at certificering kan anvendes med henblik på tredjelandsoverførsler, såfremt en virksomhed i et tredjeland opnår certificering i medfør af artikel 42 og afgiver bindende tilsagn om at efterleve denne certificering, herunder dennes håndhævelsesmuligheder. Certificering forestås af et akkrediteret certificeringsorgan, jf. artikel 43.

---

[56] *Ibid.*, præambelbetragtning 2.
[57] Beslutning 2004/915/EF, bilag 1, standardbestemmelse III samt præambelbetragtning 5.
[58] Beslutning 2010/87/EU.
[59] For en nærmere gennemgang af fordele og ulemper ved anvendelse af standardkontraktbestemmelser som grundlag for tredjelandsoverførsler samt deres anvendelse i praksis se Peter Blume: Retlig regulering af internationale persondataoverførsler, s. 136 samt Christopher Kuner: European Data Protection Law, s. 192ff.
[60] Databeskyttelsesforordningens præambelbetragtning 109.
[61] *Ibid.*, præambelbetragtning 98.
[62] *Ibid.*, præambelbetragtning 100.

### 2.4.3. Undtagelser i særlige situationer

I artikel 49 findes en række undtagelser, hvorefter en overførsel til tredjelande kan finde sted til trods for en manglende tilstrækkelighedsafgørelse i henhold til artikel 45, stk. 3, eller fornødne garantier i henhold til artikel 46. Herom kan der generelt siges, at der er tale om snævre, singulære undtagelser, der skal fortolkes restriktivt.[63]

Undtagelserne, der er relevante for private aktører, er særligt artikel 49(1)(a), hvorefter en overførsel kan ske, hvis den registrerede har samtykket heri, samt artikel 49(1)(c) og (d). Herefter kan der foretages en overførsel, hvis det sker med henblik på opfyldelsen af en kontrakt mellem den dataansvarlige og den registrerede, jf. artikel 49(1)(c) eller opfyldelsen af en kontrakt indgået mellem den dataansvarlige og en tredjemand i den registreredes interesse, jf. artikel 49(1)(d).

Artikel 29-gruppen forholder sig generelt skeptisk til anvendelsen af undtagelserne i artikel 49 (direktivets artikel 26), idet dataeksportøren ikke er forpligtet til at beskytte personoplysningerne i importlandet, ligesom eksportøren ikke er forpligtet til at indhente forudgående tilladelse fra den relevante tilsynsmyndighed til overførslen.[64] Disse undtagelser bør således alene benyttes, når muligheden for at foretage overførsler i medfør af de øvrige muligheder i artikel 45-47 nærmer sig det umulige. Det understreges på det kraftigste af Artikel 29-gruppen, at undtagelserne er uegnede til at fungere som grundlag for overførsler af betydelig størrelse og alene bør benyttes som sidste udvej.[65] Henset til afhandlingens omfang vil disse undtagelser ikke omtales yderligere, men er ikke desto mindre nævneværdige, eftersom de undtagelsesvist kan danne grundlag for overførsler til tredjelande.

Der findes således samlet set en række grundlag i Databeskyttelsesforordningen, der kan benyttes som grundlag for at overføre personoplysninger til tredjelande. Nedenfor omtales et yderligere tidligere overførselsgrundlag, som er ulig de ovennævnte og påkalder sig særlig opmærksomhed henset til dens specielle karakter.

# 3. Safe Harbor

## 3.1. Introduktion

EU's og USA's økonomier tegner sig tilsammen for halvdelen af verdens BNP og cirka en tredjedel af al verdenshandel[66], og USA er hjemsted for størstedelen af verdens teknologivirksomheder. Det kan derfor næppe undre, at EU og USA tilsammen står for den største procentdel af den samlede tværkontinentale datatrafik.[67] Desuagtet betragtes USA af EU i databeskyttelsesretlig henseende ikke som et land, der sikrer et tilstrækkeligt beskyttelsesniveau, og der foreligger ikke en tilstrækkelighedsafgørelse i medfør af artikel 45(3) for USA.[68] I betragtning af ovenstående kendsgerninger var det efter vedtagelsen af Databeskyttelsesdirektivet nødvendigt at tilvejebringe et grundlag, hvorefter overførsler til USA kunne ske. Dette overførselsgrundlag blev til ved Safe Harbor-ordningen, der tillod overførsel af personoplysninger til udvalgte virksomheder i USA, som certificerede sig under ordningen.

---

[63] Article 29 Working Party: Transfers of personal data to third countries, s. 24.
[64] Article 29 Working Party: Working document: Article 26(1), s. 6.
[65] *Ibid.*, s. 9.
[66] European Commission: United States - Trade.
[67] McKinsey Global Institute: Digital Globalization: The New Era of Global Flows, s. 4.
[68] European Commission: Commission decisions on the adequacy of the protection of personal data in third countries.

I afsnit 3.2. behandles selve ordningen, herunder dens tilblivelse, samt hvordan den fungerede i praksis. Herefter anskues ordningen i 3.3. og 3.4. fra to vinkler. Hvorfor var der overhovedet behov for en særlig ordning for overførsler mellem EU og USA, og herefter drøftes hvilke problemer ordningen i praksis stødte på i dens forsøg på at opfylde dette behov.

## 3.2. Kommissionsbeslutning 2000/520/EF

Kommissionen vedtog den 26. juli 2000 beslutning 2000/520/EF. Denne fastslog, at Safe Harbor-ordningen, der var udarbejdet af det amerikanske handelsministerium, kunne benyttes som grundlag for at overføre personoplysninger fra EU til certificerede virksomheder i USA.[69] Grundlaget for ordningen var en række dokumenter, der fandtes som bilag til Kommissionsbeslutningen, herunder navnlig Safe Harbor-principperne samt hyppigt stillede spørgsmål, der gav vejledning for implementeringen af principperne.[70] Selve Kommissionsbeslutningen var baseret på Databeskyttelsesdirektivets artikel 25(6) (forordningens artikel 45(3)), og der var således tale om en form for afgørelse om tilstrækkeligheden af beskyttelsesniveauet.[71]

Ordningen omfattede alene den private sektor og fungerede ved, at amerikanske virksomheder kunne tilslutte ordningen ved offentligt at tilkendegive, at de forpligtede sig til at overholde principperne, der gennemføres i overensstemmelse med de hyppigt stillede spørgsmål[72], hvilket skulle meddeles det amerikanske handelsministerium.[73] Det var endvidere kun muligt for virksomheder underlagt enten Federal Trade Commission (herefter FTC) eller det amerikanske transportministerium at tilslutte sig ordningen.[74] Dette udelukkede en række virksomheder såsom finansielle virksomheder og teleudbydere fra at benytte ordningen, eftersom disse er undtaget FTC's kompetence.[75] Når en amerikansk virksomhed havde certificeret sig som en Safe Harbor-virksomhed, kunne der herefter ske fri overførsel af personoplysninger fra EU til denne virksomhed, idet virksomheden således antoges at sikre et tilstrækkeligt beskyttelsesniveau i kraft af Safe Harbor-certificeringen.

Safe Harbor-ordningen bestod i al væsentlighed af syv principper, der fandtes som bilag I til Kommissionsbeslutning 2000/520/EF, navnlig oplysningspligt, valgfrihed, videreoverførsel, sikkerhed, dataintegritet, indsigt og håndhævelse. Virksomheden var først og fremmest forpligtet til at informere de registrerede, når der blev indsamlet oplysninger, herunder give oplysninger om til hvilke formål oplysningerne indsamledes, samt hvordan oplysningerne anvendtes. De registrerede skulle kunne frasige sig, at oplysningerne anvendtes i strid med det oprindelige formål eller videregives til tredjemand. Såfremt virksomheden ønskede at videregive oplysningerne til tredjemand, skulle virksomheden sikre sig, at tredjemand ligeledes overholdt Safe Harbor-principperne, var omfattet af databeskyttelsesdirektivet eller at tredjemand på anden måde ydede tilstrækkelig beskyttelse af personoplysningerne. Virksomheden skulle træffe passende foranstaltninger for at sikre datasikkerheden. Endeligt måtte virksomheden ikke behandle personoplysningerne i uoverensstemmelse med det formål, hvortil de oprindeligt blev indsamlet, ligesom der skulle gives indsigt i de oplysninger, som virksomheden var i besiddelse af. Det syvende princip angik håndhævelse, og fastslog, at der bl.a. skulle være tilgængelige og uafhængige klageadgange, der var forpligtede til at afhjælpe even-

[69] Beslutning 2000/520/EF, artikel 1.
[70] *Ibid.*, præambelbetragtning 5.
[71] *Ibid.*, præambelindledningen.
[72] *Ibid.*, artikel (1)(2)(a).
[73] *Ibid.*, artikel 1(3).
[74] *Ibid.*, artikel 1(2)(b) samt præambelbetragtning 6.
[75] *Ibid.*, bilag III (s. 2).

tuelle problemer, som skyldes manglende overholdelse af principperne, samt mulighed for at sanktionere dette.[76]

## 3.3. Europæisk kontra amerikansk databeskyttelsesret

Der eksisterer unægtelig et behov for både europæiske og amerikanske virksomheder for at kunne overføre personoplysninger på tværs af Atlanten. Det kan imidlertid undre, at behovet alene kan opfyldes ved en form for modificeret tilstrækkelighedsafgørelse, som Safe Harbor-ordningen kan siges at være.[77] Dette skal ses i lyset af de fundamentale forskelle mellem den europæiske og amerikanske opfattelse af privatlivsbeskyttelse og regulering af databeskyttelse.

Siden Europarådets Konvention 108 har grundtanken i europæisk databeskyttelsesregulering været, at der skal sikres en overordnet regulering af behandlingen af personoplysninger. Et stort skridt i denne retning blev taget med vedtagelsen af Databeskyttelsesdirektivet, der fandt generel anvendelse på behandling af personoplysninger, såvel elektronisk som ikke-elektronisk, og som blev implementeret i samtlige EU's medlemslande.[78] Denne opfattelse og tilgang til databeskyttelse må siges være blevet cementeret med vedtagelsen af Databeskyttelsesforordningen, og retten til privatliv og beskyttelse af personoplysninger anses i EU i øvrigt som fundamentale og grundlæggende rettigheder, jf. Chartrets artikel 7 og 8.

I USA er der tilsvarende en tradition for privatlivsbeskyttelse, der kan spores tilbage til den amerikanske uafhængighedserklæring.[79] Ved et nærmere kig på den amerikanske privatlivsbeskyttelse kommer væsentlige forskelle dog til syne, alt afhængigt om der er tale om den offentlige eller private sektor. For så vidt angår den offentlige sektor er der i amerikansk højesteretspraksis udviklet en ret til privatliv på baggrund af en række forfatningstillæg.[80] Derudover gennemførtes i 1974 Privacy Act, der har til formål at beskytte borgerne mod offentlige myndigheders uberettigede indgreb i borgernes privatliv.[81] Ved vedtagelsen beskyttede loven dog kun amerikanske statsborgere.[82] I den private sektor findes der på føderalt niveau kun få bestemmelser, der regulerer specifikke brancher.[83] I de individuelle stater er lovgivningen tilsvarende sektororienteret.[84]

Forskellene mellem europæiske og amerikansk databeskyttelse må siges at være et resultat af denne forskellige tilgang til privatlivsbeskyttelse. Mens en grundlæggende, altomfattende, regulering foretrækkes på europæisk plan, har reguleringen i USA altovervejende været baseret på specifikke lovregler samt normer udviklet af erhvervslivet selv.[85]

## 3.4. Kritik af ordningen

Både før dens undfangelse og i løbet af dens levetid blev Safe Harbor-ordningen af forskellige årsager kritiseret fra flere sider. Kritikken er i denne sammenhæng nævneværdig, da Domstolen ved dens underkendelse af Safe Harbor-beslutningen hæftede sig ved nogle af nedenstående kritikpunkter, ligesom dele af kritikken ikke er begrænset til selve Safe Harbor-ordningen, men kan siges at

[76] Beslutning 2000/520/EF, bilag I (s. 2f.).
[77] Se oven for note 66.
[78] Daniel R. Leathers: Giving Bite to the EU-U.S. Data Privacy Safe Harbor, s. 197.
[79] Martin Weiss et al.: U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, s. 3.
[80] Peter Blume: Databeskyttelsesret, s. 345.
[81] United States Department of Justice: Overview of the Privacy Act of 1974, s. 4.
[82] United States Department of Justice: Overview of the Privacy Act of 1974, s. 15.
[83] Daniel R. Leathers: Giving Bite to the EU-U.S. Data Privacy Safe Harbor, s. 197.
[84] Executive Office of the President: Big Data: Seizing Opportunities, Preserving Values, s. 18.
[85] Joel R. Reidenberg: Setting Standards for Fair Information Practice in the US Private Sector, s. 500.

gælde generelt for denne type selvcertificeringsordninger. Privacy Shield-ordningen er tilsvarende en selvcertificeringsordning, og kritikken tjener til at belyse, hvorvidt en sådan ordning er levedygtig under Databeskyttelsesforordningens bestemmelser om overførsel til tredjelande.

