INTERNATIONALE PERSONDATAOVERFØRSLER – EN BEDØMMELSE AF PRIVACY SHIELDS KONFORMITET MED PERSONDATAFORORDNINGEN

INTERNATIONAL TRANSFERS OF PERSONAL DATA – AN EVALUATION OF THE PRIVACY SHIELD SCHEME'S CONFORMITY WITH THE EU GENERAL DATA PROTECTION REGULATION

af HANY DUGHAIM

Afhandlingen har til formal at undersøge, hvordan europæiske virksomheder rent praktisk anvender Privacy Shield-ordningen til at foretage internationale persondataoverførsler til USA. Det undersøges også i hvilket omfang Privacy Shield-ordningen skal revideres for at blive konform med persondataforordningen samt EU-domstolens og Den Europæiske Menneskerettighedsdomstols praksis om data- og privatlivsbeskyttelse.

I afhandlingen konkluderes det, at der må være et grænseoverskridende element til stede i forbindelse med en persondataoverførsel, før overførslen kan være underlagt persondataforordningens regler om tredjelandsoverførsler. Derudover skal det grænseoverskridende element føre til en form for skift af jurisdiktion over databehandlingen i det pågældende modtagerland. I afhandlingen konkluderes det også, at der på trods af enkelte forbedringer siden ugyldiggørelsen af den før gældende Safe Harbor-ordning stadig savnes specifikke forbedringer, som vil opfylde de principper, der er udtrykt i persondataforordningen. Disse forbedringer vil i større grad sikre transparens og give den registrerede endnu mere selvbestemmelse. Dette kan Kommissionen sikre, når den skal lave sin årlige revidering, ved at implementere regler om profilering og dataminimering samt kræve at princippet om oplysningspligt skal opfyldes på et tidligere stadie, end hvad der oprindeligt kræves i Privacy Shield-ordningen.

Indholdsfortegnelse

Abstract

This thesis seeks to examine how European companies use the Privacy Shield Scheme to perform international transfers of personal data to the U.S, and to what extent the Privacy Shield Scheme needs to be revised to be fully compliant to the EU General Data Protection Regulation.

This thesis concludes that when transferring personal data there must be a cross-border element related to the transfer before the data transfer can be subject to the third-country transfer rules in the EU General Data Protection Regulation. The cross-border element must also lead to a form of jurisdictional change regarding the data processing in the receiving country.

Despite of a few adjustment made since the invalidation of the now pre-existing Safe Harbor Arrangement, this thesis concludes that the Privacy Shield Scheme still lacks specific improvements that would fulfill the principles set out in the EU General Data Protection Regulation. The improvements would ensure even greater transparency and provide the data subject with even more self-determination. This can be made by requiring that the notice principle should be fulfilled at an earlier stage than what is required in the Privacy Shield Scheme. The Commission should implement rules regarding profiling and data minimization in accordance with the EU General Data Protection Regulation.

Forkortelser

Visse begreber og henvisninger er af så central karakter i denne afhandling, at de for overskuelighedens skyld vil anvendes i følgende forkortelser:

Charteret	Den Europæiske Unionens Charter om Grundlæggende Rettigheder.
Commissioner	Den irske Data Protection Commissioner.
EU	Den Europæiske Union (i afhandlingen omfattes også EØS).
EMD	Den Europæiske Menneskerettighedsdomstol.
EMRK	Den Europæiske Menneskerettighedskonvention.
FTC	Federal Trade Commission.
Handelsministeriet	The Department of Commerce.
Kommissionen	Europa-Kommissionen.
Leander-dommen	Leander mod Sverige, 9248/81, 26.03.87.
Safe Harbor	Kommissionens beslutning af 26. juni 2000 (2000/520) EF.
Schrems-dommen	C-362/14 Schrems mod Data Protection Commissioner.
Persondatadirektivet	Direktiv 95/46 EF.
Persondataforordningen	Forordning 2016/679 EU.
Privacy Shield	Kommissionens gennemførelsesafgørelse (EU) 2016/1250.

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 jf. persondataforordningens artikel 4 nr.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, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse jf. persondataforordningens artikel 4 nr.2.