Vedrørende ordningen påpegede Europa-Parlamentet først og fremmest, at Kommissionens udkast til en tilstrækkelighedsafgørelse ikke baserede sig på en eksisterende Safe Harbor-ordning, men alene på et udkast til ordningen med dertilhørende forklaringer, som vil blive udstedt.[86] Det er endvidere blevet påpeget, at Kommissionen ved en tilstrækkelighedsafgørelse efter Databeskyttelsesdirektivets artikel 25(2), skal vurdere tredjelandets beskyttelsesniveau på baggrund af "de retsregler, almindelige regler eller sektorregler, der er i kraft i det pågældende tredjeland."[87] Kommissionen kan først efter det tidspunkt, hvor det er blevet konstateret, at et tredjeland ikke sikrer et tilstrækkeligt beskyttelsesniveau, forsøge at imødegå denne situation.[88] Kommissionen fastslog i denne henseende aldrig formelt, at USA ikke sikrer et tilstrækkeligt beskyttelsesniveau før vedtagelsen af Safe Harbor-beslutningen.[89]

Artikel 29-gruppen udtalte tidligt, at principperne for at anses som værende tilstrækkelige mindst skal indeholde principperne, der findes i OECD's Privacy Guidelines af 1980[90], og princippernes mangel i denne henseende blev kritiseret af gruppen.[91] Gruppen gik videre i deres kritik af ordningens indhold og påpegede, at principperne blev undermineret af såvel antallet som omfanget af undtagelserne til principperne.[92] Gruppen udtalte, at princippernes overholdelse alene skulle begrænses i det omfang, det er nødvendigt for at efterkomme modstridende forpligtelser.[93]

Artikel 29-gruppen konkluderede videre, at ordningen i praksis ikke garanterede de registrerede en mulighed for at kunne indbringe deres sag for en uafhængig klageinstans[94], hvilket Europa-Parlamentet ligeledes kritiserede.[95] Tilsynet med ordningen var ligeledes mangelfuldt på en række punkter. Det amerikanske handelsministerium blev kritiseret for ikke i tilstrækkelig grad at føre kontrol med, hvorvidt virksomhederne, der certificerede sig som Safe Harbor-virksomhed over for handelsministeriet, havde en offentlig tilgængelig privatlivspolitik, som ordningen krævede. Et væsentligt mindretal af virksomhederne, der fremgik af handelsministeriets liste over Safe Harbor-virksomheder, fandtes ikke at have en offentligt tilgængelig privatlivspolitik.[96] Dette var særligt problematisk, eftersom FTC alene er kompetent til at "gribe ind over for foretagender, der ikke beskytter privatlivets fred med hensyn til personoplysninger til trods for deres erklæringer og/eller forpligtelser i denne henseende"[97], og efter amerikansk retspraksis er manglende afgivelse af en erklæring ikke omfattet af FTC's kompetence.[98]

Implementeringen af ordningen blev ligeledes udsat for kritik. Allerede tre år efter ordningens ibrugtagen fandt Kommissionen ved gennemgang af en række Safe Harbor-virksomheders privat-

---

[86] European Parliament: Report A5-0177/2000, s. 9.
[87] Joel R. Reidenberg: E-Commerce and Trans-Atlantic Privacy, s. 741f. samt Databeskyttelsesdirektivet, artikel 25(2).
[88] Databeskyttelsesdirektivet, artikel 25(4) og (5).
[89] Joel R. Reidenberg: E-Commerce and Trans-Atlantic Privacy, s. 742.
[90] Article 29 Working Party: Opinion 1/99 concerning the level of data protection in the United States, s. 3.
[91] Article 29 Working Party: Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles", s. 5f.
[92] Article 29 Working Party: Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles", s. 4f.
[93] *Ibid.*, s. 5.
[94] Article 29 Working Party: Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles", s. 7.
[95] European Parliament: Report A5-0177/2000, s. 8.
[96] European Commission: Commission Staff Working Document on the implementation of Commission Decision 520/2000/EC, s. 6.
[97] Beslutning 2000/520/EF, bilag III (s. 1).
[98] Daniel R. Leathers: Giving Bite to the EU-U.S. Data Privacy Safe Harbor, s. 221.

livspolitikker, at disse ikke i tilstrækkelig grad implementerede samtlige af ordningens principper, og kun et fåtal af virksomheder havde en privatlivspolitik, der afspejlede alle ordningens principper.[99] En uafhængig undersøgelse fra 2008 konkluderede tilsvarende bl.a., at handelsministeriets liste over Safe Harbor-virksomheder ikke var tidssvarende, at alene cirka en tredjedel af virksomhederne havde en privatlivspolitik, der implementerede Safe Harbor-principperne fuldt ud, at en række virksomheder fejlagtigt tilkendegav deres tilslutning til Safe Harbor-ordningen til trods for ikke faktisk at være certificeret, ligesom et mindretal af selskaber på anden vis gav misvisende oplysninger vedrørende deres tilknytning til Safe Harbor-ordningen.[100]

Kommissionen udsendte i 2013 en meddelelse om, hvordan Safe Harbor-ordningen fungerede.[101] Kommissionen konstaterede heri en række af de samme utilstrækkeligheder ved ordningen, som var blevet dokumenteret af Kommissionens 2004-rapport samt den uafhængige 2008-rapport. Kritikken gik navnlig på virksomhedernes utilstrækkelige efterlevelse af ordningen i praksis, herunder virksomheders manglende offentliggørelse af deres privatlivspolitik samt den mangelfulde implementering af principperne i virksomhedernes privatlivspolitikker.[102] Kommissionen konstaterede hertil, at "de amerikanske myndigheders overvågning af og tilsyn med de certificerede virksomheders overholdelse af Safe Harbor-principperne skal gøres mere effektiv og systematisk, hvis Safe Harbor skal komme til at fungere efter hensigten."[103]

I relation til de amerikanske overvågningsprogrammer, som Snowden havde afsløret eksistensen af tidligere på året, påpegede Kommissionen, at ordningens "undtagelsesbestemmelse vedrørende national sikkerhed kun skal anvendes i strengt nødvendigt og forholdsmæssigt omfang"[104], og at det skal ske på en sådan måde, at beskyttelsen, som ordningen fordrer, ikke udhules.[105] Det bemærkelsesværdige er, at dette som nævnt ovenfor også blev påpeget af Artikel 29-gruppen i 2000.[106] Særligt bemærkede Kommissionen, at ordningens undtagelser vedrørende national sikkerhed, hvorigennem disse omfattende overvågningsprogrammer kunne indsamle overførte oplysninger, muligvis gik "ud over hvad der er strengt nødvendigt og proportionalt i forhold til beskyttelsen af statens sikkerhed."[107] Kommissionen konstaterede endelig, at den beskyttelse, som amerikansk lovgivning sikrer mod statens eventuelle adgang til de registreredes personoplysninger, alene beskytter amerikanske statsborgere.[108]

I kølvandet på afsløringerne om de amerikanske overvågningsprogrammer og Kommissionens udtalelser i 2013 kendte Domstolen i oktober 2015 kommissionsbeslutning 2000/520/EF ugyldig, og Safe Harbor-ordningen kunne følgelig ikke tjene som grundlag for overførsel af personoplysninger til USA. Hvilke omstændigheder, der gik forud for dommen, og dommens præmisser i sag C-362/14 undersøges nærmere nedenfor i kapitel 4.

---

[99] European Commission: Commission Staff Working Document on the implementation of Commission Decision 520/2000/EC, s. 7f.
[100] Chris Connolly: The US Safe Harbor - Fact or Fiction?, s. 4f.
[101] Europa-Kommissionen: COM(2013) 847.
[102] Europa-Kommissionen: COM(2013) 847, s. 6ff.
[103] Europa-Kommissionen: COM(2013) 846, s. 8.
[104] *Ibid.*
[105] Europa-Kommissionen: COM(2013) 847, s. 18.
[106] Article 29 Working Party: Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles", s. 4f.
[107] Europa-Kommissionen: COM(2013) 847, s. 18.
[108] *Ibid.*, s. 19.

# 4. Maximillian Schrems v Data Protection Commissioner

Domstolen afsagde den 6. oktober 2015 dom i Schrems-sagen, hvorved den bl.a. kendte Safe Harbor-beslutningen ugyldig. I afsnit 4.1. gives en kort introduktion til forløbet, der ledte op til Domstolens afgørelse, og hvad der lå til grund for sagen. Det gennemgås efterfølgende på hvilke præmisser, Domstolen kendte Safe Harbor-beslutningen ugyldig, og hvad den konkret og generelt udtalte i denne forbindelse. Dette sker med henblik på at kunne vurdere i afsnit 4.2.4., hvilke umiddelbare konsekvenser dommen har haft, samt hvorvidt dommen har haft indirekte betydning for overførsler til tredjelande og i bekræftende fald hvilken.

## 4.1. Introduktion

Europæiske brugere af Facebook indgår per Facebooks brugerbetingelser en aftale med Facebook Ireland Ltd., hvorefter brugerne ved deres brug af Facebooks tjenester samtykker til, at deres personoplysninger bliver overført til USA, hvor de bliver behandlet.[109]

Maximillian Schrems, en østrigsk ph.d.-studerende og Facebookbruger, indgav i juni 2013 en klage til det irske datatilsyn, Data Protection Commissioner (herefter DPC), vedrørende Facebooks overførsel af personoplysninger til USA.[110] Måneder forinden havde Edward Snowden afsløret, at det amerikanske efterretningsvæsen, navnlig NSA, opererer en række masseovervågningsprogrammer, der overvåger internet- og telekommunikation globalt.[111] En række af disse overvågningsprogrammer gør NSA i stand til at tilgå oplysninger direkte hos større tjenesteudbydere som Google og Facebook.[112]

Ifølge Schrems sikrede USA, henset til Snowdens afsløringer, ikke et tilstrækkeligt beskyttelsesniveau, og DPC skulle som følge heraf beordre Facebook Ireland til at standse deres overførsel af personoplysninger til USA.[113]

DPC anførte i deres svar, at Schrems ikke kunne påvise, at det amerikanske efterretningsvæsen havde tilgået netop hans personoplysninger. Endvidere var Facebook en certificeret Safe Harbor-virksomhed, og eftersom certificerede Safe Harbor-virksomheder efter Kommissionens beslutning 2000/520/EF måtte anses for at sikre et tilstrækkeligt beskyttelsesniveau, anså DPC sig bundet heraf og så sig ikke kompetent til selvstændigt at undersøge tilstrækkelighedsniveauet. DPC afviste på denne baggrund Schrems' klage.[114]

Schrems anfægtede DPC's afvisning og lagde sag an ved den irske High Court. Retten fandt først og fremmest, at Schrems havde retlig interesse i at få sin klage behandlet, idet retten bemærkede, at Snowden-afsløringerne havde vist, at borgernes ret til databeskyttelse var blevet bragt i fare som følge af de omfattende masseovervågningsprogrammer iværksat af det amerikanske efterretningsvæsen.[115] Det var henset hertil underordnet, hvorvidt Schrems' egne personoplysninger faktisk var berørt af overvågningsprogrammerne.[116]

---

[109] Facebook: Statement of Rights and Responsibilities.
[110] Schrems -v- Data Protection Commissioner [2014] IEHC 310, præmis 16 og 18.
[111] *Ibid.*, præmis 1.
[112] *Ibid.*, præmis 11.
[113] *Ibid.*, præmis 2.
[114] *Ibid.*, præmis 30-32.
[115] *Ibid.*, præmis 8.
[116] *Ibid.*, præmis 45.

Retten fandt, at spørgsmålet omkring, hvorvidt DPC var bundet af Kommissionsbeslutning 2000/520/EF om Safe Harbor-ordningen, havde betydning for alle EU's medlemslande.[117] Retten spurgte derfor Domstolen præjudicielt, om en national tilsynsmyndighed, såfremt der foreligger en Kommissionsbeslutning i medfør af artikel 25, er afskåret fra at behandle en klage over tilstrækkeligheden af beskyttelsesniveauet i et tredjeland.[118] Dette fandt Domstolen ikke at være tilfældet.[119] Domstolen undersøgte herefter endvidere gyldigheden af Kommissionsbeslutning 2000/520/EF om Safe Harbor.

## 4.2. Gyldigheden af Kommissionsbeslutning 2000/520/EF

Selv om Schrems i sin klage til DPC ikke formelt anfægtede Safe Harbor-ordningens gyldighed, anførte han, at Snowdens afsløringer viste, at USA ikke sikrede en tilstrækkelig beskyttelse af personoplysninger.[120] Den irske High Court bemærkede hertil, at klagen reelt måtte anses for at angå Safe Harbor-ordningens gyldighed, men anmodede ikke direkte EU-domstolen om en stillingtagen til beslutningens gyldighed.[121] Generaladvokat Bot, der fremsatte forslag til afgørelse i sagen, førte denne stafet videre. Han påpegede, at Schrems og den irske High Court indirekte havde stillet spørgsmålstegn ved gyldigheden af Kommissionsbeslutning 2000/520/EF.[122] Domstolen så sig enige heri og gav sig for at undersøge, "om beslutningen er i overensstemmelse med de krav, der følger af direktivet, sammenholdt med Chartret."[123]

Generaladvokatens og Domstolens er siden blevet beskyldt for at have været på tynd juridisk is i deres begrundelse for at undersøge gyldigheden af Kommissionsbeslutning 2000/520/EF, når et spørgsmål om beslutningens gyldighed ikke formelt blev forelagt Domstolen.[124] Generaladvokat Bot mente ikke desto mindre, under henvisning til Domstolens egen praksis, at Domstolen, når den er forelagt bestemmelser til fortolkning, også er berettiget til at undersøge gyldigheden af disse bestemmelser.[125]

Domstolen fandt først og fremmest, at alene den kan afgøre, hvorvidt en EU-retsakt, som fx en tilstrækkelighedsafgørelse efter artikel 25(6), er gyldig eller ej.[126]

For at undersøge hvorvidt beslutning 2000/520/EF var i overensstemmelse med Databeskyttelsesdirektivet, fandt Domstolen det herefter nødvendigt at præcisere, hvad der kræves af en tilstrækkelighedsafgørelse efter direktivets artikel 25(6), herunder hvordan begrebet 'tilstrækkeligt beskyttelsesniveau' skal forstås.

Domstolen bemærkede, at begrebet 'tilstrækkeligt beskyttelsesniveau' ikke var defineret i Databeskyttelsesdirektivet.[127] Domstolen udledte herefter ud fra en fortolkning af artikel 25(6) med udgangspunkt i Chartret, hvilke krav bestemmelsen stiller til et tilstrækkeligt beskyttelsesniveau.[128] Domstolens fortolkning af direktivets artikel 25(6) er efterfølgende blevet inkorporeret i Databe-

[117] *Ibid.*, præmis 71.
[118] Sag C-362/14 Schrems [2015], præmis 36.
[119] *Ibid.*, præmis 66.
[120] Schrems -v- Data Protection Commissioner [2014] IEHC 310, præmis 29.
[121] *Ibid.*, præmis 69-70.
[122] Forslag til afgørelse fra Generaladvokat Y. Bot i Sag C-362/14 Schrems [2015], afsnit 121-123.
[123] Sag C-362/14 Schrems [2015], præmis 67.
[124] Xavier Tracol: Invalidator Strikes Back, s. 350.
[125] Forslag til afgørelse fra Generaladvokat Y. Bot i Sag C-362/14 Schrems [2015], afsnit 125-126.
[126] Sag C-362/14 Schrems [2015], præmis 61.
[127] *Ibid.*, præmis 70.
[128] Sag C-362/14 Schrems [2015], præmis 71-78.

skyttelsesforordningens artikel 45 samt præambelbetragtningerne hertil, som er nærmere omtalt i afsnit 2.4.1. Det kan kort opsummeres, at Domstolen fandt, at tredjelandets beskyttelsesniveau ikke behøves at være identisk med det, der sikres inden for EU, men skal i det væsentlige svare hertil.[129] Henset til, at Databeskyttelsesforordningens artikel 45 er indgående beskrevet i det nævnte afsnit, behandles Domstolens fortolkning ikke nærmere. Domstolen vurderede herefter, hvorvidt Kommissionsbeslutning 2000/520/EF om Safe Harbor var i overensstemmelse med Databeskyttelsesdirektivets artikel 25(6) og Domstolens fortolkning heraf.