Grænseoverskridende behandling: behandling af personoplysninger, der finder sted som led i aktiviteter, som udføres for en dataansvarligs eller en databehandlers virksomheder i mere end én medlemsstat i Unionen, hvor den dataansvarlige eller databehandleren er etableret i mere end én medlemsstat, eller b) behandling af personoplysninger, der finder sted som led i aktiviteter, som udføres for en dataansvarligs eller en databehandlers eneste etablering i Unionen, men som i væsentlig grad påvirker eller sandsynligvis i væsentlig grad vil kunne påvirke registrerede i mere end én medlemsstat jf. persondataforordningens artikel 4 nr.23.

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 jf. persondataforordningen artikel 4 stk. nr.7.

Databehandler: en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne jf. persondataforordningens artikel 4 nr.8.

1. Introduktion

1.1. Indledning

‘’Big Brother is watching you’’

Dette verdensberømte citat kom til udtryk i 1949 af George Orwell i romanen *1984*. Udtrykket Big Brother refererer til en leder eller regering som invaderer borgernes privatliv gennem masseovervågning ved hjælp af avanceret teknologi. Selvom udtrykket er fra 1949 er den fortsat yderst relevant i nutidens verden. Som forudset af George Orwell har den informationsteknologiske udvikling, der har sin baggrund i globaliseringen, gjort det nemmere at overvåge borgere og invadere deres privatliv. Dette blev belyst i 2013, hvor whistlebloweren Edward Snowden afslørede for omverdenen, at den amerikanske efterretningstjeneste, NSA, brugte sit PRIS-program til at indsamlede personlige oplysninger om blandt andre europæiske borgere fra amerikanske virksomheder som havde tilsluttet sig Safe Harbor-ordningen. Dette blev gjort uden borgernes viden eller samtykke. Der var tale om en masseovervågning af europæiske borgere uden hensyn til deres ret til data- og privatlivsbeskyttelse.

Afsløringerne belyser den teknologiske udviklings negative konsekvens på persondatabeskyttelsen. Stater har grænser, men internettet kender ingen grænser. Elektronisk persondata kan overføres på tværs af landegrænser, og dermed være undergivet forskellige landes lovgivninger. Persondata kan således risikere at blive overført til steder, hvor der er ringe eller ingen databeskyttelse; de såkaldte data havens.[1] I 2000 vedtog Kommissionen en aftale med USA om Safe-Harbor-ordningen. Årsagen hertil var, at USA betragtede persondatadirektivet som en handelsbarriere.[2] Ordningen gjaldt for amerikanske virksomheder, der tilsluttede sig den. Disse virksomheder kunne frit modtage persondata fra europæiske virksomheder uden for persondatadirektivet. Dette kunne ske fordi Safe Harbor-ordningen var udtryk for, at Kommissionen betragtede USA som en *sikker havn* for persondata. Edward Snowdens afsløringer dannede grundlag for Safe-Harbor-ordningens bortfald og senere til skabelsen af Privacy Shield-ordningen. Afsløringerne viser også, at der som følge af den teknologiske udvikling er behov for et harmoniserende internationalt regelsæt som regulerer grænseoverskridende behandling af persondata og som sikrer ensartethed i databeskyttelsesretten. Dette er blandt andet formålet med den nye persondataforordning som skal erstatte persondatadirektivet.

1.2. Problemformulering

Grundlaget for Privacy Shield er persondatadirektivet, der fortsat er gældende indtil persondataforordningen træder i kraft i maj 2018. Privacy Shield er dog udformet med udsigt til en mulig revidering, med det formål at være konform med persondataforordningen.[3]

Det vil i afhandlingen afklares, hvad der forstås ved en persondataoverførsel. Dette gøres for at fastslå det præcise anvendelsesområde for Privacy Shield. Der vil redegøres for de almindelige overførselsregler i persondataforordningen. Formålet hermed er løbende at drage paralleller og sammenligninger med Privacy Shield. For at få en forståelse for indholdet af Privacy Shield og eventuelle forskelle mellem denne og persondataforordningens overførselsregler foretages en gennemgang af forholdet mellem USA og EU, herunder forskelle på amerikansk og europæisk databeskyttelsesret. Dernæst foretages en gennemgang af Privacy Shield princippernes praktiske anvendelse, hvor der drages sammenligninger med principperne i persondataforordningen. Samtidig gennemgås de generelle kritikpunkter til de enkelte Privacy Shield principper. Derefter vurderes det, i hvilket omfang Privacy Shield principperne opfylder de krav til beskyttelse af privatliv og effektive retsmidler, der er blevet fastlagt i retspraksis.