### 4.2.1. Ret til respekt for privatlivet

I relation til Safe Harbor-ordningen hæftede Domstolen sig først og fremmest ved, at ordningen alene tillod amerikanske virksomheder at tilslutte sig ordningen og anvende den som grundlag for at overføre personoplysninger fra EU. Offentlige myndigheder i USA var således på ingen måde forpligtet af ordningen.[130] Ordningen specificerede endvidere, at efterlevelsen af Safe Harbor-principperne kunne begrænses, når det var påkrævet af hensyn til "statens sikkerhed, almenvellet eller opretholdelsen af lov og orden".[131] Det fremgik ligeledes, at certificerede, amerikanske virksomheder, uanset Safe Harbor-principperne, skulle overholde amerikansk lovgivning, såfremt der forekom modstridende forpligtelser. Sammenlagt betød dette, at forpligtelser af den nævnte karakter i modstridende tilfælde fik forrang for Safe Harbor-principperne.[132]

Domstolen konstaterede på ovenstående baggrund, at Safe Harbor-ordningen åbnede for indgreb i unionsborgeres fundamentale rettigheder, idet certificerede, amerikanske virksomheder var nødsaget til lade amerikanske offentlige myndigheder tilgå unionsborgeres personoplysninger, når det var nødvendigt af hensyn til statens sikkerhed eller påkrævet efter amerikansk lovgivning.[133] Under henvisning til *Digital Rights Ireland*[134], fremhævede Domstolen endvidere, at der kan være tale om et indgreb i fundamentale rettigheder, uanset om "indgrebet har medført eventuelle ubehageligheder for de berørte."[135] Domstolen skelede herunder også til Kommissionens udtalelse fra 2013, hvor Kommissionen i deres egen undersøgelse af Safe Harbor-ordningen fandt, at de amerikanske myndigheder kunne tilgå personoplysninger overført under ordningen i et omfang, der var uproportionalt og ikke begrænset til det strengt nødvendige i forhold til hensynet til statens sikkerhed.[136]

Generaladvokat Bot fandt i sit forslag til afgørelse, at det amerikanske efterretningsvæsen ikke havde begrænset deres anvendelse af ovenfor beskrevne undtagelser i Safe Harbor-beslutningen til det strengt nødvendige.[137] Generaladvokaten lagde til grund, at det amerikanske efterretningsvæsen "i forbindelse med vilkårlig masseovervågning" havde adgang til de personoplysninger, der blev overført under Safe Harbor-ordningen.[138] Generaladvokaten lagde også Kommissionens udtalelse fra 2013 til grund, hvori Kommissionen pointerede, at en række af de amerikanske virksomheder, der var certificeret under Safe Harbor-ordningen, ligeledes deltog i et af det amerikanske efterretnings-

[129] *Ibid.*, præmis 73.
[130] *Ibid.*, præmis 82.
[131] Beslutning 2000/520/EF, bilag I, afsnit 4.
[132] Sag C-362/14 Schrems [2015], præmis 86.
[133] *Ibid.*, præmis 87.
[134] De forenede sager C-293/12 og C-594/12 Digital Rights Ireland [2014].
[135] Sag C-362/14 Schrems [2015], præmis 87 samt de forenede sager C-293/12 og C-594/12 Digital Rights Ireland [2014], præmis 33.
[136] Sag C-362/14 Schrems [2015], præmis 90.
[137] Forslag til afgørelse fra Generaladvokat Y. Bot i Sag C-362/14 Schrems [2015], afsnit 164.
[138] *Ibid.*, afsnit 155.

væsens masseovervågningsprogrammer.[139] Generaladvokaten konkluderede på denne baggrund, at "amerikansk lovgivning og praksis [tillod] storstillet indsamling af unionsborgeres personoplysninger", der var blevet overført under Safe Harbor-ordningen.[140]

Generaladvokat Bot vurderede herefter, hvorvidt det amerikanske efterretningsvæsens masseovervågning var forenelig med EU-retten.[141] Først og fremmest er der tale om et indgreb i retten til respekt for privatlivet som er sikret ved Chartrets artikel 7, konstaterede Generaladvokaten, når indsamlede personoplysninger videregives til offentlige myndigheder, "uanset hvordan [oplysningerne] efterfølgende anvendes."[142] Domstolen fandt i Digital Rights Ireland, at enhver behandling af personoplysninger er et indgreb i den grundlæggende ret til beskyttelse af personoplysninger, som er sikret ved Chartrets artikel 8.[143] Der var således tale om et indgreb i beskyttelsen efter Chartrets artikel 8, når det amerikanske efterretningsvæsens behandlede personoplysninger overført under Safe Harbor-ordningen.[144]

I vurderingen af, hvorvidt disse indgreb herefter var forholdsmæssige, karakteriserede Generaladvokat Bot det amerikanske efterretningsvæsens adgang til personoplysningerne overført under Safe Harbor-ordningen, som "[en] adgang, [der] generelt omfatter alle personer og alle elektroniske kommunikationsmidler samt alle overførte oplysninger, herunder indholdet af den pågældende kommunikation, uden nogen form for differentiering, begrænsning eller undtagelse under hensyn til det mål af almen interesse, der forfølges."[145] En sådan overvågning, udtalte Generaladvokaten, er "et uberettiget indgreb i de rettigheder, der sikres ved Chartrets artikel 7 og 8."[146]

Domstolen accentuerede derimod med afsæt i *Digital Rights Ireland* generelt, at unionslovgivning, der hjemler indgreb i de fundamentale rettigheder, som er sikret ved Chartrets artikel 7 og 8, skal "fastsætte klare og præcise regler, som regulerer rækkevidden og anvendelsen" af disse indgreb og indføre beskyttelsesforanstaltninger, der muliggør en effektiv beskyttelse af personoplysningerne mod risikoen for misbrug og mod ulovlig adgang, samt at "undtagelser fra og begrænsninger af [denne beskyttelse skal] holdes inden for det strengt nødvendige."[147]

Med udgangspunkt i ovenstående fandt Domstolen, at:

"En lovgivning, der på generel vis tillader opbevaring af samtlige personoplysninger fra samtlige de personer, hvis oplysninger er blevet videregivet fra Unionen til USA, uden at der bliver foretaget nogen form for differentiering, begrænsning eller undtagelse under hensyn til det forfulgte mål, og uden at der bliver fastsat noget objektivt kriterium, som gør det muligt at afgrænse de offentlige myndigheders adgang til oplysningerne og deres senere anvendelse heraf med henblik på veldefinerede formål, der er strengt begrænsede, og som kan begrunde det indgreb, som såvel adgangen til disse oplysninger som anvendelsen heraf indebærer, er således ikke begrænset til det strengt nødvendige. Navnlig skal en lovgivning, der gør det *muligt for de offentlige myndigheder på generel vis at få adgang til indholdet af elektronisk kommunikation, anses for at udgøre et indgreb i det væsentligste indhold af den grundlæggende ret til respekt for privatlivet*, således som denne er sikret ved Chartrets artikel 7" (egen fremhævning).[148]

---

[139] *Ibid.*, afsnit 157.
[140] *Ibid*., afsnit 158.
[141] *Ibid.*, afsnit 168.
[142] *Ibid.*, afsnit 170.
[143] De forenede sager C-293/12 og C-594/12 Digital Rights Ireland [2014], præmis 36.
[144] Forslag til afgørelse fra Generaladvokat Y. Bot i Sag C-362/14 Schrems [2015], afsnit 170.
[145] Forslag til afgørelse fra Generaladvokat Y. Bot i Sag C-362/14 Schrems [2015], afsnit 198.
[146] *Ibid.*, afsnit 200.
[147] Sag C-362/14 Schrems [2015], præmis 91 og 92. samt de forenede sager C-293/12 og C-594/12 Digital Rights Ireland [2014], præmis 52, 54 og 55.
[148] *Ibid.*, præmis 93 og 94.

Domstolen fandt således, at masseovervågning af elektronisk kommunikation, hvorved offentlige myndigheder tillades generel adgang til indholdet heraf, udgør en krænkelse af retten til respekt for privatlivet som sikret ved Chartrets artikel 7.

Det bemærkes, at Domstolen i modsætning til Generaladvokat Bot af uvisse årsager ikke tog stilling til, hvorvidt en sådan lovgivning tillige udgør en krænkelse af retten til beskyttelse af personoplysninger efter Chartrets artikel 8.[149] Ifølge Kuner er artikel 7 og 8 tæt forbundne, og det forekommer svært at se, hvordan der ved masseovervågning af indholdet af elektronisk kommunikation ikke sker behandling af personoplysninger.[150] Kuner mener, at ovenstående er et udtryk for Domstolens forvirring når det kommer til forskellene mellem disse rettigheder.[151] Andre har anført, at Domstolen herved giver udtryk for, at den ikke anser retten til persondatabeskyttelse efter Chartrets artikel 8 som en særskilt fundamental rettighed.[152]

### 4.2.2. Effektiv domstolsbeskyttelse

Et af kravene, som Domstolen udledte af artikel 25(2), var kravet til effektiv beskyttelse. Domstolen bemærkede, at databeskyttelsesreguleringen i et tredjeland "i praksis [skal] vise sig at være effektiv med henblik på at sikre en beskyttelse, som i det væsentlige svarer til den inden for Unionen sikrede beskyttelse."[153] Domstolen udtalte generelt, at et system baseret på selvcertificering ikke i sig selv var uegnet til at sikre et tilstrækkeligt beskyttelsesniveau som krævet efter artikel 25(6), men systemet skal være ledsaget af effektive kontrol- og håndhævelsesmekanismer, sådan at systemet også i praksis sikrer et tilstrækkeligt beskyttelsesniveau.[154] Generaladvokat Bot pointerede endvidere nødvendigheden af en uafhængig tilsynsmyndighed i "ethvert system, som skal sikre overholdelsen af regler om beskyttelse af personoplysninger."[155] Kravet til effektiv håndhævelse genses i Databeskyttelsesforordningens artikel 45(2)(a) in fine samt artikel 45(2)(b) som elementer, der tillægges vægt ved tilstrækkelighedsvurderingen.

Som nævnt i afsnit 3.3.2. er FTC's kompetence begrænset til "illoyal(e) eller vildledende handlinger eller praksis i forbindelse med handel", og dens muligheder for at gribe ind over for amerikanske virksomheders overtrædelse af Safe Harbor-principperne var begrænsede.[156] FTC kunne således ikke sidestilles med et af de europæiske datatilsyn.[157] Generaladvokat Bot anførte, at de private voldgiftsorganer, som de registrerede alternativt kunne indgive klage til vedrørende virksomhedernes overholdelse af Safe Harbor-principperne, alene havde mulighed for at behandle klager over certificerede virksomheders overholdelse af Safe Harbor-principperne.[158] Generaladvokat Bot hæftede sig således i sit forslag til afgørelse særligt ved den manglende eksistens af en uafhængig tilsynsmyndighed.[159]

Domstolen bemærkede, at det ikke fremgik af Safe Harbor-beslutningen, hvorvidt der eksisterede en effektiv domstolsbeskyttelse mod indgreb i fundamentale rettigheder.[160] Ingen af ordningens

---

[149] Xavier Tracol: Invalidator Strikes Back, s. 355.
[150] Christopher Kuner: Reality and Illusion in EU Data Transfer Regulation Post Schrems, s. 9.
[151] *Ibid.*, s. 10.
[152] Xavier Tracol: Invalidator Strikes Back, s. 355.
[153] Sag C-362/14 Schrems [2015], præmis 74.
[154] *Ibid.*, præmis 81.
[155] Forslag til afgørelse fra Generaladvokat Y. Bot i Sag C-362/14 Schrems [2015], afsnit 145.
[156] Beslutning 2000/520/EF, bilag III, afsnit 2.
[157] Forslag til afgørelse fra Generaladvokat Y. Bot i Sag C-362/14 Schrems [2015], afsnit 205.
[158] *Ibid.*, afsnit 206.
[159] *Ibid.*, afsnit 204-210.
[160] Sag C-362/14 Schrems [2015], præmis 89.

håndhævelsesmekanismer var anvendelige ved amerikanske virksomheders potentielle overtrædelser i forbindelse med deres behandling af personoplysninger, der var blevet overført under Safe Harbor-ordningen.[161] Kommissionens havde i deres føromtalte udtalelse fra 2013 ligeledes konstateret mangler i ordningens håndhævelsesmuligheder vedrørende de registreredes personoplysninger, herunder de registreredes muligheder for at få oplysninger berigtiget eller slettet.[162]

Domstolen udtalte herefter, igen i generelle vendinger, at en unionslovgivning, der ikke giver de registrerede håndhævelsesmuligheder med henblik på at få adgang til deres personoplysninger eller mulighed for at få oplysningerne berigtiget eller slettet, ikke opfylder "det væsentligste indhold af den grundlæggende ret til en effektiv domstolsbeskyttelse, således som denne er sikret ved Chartrets artikel 47."[163]

Domstolen lagde sig op ad således til en vis grad op ad Generaladvokat Bots forslag til afgørelse i denne henseende, men hvor Generaladvokat Bot i sit forslag til afgørelse faktisk sammenholdt Safe Harbor-ordningens håndhævelsesmekanismer med Chartrets artikel 8(3), undlod Domstolen at gøre det samme.[164]

### 4.2.3. Artikel 1 og 3 i beslutning 2000/520/EF

Domstolen fastslog i deres fortolkning af artikel 25(6) i præmis 68-78, at det er et krav efter denne bestemmelse og dermed en forudsætning for en gyldig tilstrækkelighedsafgørelse, at Kommissionen faktisk har fastslået, hvorvidt det pågældende tredjeland sikrer et tilstrækkeligt beskyttelsesniveau.

For en sidebemærkning ses det, at det af den danske udgave af Databeskyttelsesforordningens artikel 45 fremgår, at Kommissionen skal fastslå, at tredjelandet "har et tilstrækkeligt beskyttelsesniveau", mens den engelske ordlyd af samme bestemmelse er "ensures an adequate level of protection". I sagen, der er procederet på engelsk, anvendes udtrykket "ensures", ligesom den danske udgave af dommen benytter ordet "sikrer".[165] Det må på denne baggrund antages, at der ikke ved den danske ordlyd af artikel 45 er tilsigtet en afvigelse fra Domstolens fortolkning af artikel 25, der svarer til forordningens artikel 45.

Ifølge Kommissionsbeslutning 2000/520/EF, artikel 1, formodedes Safe Harbor-principperne at sikre et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overførtes fra EU til amerikanske virksomheder. Efter artikel 2 angik beslutningen kun den beskyttelse, der sikredes gennem Safe Harbor-ordningen, og det fremgik ikke, hvorvidt USA i kraft af landets lov eller internationale forpligtelser sikrer et tilstrækkeligt beskyttelsesniveau.[166] Henset hertil udtalte Domstolen, at Kommissionen således ikke havde konstateret, hvorvidt "USA faktisk 'sikrer' et tilstrækkeligt beskyttelsesniveau på grundlag af landets nationale lovgivning eller dets internationale forpligtelser."[167] Domstolen fandt på denne baggrund, at artikel 1 af Safe Harbor-beslutningen var ugyldig, idet Kommissionen ikke havde opfyldt de krav, der følger af artikel 25(6).[168] Domstolen fandt det følgeligt ikke nødvendigt, at undersøge indholdet af Safe Harbor-principperne.

---

[161] Forslag til afgørelse fra Generaladvokat Y. Bot i Sag C-362/14 Schrems [2015], afsnit 207 samt Sag C-362/14 Schrems [2015], præmis 89.
[162] Sag C-362/14 Schrems [2015], præmis 90.
[163] Sag C-362/14 Schrems [2015], præmis 95.
[164] Xavier Tracol: Invalidator Strikes Back, s. 354.
[165] Sag C-362/14 Schrems [2015], præmis 71.
[166] Beslutning 2000/520/EF, artikel 1 og 2 samt sag C-362/14 Schrems [2015], præmis 79 og 83.
[167] Sag C-362/14 Schrems [2015], præmis 97.
[168] *Ibid.*, præmis 98.

Domstolen vurderede slutteligt, at Safe Harbor-beslutningens artikel 3, der afgjorde, i hvilke tilfælde de nationale tilsynsmyndigheder kunne suspendere overførsler til en certificeret Safe Harbor-virksomhed, udgjorde "en høj interventionstærskel".[169] Domstolen fandt, at Kommissionen herved havde begrænset den kompetence, der tilkommer de nationale tilsynsmyndigheders i medfør af Databeskyttelsesdirektivets artikel 28.[170] Der fandtes ikke i unionslovgivningen hjemmel til, at Kommissionen kunne begrænset tilsynsmyndighedernes kompetence på den pågældende måde, og Domstolen fandt på den baggrund, at Kommissionen havde overskredet deres beføjelser ved at vedtage artikel 3, som derfor var ugyldig.[171]

Eftersom artikel 1 og 3 ikke kunne adskilles fra de øvrige artikler og bilagene til beslutningen i øvrigt, kendte Domstolen hele beslutning 2000/520/EF ugyldig.[172]

Domstolens vurdering af Safe Harbor-beslutningen angik således i høj grad, hvorvidt beslutningen opfyldte de krav, som Domstolen havde udledt af Databeskyttelsesdirektivets artikel 25(6), og hvorvidt Kommissionen ved deres vedtagelse af beslutning 2000/520/EF havde opfyldt disse krav. Modsat Generaladvokat Bot, tog Domstolen således ikke stilling til det amerikanske efterretningsvæsens adgang til personoplysningerne overført under Safe Harbor-ordningen, eller hvorvidt USA faktisk sikrer et tilstrækkeligt beskyttelsesniveau.[173] Som en af sagens dommere efterfølgende udtalte: "We [are] not judging the US system here; we are judging the requirements of EU law in terms of the conditions to transfer data to third countries, whatever they may be."[174] Ikke desto mindre er der en opfattelse af, at Domstolen, særligt ved dens henvisning til Kommissionens udtalelse fra 2013 vedrørende Safe Harbor-ordningens funktion, indirekte fældede dom over det amerikanske efterretningsvæsen og deres masseovervågning.[175]

### 4.2.4. Eftervirkninger

Dommens umiddelbare konsekvens for overførsel af personoplysninger var, at Safe Harbor-ordningen ikke længere kunne danne grundlag for overførsel af personoplysninger fra EU til USA. Eftersom der ikke længere forelå en tilstrækkelighedsafgørelse efter Databeskyttelsesdirektivets artikel 25(6) for virksomheder i USA eller for USA i øvrigt, måtte overførsler herefter ske på baggrund af de særlige overførselsgrundlag efter artikel 26.

Dommens tidsmæssige virkning var dog umiddelbart uklar. Domme, hvorved Domstolen kender unionsregler ugyldige, har som udgangspunkt virkning *ex tunc*.[176] Dette udgangspunkt blev ikke fraveget i Schrems, da der ikke blev anmodet herom, hvilket betød, at Kommissionsbeslutning 2000/520/EF skulle betragtes som aldrig at have eksisteret, og alle overførsler foretaget alene på baggrund af Safe Harbor-ordningen har været ulovlige.[177] Dette blev til en vis grad imødegået af Artikel 29-gruppen, der umiddelbart efter afgørelsen kom med en meddelelse om, at Safe Harbor-ordningen ikke længerere kunne danne grundlag for overførsler til USA, og at overførsler foretaget på grundlag af Safe Harbor-ordningen *efter dommens afsigelse* var ulovlige (egen fremhævning).

---

[169] *Ibid.*, præmis 101.
[170] Sag C-362/14 Schrems [2015], præmis 102.
[171] *Ibid.*, præmis 103 og 104.
[172] *Ibid.*, præmis 105 og 106.
[173] Xavier Tracol: Invalidator Strikes Back, s. 355 samt Christopher Kuner: Reality and Illusion in EU Data Transfer Regulation Post Schrems, s. 13.
[174] Xavier Tracol: Invalidator Strikes Back, s. 355f.
[175] Christopher Kuner: Reality and Illusion in EU Data Transfer Regulation Post Schrems, s. 13.
[176] Sag C-228/92 Roquette Frères [1994], præmis 17.
[177] Xavier Tracol: Invalidator Strikes Back, s. 357.

Artikel 29-gruppen bemærkede i øvrigt, at standardkontraktbestemmelser samt bindende virksomhedsregler fortsat kunne benyttes som overførselsgrundlag.[178]

Udover at kende Safe Harbor-beslutningen ugyldig fastsatte Domstolen ved dens fortolkning af Databeskyttelsesdirektivets artikel 25(6) en række krav, som tredjelande skal opfylde for at blive vurderet af Kommissionen til at sikre et beskyttelsesniveau, der "i det væsentlige svarer til det, der sikres i Unionen".[179] Domstolen satte hermed en høj standard for databeskyttelse.[180]

Domstolen fastslog, at Chartret udgør standarden som et tredjeland skal holdes op imod, når landets beskyttelsesniveau skal fastslås.[181] Domstolen fandt endvidere, at Kommissionens vurdering af et tredjelandes beskyttelsesniveau skal vurderes i lyset af beskyttelsesniveauet i Unionen, og at Kommissionens skal foretage en streng efterprøvelse af de krav, der følger af artikel 25(6) sammenholdt med Chartret.[182] Det skal herunder bemærkes, at efter Databeskyttelsesdirektivet kunne en tilstrækkelighedsafgørelse efter artikel 25 træffes enten af medlemsstaterne eller af Kommissionen.[183] Dette kunne give anledning til forskelligartede vurderinger, eftersom Kommissionens vurdering skulle ske i lyset af beskyttelsesniveauet i Unionen, mens medlemslandenes vurdering skulle ske på baggrund af beskyttelsesniveauet i det pågældende medlemsland. Eftersom en række kernebestemmelser i Databeskyttelsesdirektivet, jf. artikel 13, kunne begrænses af hensyn til statens sikkerhed, og idet national sikkerhed, jf. TEU, artikel 4(2), er det enkelte medlemslands eneansvar, kunne der forekomme variationer i de enkelte landes beskyttelsesniveau, særligt for så vidt angår medlemslandenes praksis vedrørende landenes efterretningstjenesters behandling af personoplysninger.[184] Dette er ikke længere tilfældet efter Databeskyttelsesforordningen, da kompetencen til fastslå tilstrækkeligheden af tredjelandets beskyttelsesniveau alene tilkommer Kommissionen, jf. artikel 45. Tredjelandets beskyttelsesniveau skal således holdes op mod beskyttelsesniveauet, som er sikret i Unionen generelt.

En række af de krav, som Domstolen udledte af artikel 25(6) sammenholdt med Chartret, er som nævnt blevet indskrevet i Databeskyttelsesforordningen. Det er dog ikke alle krav, der er medtaget i forordningen. Det gælder navnlig Domstolens betragtninger under afsnittet "Om artikel 1 i beslutning 2000/520", som er omtalt ovenfor i afsnit 4.2. Kommissionens opfattelse er da også, at dommens rækkevidde er begrænset til Safe Harbor-beslutningen. Kommissionen anerkendte dog, at der også findes bestemmelser svarende til Safe Harbor-beslutningens artikel 3, der begrænsede de nationale tilsynsmyndigheders kompetence, og som Domstolen derfor kendte ugyldig, i de øvrige tilstrækkelighedsafgørelser.[185] Kommissionens forslag til berigtigelse af artikel 3 i samtlige tilstrækkelighedsafgørelser er per november 2016 blevet vedtaget i artikel 31-udvalget.[186]

Det er fra anden side blevet anført, at Domstolen mere generelt udtalte sig om kravene, der følger af artikel 25(6) sammenholdt med Chartret og således ikke alene Safe Harbor-beslutningen, se herom afsnit 4.2.3. *in fine*, ligesom flere af Domstolens betragtninger synes at gælde for tilstrækkeligheds-

[178] Article 29 Working Party: Statement (2015-10-16), s. 1f.
[179] Databeskyttelsesforordningens præambelbetragtning 104.
[180] Christopher Kuner: Reality and Illusion in EU Data Transfer Regulation Post Schrems, s. 10
[181] Sag C-362/14 Schrems [2015], præmis 67 samt mere generelt i præmis 38.
[182] *Ibid.*, præmis 73, 74, og 78 samt 96.
[183] Forslag til afgørelse fra Generaladvokat Y. Bot i Sag C-362/14 Schrems [2015], afsnit 86 samt Sag C-362/14 Schrems [2015], præmis 50.
[184] Sidley: Essentially Equivalent, s. 28. Se afsnit 1.4.1. heri for nærmere herom.
[185] Europa-Kommissionen: COM(2015) 566, s. 16.
[186] Europa-Kommissionen: Dokument S047662/01 (referat) i sagsmappe CMTD(2016)1144 og Dokument S048385/01 (referat) i sagsmappe CMTD(2016)1365.

vurderinger generelt. Denne opfattelse deles af Artikel 29-gruppen, der på baggrund af dommen udsendte et arbejdsdokument om "European Essential Guarantees".[187]

Først og fremmest skal Kommissionen faktisk fastslå, at et tredjeland i kraft af landets nationale lovgivning og internationale forpligtelser sikrer et tilstrækkeligt beskyttelsesniveau, og Kommissionens tilstrækkelighedsvurdering skal indeholde en angivelse af, hvordan landets lovgivning og internationale forpligtelser sikrer dette beskyttelsesniveau.[188]

Derudover skal der være fastsat klare og præcise regler for offentlige myndigheders indgreb i borgernes fundamentale rettigheder, som er sikret ved Chartrets artikel 7 og 8, eksempelvis behandling af personoplysninger af hensyn til national sikkerhed.[189] Indgrebene skal endvidere være nødvendige og proportionale i forhold til det formål, der forfølges, jf. Chartrets, artikel 52(1), hvilket Domstolen også berørte i forhold til Safe Harbor-ordningen.[190] Domstolen fastslog endvidere, at undtagelser, der muliggør indgreb i retten til beskyttelse af personoplysninger, skal være begrænset til det *strengt* nødvendige.[191] Endvidere skal effektive retsmidler være tilgængelige for de registrerede, således de kan håndhæve deres rettigheder.[192]

Foranlediget af Schrems-dommen har Artikel 29-gruppen udsendt et arbejdsdokument, hvori gruppen gennemgår og opsummerer EU-Domstolens og Den Europæiske Menneskerettighedsdomstols praksis vedrørende beskyttelsen af retten til respekt for privatlivet samt retten til beskyttelse af personoplysninger. Gruppen understreger indledningsvist, at der ikke alene er tale om garantier, som kun skal overholdes ved Kommissionens vurdering af beskyttelsesniveauet i et tredjeland, men at garantierne skal overholdes ved alle behandlinger af personoplysninger i Unionen, herunder også ved overførsler til tredjelande.[193] Garantierne har betydning ved vurderingen af national lovgivning, enten medlemsstaternes eller tredjelandes, der tillader indgreb i fundamentale rettigheder vedrørende privatlivs- og databeskyttelse.[194] Garantierne svarer indholdsmæssigt i høj grad til, hvad Domstolen bemærkede i Schrems med tilføjelse af, at der bør eksistere en uafhængig mekanisme, der muliggør et tilsyn med indgreb i retten til privatlivs- og databeskyttelse.[195]

Samlet set må Domstolen med Schrems siges at have sat en høj tærskel, som tredjelandes beskyttelsesniveau skal opnå for at blive vurderet til at være tilstrækkeligt i Kommissionens øjne. Ifølge nogle endda et uopnåeligt højt beskyttelsesniveau, hvor beskyttelsen af fundamentale rettigheder sker på bekostning af hensyn til markedet og samhandelen, som Databeskyttelsesforordningen også har til formål at styrke.[196]

# 5. Post-Schrems: Alternative overførselsgrundlag og EU-U.S. Privacy Shield

Ved Schrems-dommen har Domstolen fjernet et af grundlagene for at overføre personoplysninger til USA, og dommen har ligeledes indirekte haft betydning for afgørelser om tilstrækkeligt beskyt-

[187] Article 29 Working Party: Working Document 01/2016 (European Essential Guarantees).
[188] Sag C-362/14 Schrems [2015], præmis 96 og 83.
[189] *Ibid.*, præmis 91.
[190] *Ibid.*, præmis 90.
[191] *Ibid.*, præmis 92.
[192] *Ibid.*, præmis 95.
[193] Article 29 Working Party: Working Document 01/2016 (European Essential Guarantees), s. 3.
[194] Article 29 Working Party: Working Document 01/2016 (European Essential Guarantees), s. 6.
[195] *Ibid.*, s. 6.
[196] Databeskyttelsesforordningens præambelbetragtning 2 samt Peter Blume: Overførsel af personoplysninger, s. 419 og Orla Lynskey: Negotiating the Data Protection Thicket: Life in the Aftermath of Schrems.

telsesniveau, som drøftet ovenfor. Nedenfor undersøges først, om dommen har en betydning for de alternative overførselsgrundlag, der findes i artikel 46 (direktivets artikel 26), heriblandt standardkontraktsbestemmelser og bindende virksomhedsregler, og i bekræftende fald hvilken. Herefter vurderes den nyligt vedtagne EU-U.S. Privacy Shield-ordning i lyset af Schrems-dommen.

## 5.1. Schrems' betydning for overførsler i medfør af artikel 46-49

Ved Schrems-dommen har Domstolen, ud over at kende Safe Harbor-beslutningen ugyldig, tillige potentielt sået en fundamental tvivl om validiteten af de øvrige mekanismer, der muliggør overførsler af personoplysninger til USA og tredjelande i øvrigt. Svaret på, om dette er tilfældet, afhænger af, i hvilket omfang Domstolens betragtninger vedrørende indgreb i fundamentale rettigheder også kan gøres gældende med hensyn til de alternative overførselsgrundlag der følger af artikel 46-49.