Formålet med at gennemgå Privacy Shield kritikpunkterne og at drage sammenligninger med principperne i persondataforordning er at lave en vurdering af, hvorvidt der er behov for en revidering af Privacy Shield og i så fald, i hvilket omfang ordningen skal revideres. Vurderingen af revideringens nødvendighed og omfang sker i lyset af retspraksis og afhandlingens gennemgang af forholdet mellem USA og EU, herunder forskellene på de to aktørers syn på databeskyttelsesretten.

1.3. Emneafgrænsning

Denne afhandling har fokus på datastrømninger mellem private virksomheder i EU og USA. Dette skyldes USA's afgørende på det globale marked og de mange dataoverførsler mellem EU og USA, herunder fra amerikanske virksomheder etableret i EU. USA's globale status kan man ikke politisk eller økonomisk se bort fra, og det er af hensyn til den fri internationale handel og den generelle interesse i, at der ikke findes for restriktive barrierer, at der er skabt en hel speciel ordning for USA. Hovedfokus bliver derfor Privacy Shield-ordningen, som kun gælder mellem EU og USA. Der vil dog i generelle træk redegøres for og sammenlignes med andre overførselsgrundlag.

[1] Peter Blume: Persondataretlige Grundfigurer, 1. udgave, 2017, s. 113.
[2] Ibid., s. 121.
[3] Peter Blume: Den Nye Persondataret, 1. udgave, 2016, s. 144.

Den første årlige revidering af Privacy Shield fandt sted i september 2017 og resultatet blev først offentliggjort d. 18. oktober 2017.[4] Det har været uklart, hvor længe revideringen vil foregå, og præcist hvornår resultatet af revideringen vil blive offentliggjort.[5] Det var derfor ikke praktisk muligt at inddrage resultatet af den endelige årlige revidering i denne afhandling. Det skal dog bemærkes, at rapportens 10 anbefalinger til revideringer af Privacy Shield for det meste drejer sig om præciseringer af forholdet mellem amerikanske og europæiske datatilsynsmyndigheder samt præciseringer af amerikanske datatilsynsmyndigheders kompetencer, hvilket netop var nogle af afhandlingens kritikpunkter og anbefalinger.

1.4. Metode og retskilder

Det er målet med denne afhandling at beskrive, fortolke, analysere og systematisere gældende ret inden for internationale persondataoverførsler. Der er således tale om en retsdogmatisk afhandling.[6]

Afhandlingens omdrejningspunkt er Privacy Shield, der kom til verden som reaktion på Schrems-dommen, der blev afsagt med udgangspunkt i persondatadirektivet. Til analysering af retstilstanden for internationale persondataoverførsler mellem EU og USA tages der udgangspunkt i persondataforordningen. Der vil dog henvises til persondatadirektivet, der fortsat er gældende, i det omfang forordningen afviger fra direktivet.

Det følger af persondatadirektivets artikel 2, at medlemsstaterne skal sikre overholdelsen af grundlæggende rettigheder og friheder, navnlig den ret til privatlivets fred, der følger af EMRK artikel 8 og i fællesskabets generelle principper. Afhandlingen inddrager derfor de retskilder, der knytter sig til de europæiske menneskerettigheder, såsom EMRK og Charteret, samt retspraksis fra EU-Domstolen og EMD. Der vil findes vejledning i øvrige traditionelle internationale persondataretlige kilder[7] i det omfang EMRK og Charteret ikke giver et fyldestgørende svar på de relevante problemstillinger.