Kommissionen udtalte umiddelbart efter Schrems-dommen, at standardkontraktsbestemmelser samt BVR fortsat kunne benyttes som grundlag for overførsler af personoplysninger til USA, ligesom undtagelserne i Databeskyttelsesdirektivets artikel 26(1) ligeledes kunne anvendes.[197] Artikel 29-gruppen tilsluttede sig delvist hertil, idet de ligeledes pointerede, at standardkontraktsbestemmelser samt BVR stadigt kunne benyttes som overførselsgrundlag.[198]

Efter Kommissionens opfattelse er Databeskyttelsesdirektivets "bestemmelser om international videregivelse af oplysninger, […] baseret på en klar sondring mellem videregivelse til tredjelande, der sikrer et tilstrækkeligt beskyttelsesniveau (direktivets artikel 25), på den ene side og videregivelse til tredjelande, der ikke findes at sikre et tilstrækkeligt beskyttelsesniveau (direktivets artikel 26), på den anden side."[199] Efter Kommissionens opfattelse har Domstolens udtalelser, eftersom de primært omhandler kravene, der følger af artikel 25, således ingen betydning for overførsler, der foretages i medfør af artikel 26.[200]

Domstolen fastslog imidlertid, at Databeskyttelsesdirektivets bestemmelser vedrørende behandling af personoplysninger, der kan krænke de fundamentale frihedsrettigheder, skal fortolkes med udgangspunkt i Chartret.[201] Af Databeskyttelsesforordningen fremgår det, at forordningen "overholder alle de grundlæggende rettigheder og følger de frihedsrettigheder og principper, der anerkendes i chartret.".[202] Det fremgår yderligere af Databeskyttelsesforordningens artikel 44, at bestemmelserne i kapitel V om overførsel af personoplysninger til tredjelande anvendes for at sikre, at beskyttelsesniveauet som sikres ved forordningen ikke undermineres. Domstolen fastslog, at direktivets artikel 25 (forordningens artikel 45) om tilstrækkelighedsafgørelser skal fortolkes med udgangspunkt i Chartret. Når det fremgår af præamblen, at forordningen overholder alle de fundamentale rettigheder, og eftersom artikel 46 findes i samme kapitel som artikel 45 og således tjener samme formål, må det udledes, at artikel 46 også skal fortolkes med udgangspunkt i Chartret.

Kommissionen har i relation til Databeskyttelsesdirektivets artikel 26 (forordningens artikel 46) pointeret, at det er den dataansvarliges "ansvar […] at sikre, at [overførsel] af oplysninger gennemføres med tilstrækkelige garantier", og at "denne vurdering skal foretages på grundlag af *samtlige forhold, der har indflydelse på den pågældende videregivelse*" (egen fremhævning).[203] Skal vurde-

[197] European Commission: First Vice-President Timmermans and Commissioner Jourová's press conference on Safe Harbour following the Court ruling in case C-362/14 (Schrems).
[198] Article 29 Working Party: Statement (2015-10-16), s. 1.
[199] Europa-Kommissionen: COM(2015) 566, s. 5.
[200] *Ibid.*
[201] Sag C-362/14 Schrems [2015], præmis 38.
[202] Databeskyttelsesforordningens præambelbetragtning 4.
[203] Europa-Kommissionen: COM(2015) 566, s. 13f.

ringen foretages på grundlag af samtlige forhold, må bl.a. tredjelandets lovgivning også inddrages i vurderingen.

Selvom Artikel 29-gruppen umiddelbart efter Schrems udtalte, at standardkontraktsbestemmelser fortsat kunne benyttes som overførselsgrundlag, har Artikel 29-gruppen tidligere identificeret et problem ved anvendelsen af kontrakter som grundlag for tredjelandsoverførsler. Gruppen påpegede i et tidligt arbejdsdokument, at dataimportørens forpligtelser efter importlandets lovgivning til at udlevere personoplysninger til offentlige myndigheder i særlige situationer, potentielt har forrang for dataimportørens kontraktslige forpligtelser.[204] Domstolen bemærkede et tilsvarende problem ved Safe Harbor-ordningen, der indeholdt undtagelser, der tillod offentlige myndigheder at tilgå personoplysninger af hensyn til national sikkerhed eller lignende. Det er dog hertil blevet bemærket, at standardkontraktsbestemmelserne, i modsætning til Safe Harbor-ordningen, ikke indeholder sådanne undtagelser.[205] Kuner anfører dog hertil, at en kontrakt mellem to private kontrahenter ikke kan begrænse tredjelandes offentlige myndigheders adgang til personoplysninger.[206]

I denne henseende fremgår endvidere af selve standardkontraktsbestemmelserne, at dataimportøren garanterer, at "han ikke har grund til at tro, at han ifølge den lovgivning, han er underlagt, er forhindret i at følge de instrukser, han har modtaget fra dataeksportøren, og overholde sine forpligtelser i henhold til kontrakten." [207] Dataeksportøren er forpligtet til at instruere dataimportøren til at behandle de modtagne personoplysninger i overensstemmelse med bl.a. den gældende databeskyttelseslovgivning, dvs. Databeskyttelsesforordningen og Chartret.[208]

Såfremt tredjelandets lovgivning, som dataimportøren er underlagt, "gør det muligt for de offentlige myndigheder på generel vis at få adgang til indholdet af elektronisk kommunikation", vil dataimportøren som følge heraf være ude af stand til at overholde sine forpligtelser i henhold til kontrakten, eftersom en sådan lovgivning udgør en krænkelse af "det væsentligste indhold af den grundlæggende ret til respekt for privatlivet" efter Chartrets artikel 7.[209] Det er blevet påpeget, at vedkommende i så fald slet ikke burde være i stand til at indgå en standardkontrakt, der skal tjene som overførselsgrundlag.[210]

Domstolen udtalte ligeledes, at "en lovgivning, der ikke fastsætter nogen mulighed for [den registrerede] til at gøre brug af retsmidler med henblik på at få adgang til personoplysninger, som vedrører den pågældende, eller til at få sådanne oplysninger berigtiget eller slettet, ikke [opfylder] det væsentligste indhold af den grundlæggende ret til en effektiv domstolsbeskyttelse" efter Chartrets artikel 47.[211]

Det er den europæiske tilsynsmyndighed, hvor dataeksportøren er etableret, der med udgangspunkt i europæisk ret, fører tilsyn med standardkontraktsbestemmelsernes overholdelse.[212] Dette er i modsætning til Safe Harbor-ordningen, hvis overholdelse FTC førte tilsyn med. Tilsvarende kræver

---

[204] Article 29 Working Party: Transfers of personal data to third countries, s. 21.
[205] Lokke Moerel: An assessment of the impact of the Schrems judgement on the data transfer grounds available under EU data protection law for data transfers to the U.S., s. 9f.
[206] Christopher Kuner: Reality and Illusion in EU Data Transfer Regulation Post Schrems, s. 26.
[207] Beslutning 2010/87/EU, bilag 1, Standardbestemmelse 5(b).
[208] Beslutning 2010/87/EU, bilag 1, Standardbestemmelse 4(b).
[209] Sag C-362/14 Schrems [2015], præmis 94.
[210] Yann Padova: The Safe Harbour is Invalid: What Tools Remain for Data Transfers and What Comes Next?, s. 152f.
[211] Sag C-362/14 Schrems [2015], præmis 95.
[212] Lokke Moerel: An assessment of the impact of the Schrems judgement on the data transfer grounds available under EU data protection law for data transfers to the U.S., s. 10 samt Beslutning 2010/87/EU, bilag 1, standardbestemmelse 8 og 9.

brug af standardkontraktsbestemmelser i en række medlemsstater godkendelse fra den kompetente tilsynsmyndighed.[213] Dette var tilfældet under Databeskyttelsesdirektivet, men efter Databeskyttelsesforordningens artikel 46(2)(b), kan brug af Kommissionens standardkontraktsbestemmelser ske uden tilsynsmyndighedens godkendelse. Endvidere er tilsynsmyndighedernes kompetence efter artikel 55(1) begrænset til deres eget medlemsstats område, og til trods for, at standardkontraktsbestemmelserne giver myndigheden ret til at foretage en inspektion af dataimportøren[214], kan tilsynsmyndigheden ikke udøve deres kompetence i tredjelande, ligesom de i øvrigt ikke på nogen måde er kompetente over for tredjelandes offentlige myndigheder.[215] Tilsvarende er det blevet pointeret, at de registrerede kan håndhæve rettighederne, som standardkontraktsbestemmelserne tillægger dem ved et tredjemandsløfte, over for dataeksportøren ved en europæisk domstol, ligesom de registrerede har mulighed for at kræve erstatning i tilfælde af kontraktparternes misligholdelse af deres kontaktslige forpligtelser.[216] Der er tvivlsomt, hvorvidt dette opfylder Chartrets artikel 47 om retten til en effektiv domstolsbeskyttelse, eftersom standardkontraktsbestemmelserne som nævnt ikke på nogen måde forpligter eller begrænser tredjelandets offentlige myndigheder. Hvorvidt de registrerede har effektive retsmidler over for tredjelands offentlige myndigheder i tilfælde af myndighedernes indgreb i de registreredes rettigheder, som er sikret ved Chartrets artikel 7 og 8, afhænger derfor af tredjelandets lovgivning, som myndighederne er underlagt.

Ovenfor vurderes med udgangspunkt i standardkontraktsbestemmelserne, hvorvidt Domstolens udtalelser også er gældende for overførsler på andre grundlag end artikel 25 (forordningens artikel 45). Eftersom hele artikel 46 må fortolkes med udgangspunkt i Chartret, er ovenstående betragtninger ikke begrænset til standardkontraktsbestemmelser. Domstolens betragtninger vedrørende lovgivning, der muliggør indgreb i fundamentale rettigheder, som er sikret ved Chartrets artikel 7 og 8, samt adgangen til effektiv domstolsbeskyttelse efter Chartrets artikel 47, må siges at være gældende for samtlige overførselsgrundlag i medfør af artikel 46 (direktivets artikel 26), herunder bl.a. også bindende virksomhedsregler. Dataeksportøren kan ikke give de fornødne garantier, når det kommer til offentlige myndigheder i tredjeland, om hvorvidt lovgivningen, der regulerer myndighederne adgang til personoplysninger, overholder de fundamentale rettigheder, som er sikret ved Chartret.[217] Ovenstående betragtninger også gør sig ligeledes gældende for overførsler, der sker på baggrund af undtagelserne i artikel 49, eftersom disse heller ikke har indflydelse på tredjelandets offentlige myndigheders adgang til at gøre indgreb i de overførte personoplysninger.[218] Artikel 29-gruppen har tilsluttet sig denne opfattelse og udtalt, at beskyttelsen af fundamentale rettigheder er universel og ikke afhængig af grundlaget, der anvendes til at overføre personoplysninger til tredjelande.[219]

Virkeligheden er imidlertid, at de nuværende standardkontraktsbestemmelser er vedtaget ved Kommissionsbeslutninger og kræver dermed, jf. artikel 46(2)(c), ikke tilsynsmyndighedernes godkendelse for at blive anvendt. Eftersom Domstolen er enekompetent til at kende EU-retsakter, så-

---

[213] Lokke Moerel: An assessment of the impact of the Schrems judgement on the data transfer grounds available under EU data protection law for data transfers to the U.S., s. 10.
[214] Beslutning 2010/87/EU, bilag 1, standardbestemmelse 8
[215] Christopher Kuner: Reality and Illusion in EU Data Transfer Regulation Post Schrems, s. 27.
[216] Lokke Moerel: An assessment of the impact of the Schrems judgement on the data transfer grounds available under EU data protection law for data transfers to the U.S., s. 10 samt Beslutning 2010/87/EU, bilag 1, standardbestemmelse 6 og 7.
[217] Se hertil eksempelvis Christopher Kuner, Reality and Illusion in EU Data Transfer Regulation Post Schrems, s. 27f., Yann Padova: The Safe Harbour is Invalid: What Tools Remain for Data Transfers and What Comes Next?, s. 153f. & Xavier Tracol: Invalidator Strikes Back, s. 360.
[218] Christopher Kuner: Reality and Illusion in EU Data Transfer Regulation Post Schrems, s. 25.
[219] Article 29 Working Party: Working Document 01/2016 (European Essential Guarantees), s. 4.

som Kommissionsbeslutninger, ugyldige[220], kan standardkontraktsbestemmelser for nuværende fortsat anvendes som grundlag for tredjelandsoverførsler desuagtet ovenstående betragtninger. Det står den kompetente tilsynsmyndighed frit for at undersøge, hvorvidt en given standardkontrakt opfylder de af Domstolen fastsatte krav, som er omtalt ovenfor. Såfremt tilsynsmyndigheden finder, at standardkontrakten ikke efterlever disse krav, er den dog indskrænket til at indbringe sagen for de nationale domstole, der herefter kan anmode om en præjudiciel afgørelse fra Domstolen.[221]

Netop det ovenstående er tilfældet i en verserende sag, der involverer den irske DPC, Facebook og Schrems. Efter Domstolens afgørelse i sag C-362/14 ophævede den irske High Court DPC's beslutning om ikke at undersøge Schrems' klage og henviste klagen til fornyet behandling ved DPC. I lyset af Safe Harbor-beslutningens ugyldighed, omformulerede Schrems herefter sin klage til at angå Facebooks anvendelse af standardkontraktsbestemmelser som grundlag for at overføre personoplysninger til USA. DPC behandlede Schrems' klage, og i maj 2016 forelå et udkast til en afgørelse, og DPC indbragte samme måned sagen for den irske High Court til en præjudiciel forelæggelse for Domstolen. DPC's foreløbige opfattelse er, at unionsborgere ikke har adgang til effektive retsmidler i USA i overensstemmelse med Chartrets artikel 47, at standardkontraktsbestemmelserne ikke imødekommer denne mangel på adgang til effektive retsmidler, og at standardkontraktsbestemmelserne derfor er i modstrid med Chartrets artikel 47. Hovedforhandlingen i sagen ved den irske High Court er i skrivende stund fastsat til primo februar 2017.[222] Udsigten til at Kommissionsbeslutningerne vedrørende standardkontraktsbestemmelserne muligvis kendes ugyldige er blevet omtalt som "the Armageddon of lawful global data flows"[223], eftersom det potentielt vil cementere opfattelsen af, at ingen af de nuværende overførselsgrundlag opfylder Domstolens krav.[224]

## 5.2. EU-U.S. Privacy Shield

Kommissionen offentliggjorde den 2. februar 2016, at man var nået til enighed om en ny ordning til overførsel af personoplysninger mellem EU og USA og fremlagde den 29. februar 2016 udkastet til ordningen kaldet EU-U.S. Privacy Shield (herefter blot Privacy Shield).[225] Efter udtalelser fra både Artikel 29-gruppen samt Europa-Parlamentet vedtog Kommissionen den 12. juli 2016 den endelige Privacy Shield-beslutning. Amerikanske virksomheder har følgelig siden 1. august 2016 haft mulighed for at tilslutte sig Privacy Shield-ordningen og benytte den som grundlag for at overføre personoplysninger mellem EU og USA.[226]

Privacy Shield-beslutningen er ganske voluminøs og består foruden Kommissionsbeslutningen af syv bilag, herunder selve Privacy Shield-principperne samt en række breve fra amerikanske embedsmænd. Det er ikke hensigten herunder at foretage en tilbundsgående analyse af Kommissionsbeslutningen, der ville være ganske omfangsrig, men derimod nærmere vurdere de væsentligste elementer af beslutningen i lyset af Domstolens udtalelser i Schrems, og hvorvidt den opfylder, de krav Domstolen fastslog følger af artikel 45(3) (direktivets artikel 25(6)) sammenholdt med Chartret.