1.4.1. Generelt om persondatadirektivet og persondataforordningen

Det følger af persondatadirektivets artikel 2, at formålet med direktivet er at sikre et højt fælles databeskyttelsesniveau i EU, og at sikre fri dataoverførsel mellem landene. Direktivet indeholder mange rettigheder for borgerne, og henviser i sin præambel til EMRK artikel 8 om ret til privatliv. Man havde en ide om, at hvis man giver borgerne en god databeskyttelse bliver det accepteret, at personoplysninger behandles digitalt.[8] Direktivet er fra 1995 og dermed fra den tidlige fase af internettets udbredelse. Siden hen har informationsteknologien udviklet sig så drastisk, at man har vedtaget persondataforordningen, fordi der har været behov for en mere tidsopdateret og harmoniserende regulering af databeskyttelsesretten.[9] Dette underbygges af, at OECD[10] har efterspurgt en mere global samarbejde og interoperabilitet når det kommer til regulering af persondatabeskyttelse.[11] Direktivet har med andre ord ikke kunne følge med den teknologiske udvikling, og har dermed ikke kunne sikre en god databeskyttelse, hvilket førte til vedtagelsen af persondataforordningen.

---

[4] COM (2017) 611 Final, ''Report from the Commission to the European Parliament and The Council on the first annual review of the functioning of the EU-U.S. Privacy Shield, Brussels, 18.10.2017.
[5] Link: http://europa.eu/rapid/press-release_SPEECH-17-826_en.htm, besøgt d. 25.09.2017, kl. 14.00.
[6] Evald og Schaumburg-Müller: Retsfilosofi, Retsvidenskab og Retskildelære, 1. udgave, 2014, s. 3.
[7] Europarådets Konvention nr. 108 af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (herefter *''Persondatakonventionen''*) og 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 (herefter *''OECD Privacy Framework Guidelines''*).
[8] Peter Blume: Persondataretlige Grundfigurer, 1. udgave, 2017, s. 18.
[9] Ibid., s. 25-26.
[10] Organisation for Økonomisk Samarbejde og Udvikling.
[11] OECD Privacy Framework Guidelines, 2013, side 33.

1.4.2. Databeskyttelsesrettens forhold til EMRK og Charteret

Det fremgår af persondataforordningens artikel 1, at formålet med forordningen er at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger. Databeskyttelse er en overordnet rettighed, som forordningen skal realisere jf. forordningens betragtning nr.1, der henviser til retten til databeskyttelse i Charterets artikel 8. Her skal det bemærkes, at persondataforordningen, modsat persondatadirektivet, ikke henviser til privatlivsbeskyttelse i EMRK artikel 8, men alene henviser til retten til databeskyttelse i Charterets artikel 8. Dette er på grund af Charterets udformning, der i artikel 7 kategoriserer beskyttelsen af privatlivets fred som en særskilt grundrettighed. Umiddelbart kan det derfor betragtes, at EMRK er overflødig når det kommer til persondatabeskyttelsen og at persondatabeskyttelse er en særlig art EU-grundrettighed i persondataforordning. Forordningens bestemmelser må dog ses som et bidrag til EU's realisering af EMRKs artikel 8, der giver en samlet beskyttelse af privatlivs- og databeskyttelse.[12] Dette underbygges af, at Charterets artikel 52 stk.3 udtrykker, at beskyttelsen ikke skal anvendes på en sådan måde, at den kommer i modstrid med den menneskeretlige privatlivsbeskyttelse. Dette må betyde, at EMRK er centralt placeret, når det kommer til, hvilken retskilde skal styre menneskerettighederne.

2. Grænseoverskridende persondataoverførsler

Persondataforordningens regler om overførsler af persondata findes i forordningens kapitel 5. Overførselsreglerne er til for at sikre, at det beskyttelsesniveau som forordningen tilsigter at opnå, også vil være gældende i det tredjeland som personoplysningerne overføres til.[13] Det er afgørende for overførselsreglernes anvendelse, at databehandlingen faktisk er en overførsel. I dette kapitel vil det derfor først klarlægges, hvornår der er tale om en dataoverførsel som er omfattet af forordningens overførselsregler. Dernæst vil der foretages en gennemgang af de relevante overførselsregler.

2.1. Overførselsbegrebet

Det følger af persondataforordningens artikel 4 stk.2, at videregivelse eller overladelse er en form for persondatabehandling. Dette er i tråd med persondatakonventionen artikel 2 (c), der definerer elektronisk behandling som elektronisk videregivelse af oplysninger. Derudover definerer OECD retningslinjerne grænseoverskridende dataoverførsler som *''movements of personal data across national borders''*.[14]

2.1.1. Overførselsbetragtningerne

Det beror typisk på en konkret vurdering, hvorvidt en behandling er udtryk for en overførsel og skal oftest fastlægges ud fra forskellige betragtninger.[15]

Det kan have en betydning for, hvorvidt der er tale om en overførsel, at persondata videregives til en modtager, som er underlagt en fremmed stats jurisdiktion til at håndhæve databeskyttelsesreglerne.[16] Det krævede jurisdiktionsskift skal være uden for EU, før der er tale om en overførsel omfattet af persondataforordningen. Det er fordi, at dataoverførsler på tværs af landegrænser inden for EU er tilladt af hensyn til det indre marked, jf. forordningens artikel 1 stk.3.

[12] Peter Blume: Den Nye Persondataret, 1. udgave, 2016, s. 47.
[13] Peter Blume: Persondataretlige Grundfigurer, 1. udgave, 2017, s. 116.
[14] OECD Privacy Framework Guidelines, 2013, side 13.
[15] Peter Blume: Den Nye Persondataret, 1. udgave, 2016, s. 134.
[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 stk.1.

Overførselsbegrebet kan også afhænge af, hvorvidt det er persondataforordningens/medlemsstatens ret eller et tredjelands lovgivning, der finder anvendelse på databehandlingen.[17] Når en databehandling er underlagt en anden jurisdiktion er den ikke nødvendigvis underlagt denne pågældende jurisdiktions lovgivning.[18] Lovvalget må findes efter en konkret vurdering på baggrund af EU-rettens etableringsbegreb.[19] Der kan lægges vægt på, hvorvidt den dataansvarlige udøver ledelses- og instruktionsret over for den person, der behandler personoplysninger i tredjelandet.[20] Er dette tilfældet kan det siges, at der ikke er tale om en dataoverførsel, eftersom den dataansvarlige kan bestemme, at EU-reglerne skal overholdes. [21] Dette ændrer dog ikke på, at det er tredjelandets myndigheder som må håndhæve databeskyttelsesretten, hvorfor tredjelandets håndhævelsesregler altid vil have en betydning.

Det kan også have en betydning for overførselsbegrebet, hvorvidt personoplysningerne i en vis grad af permanens, som følge af en aftale mellem en afsender og en modtager, er blevet flyttet til en anden jurisdiktion, hvor de bliver genstand for faktisk behandling, og ikke blot, at personoplysningerne placeres i den anden jurisdiktion uden at der gøres nærmere brug af dem.[22] Det kan ligeledes have en betydning, hvorvidt det har været intentionen at foretage videregivelsen.[23]

2.1.2. Overførselsproblematikken illustreret i retspraksis

Problematikken omkring fastsættelse af overførselsbegrebet kan illustreres ved en gennemgang af Lindqvist-dommen[24]. Sagen omhandlede Lindqvist, der oprettede en hjemmeside, hvortil hun uden samtykke uploadede personlige oplysninger om sine kollegaer. De for afhandlingen vigtigste spørgsmål er, hvorvidt Lindqvists handlinger kan karakteriseres som en dataoverførsel til et tredjeland, selv hvis ingen borgere fra tredjelandet har set eller indhentet oplysningerne.[25]

Domstolen nåede frem til, at der ikke foreligger videregivelse af personoplysninger til et tredjeland i persondatadirektivets forstand.[26] Man lagde vægt på, at Lindqvist ikke brugte en teknologisk metode, der kunne sende oplysningerne direkte til servere i tredjelandsborgeres computere. Tredjelandsborgerne skulle i stedet selv være forbundet til internettet og aktivt gå ind på linket med det formål at indhente oplysningerne.[27] Dette argument kan støttes op på ovennævnte betragtning om, at der skal være en aftale mellem en afsender og modtager af personoplysningen. Argumentet virker dog svagt, da den indikerer, at man er nødt til at vente på, at en tredjelandsborger rent faktisk aktivt går ind og indhenter oplysningerne, før der er tale om en persondataoverførsel. I så fald ville dette underminere direktivets præventive effekt. Domstolen begrundede også afgørelsen med, at hvis man betragtede Lindqvists adfærd som en videregivelse til et tredjeland i direktivets forstand, ville det have den konsekvens, at enhver upload af personoplysninger på internettet skulle betragtes som en videregivelse til et tredjeland. I sådanne situationer ville Kommissionen være forpligtet til at forbyde enhver personlig oplysning i at blive uploadet på nettet, fordi der ville være risiko for, at nogle af disse tredjelande er utilstrækkelige.[28]