---

[220] Sag C-362/14 Schrems [2015], præmis 61.
[221] *Ibid.*, præmis 65 samt Europa-Kommissionen: COM(2015) 566, s. 7.
[222] Data Protection Commissioner: Update on Litigation Involving Facebook and Maximillian Schrems.
[223] Jedidiah Bracy: Model clauses in jeopardy with Irish DPA referral to CJEU.
[224] Yann Padova: The Safe Harbour is Invalid: What Tools Remain for Data Transfers and What Comes Next?, s.154. Se hertil i samme retning Christopher Kuner: Reality and Illusion in EU Data Transfer Regulation Post Schrems, s. 29ff.
[225] Kommissionens gennemførelsesafgørelse (EU) 2016/1250.
[226] European Commission: European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows.

### 5.2.1. Privacy Shield-principperne

Ligesom Safe Harbor-ordningen er Privacy Shield en selvcertificeringsordning, hvor amerikanske selvskaber skal tilkendegive deres tilslutning til og efterlevelse af Privacy Shield-principperne over for det amerikanske handelsministerium.[227]

Selve ordningen består af syv Privacy Shield-principper samt 16 supplerende principper. De syv principper er 'oplysningspligt', 'valgfrihed', 'ansvar for videreoverførsel', 'sikkerhed', 'dataintegritet og formålsbegrænsning', 'indsigt' samt 'klageadgang, håndhævelse og ansvar'. Privacy Shield-principperne er mere udførlige, men minder ellers i høj grad om de principper, der fandtes i Safe Harbor-ordningen.[228] Af beslutningens bilag 1 fremgår en række punkter, hvorved Privacy Shield-principperne sikrer en forbedret beskyttelse af personoplysninger i forhold til Safe Harbor-principperne.[229]

Privacy Shield-ordningen er imidlertid forfattet på baggrund af Databeskyttelsesdirektivet, og det store spørgsmål er således, hvorvidt ordningens principper efter Databeskyttelsesforordningens ikrafttræden sikrer et beskyttelsesniveau, som i det væsentlige svarer til det, der sikres i Unionen.[230] Artikel 29-gruppen har i deres analyse af udkastet til Privacy Shield-ordningen pointeret, at ordningen ikke indeholder en række af de nye elementer, som indføres med Databeskyttelsesforordningen. Det drejer sig bl.a. om retten til dataportabilitet, jf. artikel 20 og den dataansvarliges forpligtelser om at efterleve kravene vedrørende databeskyttelse gennem design og gennem standardindstillinger, jf. artikel 25 samt at udføre konsekvensanalyse vedrørende databeskyttelse, jf. artikel 35.[231] Artikel 29-gruppen har ligeledes kritiseret ordningens mangel på en generel indsigelsesadgang.[232] Efter ordningens princip om valgfrihed er de registreredes indsigelsesadgang begrænset til indsigelse mod behandling af personoplysninger i uoverensstemmelse med det oprindelige formål samt mod videregivelse af oplysningerne til tredjemænd.[233] Endeligt indeholder Privacy Shield-ordningen en undtagelse, der *generelt* undtager journalistisk materiale fra Privacy Shield-principperne under henvisning til presse- og ytringsfriheden, som er sikret ved det første forfatningstillæg. Privacy Shield-principperne fortolkes efter amerikansk ret.[234] Denne undtagelse kan således være i uoverensstemmelse med retten til at blive glemt, jf. Databeskyttelsesforordningens artikel 17, da der efter denne bestemmelse med udgangspunkt i Chartret, forordningen og Domstolens praksis skal ske en afvejning mellem hensynet til ytringsfrihed og hensynet til privatlivs- og databeskyttelse.[235]

Henset til ovenstående, forekommer det i lyset af Domstolens krav om, at vurderingen af tredjelandes beskyttelsesniveau skal være streng og ske i lyset af beskyttelsesniveauet i Unionen, tvivlsomt, hvorvidt Privacy Shield-ordningen i dens nuværende form vil bestå efter Databeskyttelsesforordningens ikrafttræden, når en række væsentlige elementer, der indføres med forordningen, ikke

---

[227] Kommissionens gennemførelsesafgørelse (EU) 2016/1250, bilag II, afsnit I, 2.
[228] W. Gregory Voss: The Future of Transatlantic Data Flows, s. 14.
[229] Kommissionens gennemførelsesafgørelse (EU) 2016/1250, bilag 1, s. 1f.
[230] Databeskyttelsesforordningens præambelbetragtning 104.
[231] Article 29 Working Party: Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, s. 15.
[232] *Ibid.*, s. 20.
[233] Kommissionens gennemførelsesafgørelse (EU) 2016/1250, bilag II, afsnit II, 2(a).
[234] *Ibid.*, bilag II, afsnit I, 7.
[235] Article 29 Working Party: Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, s. 25, European Data Protection Supervisor: Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision, s. 10 samt Christopher Kuner: Reality and Illusion in EU Data Transfer Regulation Post Schrems, s. 22.

fremgår af Privacy Shield-ordningen. Artikel 29-gruppen har ligeledes betonet, at den første evaluering[236] af ordningen er afgørende for vurderingen af ordningens fortsatte anvendelighed.[237]

### 5.2.2. Ret til respekt for privatlivet

Det første store spørgsmål i relation til Privacy Shield-ordningen er, i hvilket omfang amerikanske myndigheder kan gøre indgreb i unionsborgeres fundamentale rettigheder, og om der i overensstemmelse med de af Domstolen fastsatte krav findes klare og præcise regler for disse indgreb, der skal være proportionale i forhold til det formål, der forfølges, og begrænset til det strengt nødvendige.

Ved første øjekast er der i denne henseende ingen ændringer sket i forhold til Safe Harbor-principperne. Undtagelserne i Privacy Shield-principperne, hvorefter virksomhedernes efterlevelse af ordningen kan begrænses af hensyn til national sikkerhed eller i tilfælde af modstridende forpligtelser efter amerikansk ret, er næsten identiske med de, der fandtes i Safe Harbor-principperne.[238] Kommissionen påpeger imidlertid hertil, at "USA har indført regler, hvorved det tilsigtes at begrænse de eventuelle indgreb med henblik på retshåndhævelse og andre offentlige interesser i de grundlæggende rettigheder for de personer, hvis oplysninger overføres fra EU til USA under [Privacy Shield], til det strengt nødvendige med henblik på at nå det tilsigtede mål".[239] Hvorvidt Privacy Shield-ordningen er i overensstemmelse med de af Domstolens fastsatte krav beror således på en vurdering af amerikanske retsregler, der tillader eventuelle indgreb.

#### 5.2.2.1. Klare og præcise regler[240]

Det amerikanske efterretningsvæsens indsamling af personoplysninger er hovedsageligt reguleret af to regelsæt, navnlig Foreign Intelligence Surveillance Act (FISA) samt Executive Order 12333. Efter disse regelsæt var beskyttelsen af ikkeamerikanske personers ret til privatliv tidligere nærmest ikkeeksisterende.[241] I januar 2014 udstedte Præsident Obama imidlertid Presidential Policy Directive-28 (PPD-28), der netop fastsætter "bestemte krav til procedurer for indsamling, opbevaring og formidling af personoplysninger om ikkeamerikanske personer indsamlet gennem amerikansk signalefterretning.", og som "finder anvendelse på alle amerikanske signalefterretningsaktiviteter".[242] Artikel 29-gruppen påpeger endvidere, at det overordnede regelsæt for amerikanske signalefterretningsaktiviteter suppleres af en række rapporter, politikker og procedurer.[243]

Artikel 29-gruppen udtalte desangående, at selvom et større antal af disse politikker og procedurer er blevet offentligt tilgængelige siden 2013, er det fortsat svært at fastslå klarheden og præcisionen af disse regler, der regulerer eventuelle indgreb.[244]

Det er hertil blevet anført, at brevene fra Office of the Director of National Intelligence (ODNI) og det amerikanske justitsministerium nærmere redegør for, i hvilket omfang, de ovennævnte regelsæt

---

[236] Kommissionens gennemførelsesafgørelse (EU) 2016/1250, præambelbetragtning 146, hvoraf fremgår, at afgørelsen vil "blive underlagt en årlig fælles evaluering af alle aspekter".
[237] Article 29 Working Party: Statement on the decision of the European Commission on the EU-U.S. Privacy Shield (2016-07-26), s. 1.
[238] Kommissionens gennemførelsesafgørelse (EU) 2016/1250, bilag II, afsnit I, 5.
[239] Kommissionens gennemførelsesafgørelse (EU) 2016/1250, præambelbetragtning 135.
[240] Sag C-362/14 Schrems [2015], præmis 91.
[241] Daniel Severson: American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change, s. 16.
[242] Kommissionens gennemførelsesafgørelse (EU) 2016/1250, bilag VI, afsnit I, a.
[243] Article 29 Working Party: Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, s. 35.
[244] *Ibid.*, s. 37.

tillader eventuelle indgreb.[245] Det ses i denne forbindelse direkte i en række præambelbetragtninger under præamblens afsnit 3.1.1., at Kommissionen læner sig op ad de 'udredninger', som den amerikanske regering har udarbejdet.[246] Kuner konstaterer imidlertid, at der er tale om en række garantier, der fremgår af breve fra en række embedsmænd, og brevene kan ensidigt ændres eller trækkes tilbage.[247] Det er endvidere højst usikkert, hvorvidt garantier givet i sådanne breve opfylder kravet i Chartrets artikel 52(1), hvorefter "begrænsninger af de rettigheder og friheder, der anerkendes ved [Chartret], skal være fastlagt *[ved lov]*" (egen fremhævning).[248]

Domstolen udtalte ligeledes specifikt, at Kommissionen ved en tilstrækkelighedsafgørelse "behørigt [skal konstatere], at det pågældende tredjeland på grundlag af *dets nationale lovgivning og dets internationale forpligtelser* faktisk sikrer et beskyttelsesniveau for de grundlæggende rettigheder, som i det væsentlige svarer til det niveau, der er sikret i Unionens retsorden" (egen fremhævning). Tracol fremhæver hertil, at Kommissionen ved at bero på en række breve og udredninger fra den amerikanske regering ikke har opfyldt ovenstående krav, der følger af artikel 25(6) sammenholdt med Chartret.[249] Det fremgår af Privacy Shield-beslutningens artikel 1(1), at USA sikrer "et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra EU til foretagender i USA under [Privacy Shield-ordningen]", ligesom det af præambelbetragtning 137 fremgår, at Kommissionen finder, at Privacy Shield-principperne "i deres helhed sikrer et niveau af beskyttelse af personoplysninger, der i det væsentlige svarer til det niveau", der sikres ved Databeskyttelsesdirektivet. Tracol anfører på denne baggrund, at Privacy Shield-beslutningen lider af samme formelle mangel, der førte til, at Domstolen kendte Safe Harbor-beslutningen ugyldig.[250]

#### 5.2.2.2. Proportionale i forhold til det formål, der forfølges, og begrænset til det strengt nødvendige[251]

Derudover er det fortsat usikkert, hvorvidt offentlige myndigheder er afskåret fra på generel vis at tilgå indholdet af elektronisk kommunikation. En sådan adgang, anså Domstolen som bekendt for at udgøre et indgreb i det væsentligste indhold af den grundlæggende ret til respekt for privatlivet, som er sikret ved Chartrets artikel 7.[252]

Artikel 29-gruppen konkluderede i deres vurdering, at selv efter udstedelsen af PPD-28 og implementeringen af de heriliggende begrænsninger på indsamlingen af signalefterretninger, at der stadigt er tegn på, at masseindsamling finder sted.[253] Dette bl.a. henset til, at det af PPD-28 fremgår, at masseindsamlede signalefterretninger kun må anvendes til seks afgrænsede formål, hvilket indikerer, at masseindsamling finder sted.[254]

PPD-28 opstiller dog samtidigt krav om, at indsamlingen skal være "så målrettet som muligt", hvilket kunne tyde på, at der ikke var tale om generel masseindsamling, der strider imod Chartret. Dette

---

[245] Hogan Lovells: Privacy Shield Analysis, s. 46.
[246] Se eksempelvis Kommissionens gennemførelsesafgørelse (EU) 2016/1250, præambelbetragtning 70, 71, 73, 74 og 75.
[247] Christopher Kuner: Reality and Illusion in EU Data Transfer Regulation Post Schrems, s. 22.
[248] *Ibid.*, samt Yann Padova: The Safe Harbour is Invalid: What Tools Remain for Data Transfers and What Comes Next?, s. 160.
[249] Xavier Tracol: EU-U.S. Privacy Shield: The Saga Continues, s. 776.
[250] *Ibid.*, s. 777.
[251] Chartrets artikel 52(1) samt sag C-362/14 Schrems [2015], præmis 92.
[252] Sag C-362/14 Schrems [2015], præmis 94.
[253] Article 29 Working Party: Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, s. 40.
[254] Christopher Kuner: Reality and Illusion in EU Data Transfer Regulation Post Schrems, s. 21 samt Yann Padova: The Safe Harbour is Invalid: What Tools Remain for Data Transfers and What Comes Next?, s. 159.

krav er imidlertid åbent for fortolkning, idet en indsamling kan være målrettet uden at være begrænset til det strengt nødvendige.[255] Det er i øvrigt bemærkelsesværdigt, at PPD-28, der gælder indsamling af personoplysninger vedrørende både amerikanske og ikkeamerikanske personer, alene kræver, at indsamlingen er "så målrettet som muligt", mens Executive Order 12333 for så vidt angår amerikanske personer kræver, at indsamlingen skal ske på den "mindst indtrængende" måde, hvilket tyder på forskellige standarder af beskyttelse.[256]

### 5.2.3. Effektiv domstolsbeskyttelse

Det andet spørgsmål *post-Schrems* vedrørende Privacy Shield-ordningen er, hvorvidt de registrerede, jf. Chartrets artikel 47(1), har adgang til effektive retsmidler for en domstol, såfremt deres fundamentale rettigheder er blevet krænket.[257]

Selve ordningen administreres af det amerikanske handelsministerium, og ministeriet har tilkendegivet, at den vil styrke forvaltningen og tilsynet med Privacy Shield-ordningen i forhold til ministeriets tilsyn med Safe Harbor-ordningen. Det fremgår nærmere af bilag I, bilag 1, hvilke forpligtelser ministeriet har påtaget sig i denne henseende.[258]

Virksomheder underlagt FTC's eller det amerikanske transportministeriums kompetence kan tilslutte sig ordningen, ligesom der er åbnet for, at virksomheder underlagt "andre lovbestemte organer, der kan sikre overholdelse af principperne" også kan tilslutte sig ordningen.[259] Privacy Shield minder i denne henseende på mange måder om Safe Harbor.

Klageadgangen for de registrerede er under Privacy Shield-ordningen todelt, og der eksisterer forskellige retsmidler afhængigt af, om klagen angår en certificeret virksomheds overtrædelse af Privacy Shield-principperne, eller klagen angår offentlige myndigheders eventuelle indgreb.

I tilfælde af en virksomheds manglende overholdelse af Privacy Shield-principperne kan de registrerede under Privacy Shield-ordningen enten klage direkte til den certificerede virksomhed, der herefter har 45 dage til at behandle klagen, eller de registrerede kan benytte sig af et alternativt tvistløsningsorgan, som er udpeget af virksomheden til at håndtere klager. Endvidere kan de registrerede klage til deres nationale tilsynsmyndighed eller indbringe klagen direkte for FTC.[260] Den nationale tilsynsmyndigheds kompetence til at behandle klagen beror imidlertid på, hvorvidt den certificerede virksomhed "frivilligt har underlagt sig databeskyttelsesmyndighedens tilsyn", ellers kan tilsynsmyndigheden alene henvise klagen til handelsministeriet eller FTC.[261] Artikel 29-gruppen har kritiseret denne håndhævelsesmekanisme, eftersom FTC ikke er forpligtet til at behandle en indgiven klage, uanset om den er henvist fra en europæisk tilsynsmyndighed eller indgivet direkte til FTC.[262] Slutteligt kan de registrerede i sidste ende indbringe sagen for Privacy Shield panelet, som er en bindende voldgift. Voldgiftsmodellen er nærmere beskrevet i et bilag til Privacy Shield-beslutningen.[263]

---

[255] Article 29 Working Party: Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, s. 40.
[256] Daniel Severson: American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change, s. 482.
[257] Sag C-362/14 Schrems [2015], præmis 95.
[258] Kommissionens gennemførelsesafgørelse (EU) 2016/1250, bilag I, bilag 1.
[259] *Ibid.*, bilag II, afsnit I, 2.
[260] *Ibid.*, præambelbetragtning 41, 44 og 45.
[261] *Ibid.*, præambelbetragtning 48 og 51.
[262] Article 29 Working Party: Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, s. 27.
[263] Kommissionens gennemførelsesafgørelse (EU) 2016/1250, præambelbetragtning 56 samt bilag I, bilag 2.

Under Privacy Shield-ordningen eksisterer der således en række håndhævelsesmuligheder ved certificerede virksomheders manglende efterlevelse af Privacy Shield-principperne. Der kan på mange måder siges at være tale om en udbygning Safe Harbor-ordningens håndhævelsesmekanisme, eftersom mekanismen stadigt udgøres af en række forskelligartede klageadgange.

Der er ligeledes stillet overordnet spørgsmålstegn ved, hvorvidt dette samlede system opfylder kravet i Chartrets artikel 47(1) om effektiv domstolsbeskyttelse. Der er tale om et kompliceret og uigennemsigtigt system, og det er således usikkert om de registrerede i praksis har adgang til effektive retsmidler i tilfælde af manglende efterlevelse af Privacy Shield-principperne.[264] Kuner pointerer ligeledes, at det er usikkert, hvorvidt Domstolen vil anse en samlet håndhævelsesmekanisme, der ikke inkluderer muligheden for at få prøvet sin sag ved en domstol, for at være i overensstemmelse med Chartrets artikel 47(1).[265]

I hvilket omfang de registrerede sikres en effektiv domstolsbeskyttelse ved offentlige myndigheders eventuelle indgreb afhænger af amerikansk ret, eftersom Privacy Shield-ordningen ikke er bindende for offentlige myndigheder. Som beskrevet i afsnit 3.3.1. er privatlivsbeskyttelsen i den offentlige sektor i USA bl.a. sikret gennem forfatningen, herunder særligt fjerde forfatningstillæg, samt Privacy Act. Beskyttelsen, der sikres ved det fjerde forfatningstillæg, omfatter dog ikke unionsborgere[266], ligesom Privacy Act alene beskytter amerikanske statsborgere.

I relation til beskyttelsen, der er sikret ved fjedre forfatningstillæg, betoner Kommissionen, at de registrerede herigennem ydes en indirekte beskyttelse, da de amerikanske virksomheder, som har fået overført personoplysninger fra EU, er omfattet af denne beskyttelse.[267] Det er dog tvivlsomt, hvorvidt dette er tilstrækkeligt i relation til kravet om effektiv domstolsbeskyttelse. Beskyttelsen tilkommer virksomheden, og det er virksomheden, ikke de registrerede, der følgelig har adgang til effektive retsmidler ved et eventuelt indgreb.[268]

Privacy Act's begrænsning til alene at gælde for amerikanske statsborgere er ligeledes forsøgt imødegået med vedtagelsen af Judicial Redress Act i februar 2016, der udvidede beskyttelsen sikret ved Privacy Act til også at omfatte unionsborgere.[269] Vedtagelsen af Judicial Redress Act er dog ledsaget af to væsentlige mangler; Privacy Act indeholder for det første en undtagelse, der gør det muligt at undtage fortrolige oplysninger fra at være omfattet af loven.[270] For det andet finder Judicial Redress Act alene anvendelse på udvalgte offentlige myndigheder, hvilket formentlig ikke inkluderer efterretningsvæsenet.[271] Artikel 29-gruppen har på den baggrund vurderet, at de registrerede med vedtagelsen af Judicial Redress Act ikke er sikret en adgang til effektive retsmidler ved indgreb foretaget af efterretningsvæsenet.[272]

Slutteligt oprettes der i forbindelse med Privacy Shield-ordningen en 'Privacy Shield Ombudsmand', der har til formål at behandle klager, der relaterer sig til amerikansk signalefterretningsprak-

[264] Article 29 Working Party: Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, s. 26.
[265] Christopher Kuner: Reality and Illusion in EU Data Transfer Regulation Post Schrems, s. 23.
[266] Article 29 Working Party: Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, s. 43.
[267] Kommissionens gennemførelsesafgørelse (EU) 2016/1250, præambelbetragtning 127.
[268] Article 29 Working Party: Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, s. 55.
[269] Yann Padova: The Safe Harbour is Invalid: What Tools Remain for Data Transfers and What Comes Next?, s. 160 samt note 141.
[270] David Bender: Will the CJEU do better with privacy shield? A US perspective, s. 129.
[271] David Bender: Will the CJEU do better with privacy shield? A US perspective, s. 130 samt Yann Padova: The Safe Harbour is Invalid: What Tools Remain for Data Transfers and What Comes Next?, s. 160
[272] Article 29 Working Party: Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, s. 43.

sis.[273] Opgaven som ombudsmand varetages af en embedsmand, der udpeges af og referer til den amerikanske udenrigsminister og er uafhængig af efterretningstjenesterne.[274] Selve ombudsmandsmekanismen, herunder fremgangsmåden for indgivelse af klager og behandling af disse, er nærmere beskrevet i bilag III, bilag A.

Ombudsmandsmekanismen kan imidlertid siges at rejse flere spørgsmål, end den besvarer. Artikel 29-gruppen fremhæver bl.a. i deres vurdering, at det er uklart hvilke klager ombudsmanden kan behandle. Det fremgår af bilag A, at ombudsmanden behandler klager vedrørende offentlige myndigheders "adgang til oplysninger overført fra EU til USA til nationale sikkerhedsformål", uanset om disse oplysninger er overført i medfør af Privacy Shield-ordningen eller et af de alternative overførselsgrundlag.[275] Gruppen hæfter sig imidlertid ved, at det af bilag III fremgår, at ombudsmanden alene behandler klager vedrørende *amerikansk signalefterretningspraksis*. Dette medfører uklarhed i relation til hvilke klager, ombudsmanden kan behandle. Det er dels uklart, hvilke oplysninger, der kan betragtes som indsamlet gennem signalefterretning, ligesom det er uklart hvilke myndigheders adgang til personoplysninger, der er omfattet af ombudsmandsmekanismen, idet den alene omfatter klager over efterretningstjenesters eventuelle indgreb, og således ikke tillige klager over retshåndhævende myndigheders eventuelle indgreb.[276]

Der er også blevet stillet spørgsmålstegn ved ombudsmandens uafhængighed, eftersom ombudsmandsopgaven varetages af en embedsmand fra den amerikanske regering, som kan afskediges på linje med andre embedsmænd.[277] Det fremgår, at ombudsmanden er uafhængig af efterretningstjenesterne. Det er dog under henvisning til Domstolens praksis blevet fremhævet, at en tilsynsmyndighed ikke alene skal være uafhængig af de myndigheder, der føres tilsyn med, men fuldt uafhængig.[278] Den Europæiske Ombudsmand har ligeledes stillet spørgsmålstegn ved, om denne Privacy Shield Ombudsmand opfylder de internationale standarder for ombudsmænd.[279]

Artikel 29-gruppens analyse af ombudsmanden uafhængighed er nærmere baseret på, hvilke beføjelser ombudsmanden er tillagt.[280] Gruppen bemærker hertil, at det er uklart, hvorvidt og i hvilket omfang ombudsmanden har adgang til at foretage sin egen undersøgelse i klagesagerne, eller om ombudsmandens undersøgelse er baseret på skriftlige erklæringer fra de omhandlede offentlige myndigheder.[281] Det er ligeledes uklart, hvilke beføjelser, om nogen, ombudsmanden har for at afhjælpe myndighedernes manglende overholdelse af reglerne.[282]

Artikel 29-gruppen når ikke decideret til en konklusion omkring, hvorvidt ombudsmandsmekanismen og de øvrige tilgængelige retsmidler opfylder Chartrets artikel 47 om adgang til effektive retsmidler, men udtrykker dog store betænkeligheder ved Privacy Shield-ordningen i denne henseende.[283]

---

[273] Kommissionens gennemførelsesafgørelse (EU) 2016/1250, bilag III.
[274] *Ibid.* samt *ibid.*, bilag III, bilag A.
[275] Kommissionens gennemførelsesafgørelse (EU) 2016/1250, bilag III, bilag A, s. 1.
[276] Article 29 Working Party: Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, s. 48.
[277] *Ibid.*, s. 49.
[278] Christopher Kuner: Reality and Illusion in EU Data Transfer Regulation Post Schrems, s. 22.
[279] European Ombudsman: Use of the title 'ombudsman' in the 'EU-US Privacy Shield' agreement.
[280] Article 29 Working Party: Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, s. 49f.
[281] *Ibid.*, s. 50.
[282] *Ibid.*
[283] *Ibid.*, s. 51.

### 5.2.4. Et levedygtigt alternativ?

Privacy Shield-ordningen kan dens mangler til trods benyttes som grundlag for overførsel af personoplysninger til USA. Eftersom det alene er Domstolen der kan kende en Kommissionsbeslutning ugyldig, vil ordningen kunne benyttes i al fald i den nærmeste fremtid. Spørgsmålet er dog, hvor længe ordningen vil bestå. Lige siden det første udkast til ordningen blev fremlagt af Kommissionen, er den blevet kritiseret for ikke at opfylde kravene fastslået af Domstolen i Schrems.[284] To organisationer har allerede per december 2016 på denne baggrund anlagt annullationssøgsmål ved Domstolen.[285] Skulle Privacy Shield-beslutningen overleve disse søgsmål, står herefter stadigt tilbage at se, hvordan ordningen klarer sig ved dens første evaluering, og ligeledes hvorvidt ordningen stadig opfylder kravene i artikel 45(3) sammenholdt med Chartret, når Databeskyttelsesforordningen træder i kraft i maj 2018.

# 6. Konklusion

Personoplysninger kan under Databeskyttelsesforordningen overføres på tværs af landegrænser. Såfremt overførslen sker inden for EU, gælder ingen specifikke krav til overførslen, ud over at behandlingen af personoplysningerne skal være i overensstemmelse med Databeskyttelsesforordningen. Ønskes personoplysningerne overført til et tredjeland, skal reglerne i forordningen kapitel V tillige opfyldes.

Der findes en række forskellige overførselsgrundlag i Databeskyttelsesforordningens kapitel V. Det kan dels være på baggrund af en Kommissionsbeslutning, hvorved Kommissionen har fastslået, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau. Foreligger der ikke en sådan beslutning, kan dataeksportøren selv give fornødne garantier, om at forordningens beskyttelsesniveau opretholdes, og dermed sikre de registrerede. Endeligt eksisterer særlige situationer, hvor overførsler undtagelsesvist kan ske til trods for manglen på en tilstrækkelighedsafgørelse eller de fornødne garantier.

Tidligere fandtes en særlig ordning, der kunne anvendes som grundlag for overførsler til USA. Efter denne Safe Harbor-ordning kunne personoplysninger frit overføres fra EU til udvalgte virksomheder i USA, som havde selvcertificeret sig under ordningen. Ordningen blev dog tidligt kritiseret for ikke at frembyde en tilstrækkelig beskyttelse af personoplysninger, der blev overført under ordningen. Efter Snowdens afsløringer i 2013 omkring det amerikanske efterretningsvæsens masseovervågning tog kritikken af Safe Harbor-ordningen til i styrke, da den facilitere en del af denne overvågning for så vidt angår unionsborgeres personoplysninger overført under ordningen.

Domstolen erklærede i Schrems-dommen i oktober 2015 Safe Harbor-beslutningen for ugyldig. I deres afgørelse fandt Domstolen først og fremmest, at Databeskyttelsesdirektivets artikel 25(6) sammenholdt med Chartret kræver, at Kommissionen ved en tilstrækkelighedsafgørelse skal konstatere, at det pågældende tredjeland på grundlag af dets nationale lovgivning eller dets internationale forpligtelser faktisk sikrer et beskyttelsesniveau, som i det væsentlige svarer til det niveau, der er sikret i Unionen.

Vedrørende selve Safe Harbor-ordningen gentog Domstolen en række af de kritikpunkter, der tidligere var blevet påpeget omkring ordningen og dens funktion og hæftede sig herunder ved, at Kommissionen i deres egen evaluering af ordningen havde fundet, at ordningen tillod amerikanske myn-

[284] W. Gregory Voss: The Future of Transatlantic Data Flows, s. 16.
[285] Julia Floretti et al.: Privacy group launches legal challenge against EU-U.S. data pact samt Julia Floretti: EU-U.S. personal data pact faces second legal challenge from privacy groups.

digheder at tilgå personoplysninger overført under ordningen i et uproportionalt omfang, der ikke var begrænset til det strengt nødvendige i forhold til hensynet til statens sikkerhed.

Domstolen fastslog endeligt i generelle vendinger under hvilke omstændigheder, der kan gøres indgreb i unionsborgeres fundamentale rettigheder, som disse er sikret ved Chartret.

Slutteligt fandt Domstolen, at Kommissionen i beslutningens artikel 1 ikke havde opfyldt de krav, som følger af artikel 25(6) sammenholdt med Chartret, og at Kommissionen i beslutningens artikel 3 uden hjemmel hertil havde begrænset de nationale tilsynsmyndigheders kompetence. Hele beslutningen var derfor ugyldig.

Domstolens afgørelse i Schrems har ikke alene haft betydning for Safe Harbor-ordningen, men tillige for de øvrige muligheder for at foretage tredjelandsoverførsler. Efter en vurdering af disse overførselsgrundlag i lyset af Schrems, er det usikkert, om nogle af de overførselsmuligheder, der findes i Databeskyttelsesforordningen på nuværende tidspunkt er anvendelige til tredjelandsoverførsler, hvor tredjelandets lovgivning tillader indgreb at gøre indgreb i de overførte personoplysninger i strid med de krav, som Domstolen fastslog i Schrems. Standardkontraktsbestemmelserne er i denne forbindelse særlige, eftersom de er vedtaget ved en Kommissionsbeslutning. De kan derfor fortsat benyttes, indtil Domstolen eventuelt kender beslutningerne ugyldige. Det forventes at Domstolen i løbet af 2017 får lejlighed til at udtale sig om standardkontraktsbestemmelserne, idet der verserer en sag herom.

Endeligt har Kommissionen til erstatning for Safe Harbor-ordningen vedtaget en ny Kommissionsbeslutning vedrørende Privacy Shield-ordningen. Der er imidlertid tale om samme type selvcertificeringsordning som Safe Harbor-ordningen. Privacy Shield-ordningen har siden dens introduktion mødt stor modstand og kritik, der går på, at ordningen ikke opfylder de krav, som Domstolen fastslog i Schrems. Privacy Shield-ordningen kan for nuværende benyttes som grundlag for at foretage overførsler til certificerede virksomheder i USA. Hvor længe, dette er tilfældet, er uvist, da Kommissionsbeslutningen vedrørende Privacy Shield allerede er blevet anfægtet ved Domstolen.

# 7. Litteraturfortegnelse

## 7.1. Lovgivning

Den Europæiske Unions Charter om grundlæggende rettigheder (2012/C 326/02). (Citeret: Chartret).

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).

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).

Europa-Parlamentets og Rådets Forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser.

Konsolideret udgave af Traktaten om Den Europæiske Unions Funktionsmåde. (2012/C 326/01).

Kommissionsbeslutninger

Kommissionens afgørelse af 5. februar 2010 om standardkontraktbestemmelser for videregivelse af personoplysninger til registerførere etableret i tredjelande i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF (2010/87/EU).

Kommissionens beslutning af 15. juni 2001 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til direktiv 95/46/EF (2001/497/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 harbor-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium (2000/520/EF).

Kommissionens beslutning af 27. december 2004 om ændring af beslutning 2001/497/EF for at indføre en alternativ standardkontrakt om overførsel af personoplysninger til tredjelande (2004/915/EF).

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.

## 7.2. Afgørelser

EU-Domstolen:

De forenede sager C-293/12 og C-594/12 Digital Rights Ireland [2014].

Sag C-101/01 Lindqvist [2003].

Sag C-228/92 Roquette Frères [1994].

Sag C-34/73 Variola [1973].

Sag C-362/14 Schrems [2015]

Sag C-362/14 Schrems [2015], Forslag til afgørelse fra Generaladvokat Y. Bot.

High Court of Ireland:

Schrems -v- Data Protection Commissioner [2014] IEHC 310.

## 7.3. Artikel 29-gruppen

Article 29 Data Protection Working Party, 1998. *Working document on Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive.* WP 12. (Citeret: Article 29 Working Party: Transfers of personal data to third countries).

Article 29 Data Protection Working Party, 1999. *Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government.* WP 15.

Article 29 Data Protection Working Party, 2000. *Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles"*. WP 32.

Article 29 Data Protection Working Party, 2005. *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995.* WP 114. (Citeret: Article 29 Working Party: Working document: Article 26(1)).

Article 29 Data Protection Working Party, 2010. *Opinion 8/2010 on applicable law.* WP 179.

Article 29 Data Protection Working Party, 2016. *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision.* WP 238.

Article 29 Data Protection Working Party, 2016. *Statement of the Article 29 Working Party.* (2015-10-16). (Citeret: Article 29 Working Party: Statement (2015-10-16)).

Article 29 Data Protection Working Party, 2016. *Statement on the decision of the European Commission on the EU-U.S. Privacy Shield.* (2016-07-26).

Article 29 Data Protection Working Party, 2016. *Working Document 01/2016 on the justification of interference with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).* WP 237. (Citeret: Article 29 Working Party: Working Document 01/2016 (European Essential Guarantees)).

## 7.4. Kommissionens dokumenter

Europa-Kommissionen, 2013. *Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om, hvordan safe harbor-ordningen fungerer for så vidt angår EU-borgerne og virksomhederne i EU (COM(2013) 847).* [PDF] Tilgængelig: <http://ec.europa.eu/transparency/regdoc/rep/1/2013/DA/1-2013-847-DA-F1-1.Pdf> [Besøgt: 30/10/2016] (Citeret: Europa-Kommissionen: COM(2013) 847).

Europa-Kommissionen, 2013. *Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet: Genopbygning af tilliden til datastrømmene mellem EU og USA (COM(2013) 846).* [PDF] Tilgængelig: <http://ec.europa.eu/transparency/regdoc/rep/1/2013/DA/1-2013-846-DA-F1-1.Pdf> [Besøgt: 30/10/2016] (Citeret: Europa-Kommissionen: COM(2013) 846).

Europa-Kommissionen, 2015. *Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om videregivelse af personoplysninger fra EU til USA i henhold til direktiv 95/46/EF efter Domstolens dom i sag C-362/14 (Schrems) (COM(2015) 566).* [PDF] Tilgængelig: <http://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52015DC0566&from=DA> [Besøgt: 29/12/2016]. (Citeret: Europa-Kommissionen: COM(2015) 566).

European Commission, 2004. *Commission Staff Working Document on the implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce.* [PDF] Tilgængelig: <http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf> [Besøgt: 30/10/2016] (Citeret: European Commission: Commission Staff Working Document on the implementation of Commission Decision 520/2000/EC).

European Commission, 2016. *Summary record of the 72nd meeting of the Committee on the Protection of Individuals with regard to the Processing of Personal Data (Article 31 Committee)* [DOC] Tilgængelig: <http://ec.europa.eu/transparency/regcomitology/index.cfm?do=Search.getPDF&ds_id=47662&version=1&AttLang=en&db_number=1&docType=SUMMARY_RECORD> [Besøgt: 29/12/2016].

European Commission, 2016. *Summary record of the 73rd meeting of the Committee on the Protection of Individuals with regard to the Processing of Personal Data (Article 31 Committee)* [DOC] Tilgængelig: <http://ec.europa.eu/transparency/regcomitology/index.cfm?do=Search.getPDF&ds_id=48385&version=1&AttLang=en&db_number=1&docType=SUMMARY_RECORD> [Besøgt: 29/12/2016].

## 7.5. Bøger

Blume, P., 2006. *Retlig regulering af internationale persondataoverførsler*. København: Jurist- og Økonomforbundets Forlag.

Blume, P., 2013. *Databeskyttelsesret.* 4. udgave. København: Jurist- og Økonomforbundets Forlag.

Blume, P., 2016. *Retssystemet og juridisk metode.* 3. udgave. København: Jurist- og Økonomforbundets Forlag.

Kuner, C., 2007. *European Data Protection Law - Corporate Compliance and Regulation.* 2. udgave. Oxford: Oxford University Press. (Citeret: Christopher Kuner: European Data Protection Law)

Kuner, C., 2013. *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press.

Rowland, D., Kohl, U., & Charlesworth, A., 2016. *Information Technology Law*. 5. udgave. Florence: Taylor and Francis.

Trzaskowski, J., Savin, A., Lundqvist, B. og Lindskoug, P., 2015. *Introduction to EU Internet Law.* København: Ex Tuto Publishing.

Udsen, H., 2015. *It-ret.* 2. udgave. København: Ex Tuto Publishing.

## 7.6. Artikler

Bender, D., 2016. Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective, *International Data Privacy Law*, 6(2), s. 117-138. (Citeret: David Bender: Will the CJEU do better with privacy shield? A US perspective).

Blume, P., 2014. International overførsel af personoplysninger. *Juristen*, 5, s. 149-154.

Blume, P., 2015. EU adequacy decisions: the proposed new possibilities, *International Data Privacy Law*, 5(1), s. 34-39.

Blume, P., 2015. Overførsel af personoplysninger, *Ugeskrift for Retsvæsen*, s. 417.

Kuner, C., 2016. Reality and Illusion in EU Data Transfer Regulation Post Schrems, *University of Cambridge Faculty of Law Legal Studies Research Paper Series*, 14/2016.

Leathers, D.R., 2009. Giving Bite to the EU-U.S. Data Privacy Safe Harbor: Model Solutions for Effective Enforcement, *Case Western Reserve Journal of International Law*, 41(1), s. 193-242.

Padova, Y., 2016. The Safe Harbour is invalid: what tools remain for data transfers and what comes next?, *International Data Privacy Law*, 6(2), s. 139-161.

Reidenberg, J.R., 1995. Setting Standards for Fair Information Practice in the US Private Sector, *Iowa Law Review*, 80(3), s. 497-552.

Reidenberg, J.R., 2001. E-Commerce and Trans-Atlantic Privacy, *Houston Law Review*, 38, s. 717-750.

Severson, D., 2015. American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change, *Harvard International Law Journal*, 56(2), s. 465-514.

Svantesson, D.J.B., 2015. Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation. *International Data Privacy Law*, 5(4), s. 226-234.

Tracol, X., 2016. “Invalidator” strikes back: The harbour has never been safe, *Computer Law & Security Review*, 32, s. 345-362.

Tracol, X., 2016. EU–U.S. Privacy Shield: The saga continues, *Computer Law & Security Review*, 32, s. 775-777.

Voss, W.G., 2016. The Future of Transatlantic Data Flows: Privacy Shield or Bust?, *Journal of Internet Law*, 19(11), s. 1-18.

## 7.7. Rapporter

Connolly, C., 2008. The US Safe Harbor - Fact or Fiction? [PDF] Tilgængelig: <http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf> [Besøgt: 30/10/2016].

European Parliament, 2000. Report on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles (C5-0280/2000 – 2000/2144(COS)) (A5-0177/2000). [PDF] Tilgængelig: <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/0117-02_en.pdf> [Besøgt: 30/10/2016] (Citeret: European Parliament: Report A5-0177/2000).

Executive Office of the President, 2014. Big Data: Seizing Opportunities, Preserving Values. [PDF] Tilgængelig: <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf> [Besøgt: 24/10/2016].

Hogan Lovells, 2016. Legal Analysis of the EU-U.S. Privacy Shield - An adequacy assessment by reference to the jurisprudence of the Court of Justice of the European Union. [PDF] Tilgængelig: <https://www.hoganlovells.com/~/media/hogan-lovells/pdf/news/privacy-shield-legal-analysis-by-hogan-lovells-20160331.pdf> [Besøgt: 29/12/2016].

McKinsey Global Institute, 2016. Digital Globalization: The New Era of Global Flows. [PDF] Tilgængelig: <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows> [Besøgt: 10/09/2016].

Moerel, L., 2016. An assessment of the impact of the Schrems judgement on the data transfer grounds available under EU data protection law for data transfers to the U.S. [PDF] Tilgængelig: <http://www.itic.org/dotAsset/d/2/d2988618-d28e-4888-a192-fd2cdc743a9a.pdf> [Besøgt: 29/12/2016].

Sidley, 2016. Essentially Equivalent - A comparison of the legal orders for privacy and data protection in the European Union and United States. [PDF] Tilgængelig: <http://www.sidley.com/~/media/publications/essentially-equivalent---final.pdf> [Besøgt:29/12/2016].

Weiss, M.A. og Archick, K., 2016. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. [PDF] Tilgængelig: <https://www.fas.org/sgp/crs/misc/R44257.pdf> [Besøgt: 24/10/2016].

## 7.8. Øvrige

Council of Europe Treaty No.108. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.*

Council of Europe Treaty No. 181. *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows.*

European Data Protection Supervisor, 2016. *Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision.*

OECD, 2013. The OECD Privacy Framework. [PDF] Tilgængelig: < http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>

United States Department of Justice, 2015. Overview of the Privacy Act of 1974. [PDF] Tilgængelig: <https://www.justice.gov/opcl/file/793026/download> [Besøgt: 24/10/2016]

## 7.9. Websteder

Bracy, J., 2016. *Model clauses in jeopardy with Irish DPA referral to CJEU.* Tilgængelig: <https://iapp.org/news/a/model-clauses-in-jeopardy-with-irish-dpa-referral-to-cjeu/> [Besøgt: 09/12/2016]

Data Protection Commissioner, 2016. *Update on Litigation Involving Facebook and Maximillian Schrems - Explanatory Memo.* Tilgængelig: <https://www.dataprotection.ie/docs/28-9-2016-Explanatory-memo-on-litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm> [Besøgt: 09/12/2016]

European Commission, 2015. *First Vice-President Timmermans and Commissioner Jourová's press conference on Safe Harbour following the Court ruling in case C-362/14 (Schrems).* Tilgængelig: <http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm> [Besøgt: 05/12/2016]

European Commission, 2016. *Commission decisions on the adequacy of the protection of personal data in third countries.* Tilgængelig: <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> [Besøgt: 13/10/2016]

European Commission, 2016. *European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows.* Tilgængelig: <http://europa.eu/rapid/press-release_IP-16-2461_en.htm> [Besøgt: 10/12/2016]

European Commission, 2016. *Reform of EU Data Protection Rules.* Tilgængelig: <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> [Besøgt: 22/09/2016]

European Commission, 2016. *United States - Trade.* Tilgængelig: <http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/> [Besøgt: 23/10/2016]

European Free Trade Association, 2016. *32016R0679.* Tilgængelig: <http://www.efta.int/eea-lex/32016R0679> [Besøgt: 08/10/2016]

European Ombudsman, 2016. *Use of the title 'ombudsman' in the 'EU-US Privacy Shield' agreement.* Tilgængelig: <http://www.ombudsman.europa.eu/resources/otherdocument.faces/en/64157/html.bookmark> [Besøgt: 19/12/2016]

Facebook, 2016. *Statement of Rights and Responsibilities.* Tilgængelig: <https://www.facebook.com/legal/terms/update> [Besøgt: 10/11/2016]

Floretti, J. og Volz, D., 2016. *Privacy group launches legal challenge against EU-U.S. data pact.* Tilgængelig: <http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN12Q2JK> [Besøgt: 19/12/2016]

Floretti, J., 2016. *EU-U.S. personal data pact faces second legal challenge from privacy groups.* Tilgængelig: <http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKBN12X253> [Besøgt: 19/12/2016]

Lynskey, O., 2015. *Negotiating the Data Protection Thicket: Life in the Aftermath of Schrems.* Tilgængelig: <http://blogs.lse.ac.uk/mediapolicyproject/2015/10/12/negotiating-the-data-protection-thicket-life-in-the-aftermath-of-schrems/> [Besøgt: 27/11/2016]

Metz, C., 2016. *Facebook and Microsoft Are Laying a Giant Cable Across the Atlantic.* Tilgængelig: <https://www.wired.com/2016/05/facebook-microsoft-laying-giant-cable-across-atlantic/> [Besøgt: 10/09/2016]