---

[17] Peter Blume: Persondataretlige Grundfigurer, 1. udgave, 2017, s. 115.
[18] Article 29 Working Party: Opinion 8/2010 on applicable law, s. 10.
[19] Peter Blume: Retlig Regulering af Internationale Persondataoverførsler, 1. udgave, 2006, side 21.
[20] Jon Bing: Lov og Rett, vol. 53, 3, 2014, side 134.
[21] Christopher Kuner: European Data Protection Law, 2nd edition, 2007, s. 168.
[22] Peter Blume: Retlig Regulering af Internationale Persondataoverførsler, 1. udgave, 2006, side 24.
[23] Ibid., side 25.
[24] C-101/01, straffesag mod Bodil Lindqvist, 6. november 2003.
[25] Ibid., præmis 18 nr. 5.
[26] Ibid., præmis 71.
[27] Ibid., præmis 60-61.
[28] C-101/01, straffesag mod Bodil Lindqvist, 6. november 2003, præmis 69.

Det er ligeledes værd at nævne den nedenfor gennemgået Schrems-dom, hvor Domstolen pointerede, at der er tale om en databehandling efter persondatadirektivets artikel 2 (b), når en virksomhed foretager en transaktion fra en medlemsstat til et tredjeland.[29] Dommen vedrørte Facebook Irlands videregivelse af personoplysninger til moderselskabet Facebook USA. Det må derfor betyde, at der er tale om en international persondataoverførsel omfattet af persondatadirektivet/persondataforordningens regler om tredjelandsoverførsler, når der sker videregivelser inden for koncerner fra EU-datterselskaber til et moderselskab i et tredjeland.

Konkluderende må det siges, at Domstolen ville have betragtet Lindqvists adfærd som en overførsel efter direktivet, men valgte i stedet at foretage en konsekvensafvejning, og nåede frem til det modsatte.[30] Denne fortolkningsstil illustrerer vanskeligheden ved at fastsætte overførselsbegrebet i direktivets såvel som i forordningens forstand. Lindqvist-dommen viser, at der må foretages en helt konkret vurdering, og man må se på mulige konsekvenser. Sikkert er det dog, at der kræves en form for grænseoverskridende element, hvilket i praksis næsten altid vil være tilfældet grundet de mange dataoverførsler som internettet giver mulighed for, og som var tilfældet for Lindqvist.

2.2. Overførselsreglerne

Der er adgang til fri dataoverførsel på tværs af medlemsstaternes landegrænser jf. persondataforordningens artikel 1 stk.3. Såfremt der foreligger en dataoverførsel til et tredjeland i persondataforordningens forstand finder forordningens overførselsregler i kapitel 5 dog anvendelse.

Forordningens kapitel 5 opstiller forskellige principper og krav som skal være opfyldt, og giver mulighed for at overføre persondata på grundlag af forskellige ordninger. Som noget nyt nævner forordningens kapitel 5 i sin overskrift, at der kan ske overførsler til internationale organisationer, mens artikel 44 nævner specifikke sektorer i tredjelandet.

2.2.1. Overførsler baseret på en afgørelse om tilstrækkeligt beskyttelsesniveau

Forordningens artikel 44 fastsætter udgangspunktet om, at overførsler til tredjelande kun tillades, hvis importlandet sikrer et tilstrækkeligt beskyttelsesniveau for behandling af persondata. Det vil sige, at der som minimum skal være samme beskyttelse af forordningens rettigheder i tredjelandet som i eksportlandet/medlemsstaten.

Det følger af forordningens artikel 45 stk.2, at det er Kommissionen som skal træffe afgørelse om et tredjelands beskyttelsesniveau på baggrund af momenter som fremgår af bestemmelsens litra a-c og forordningens betragtning nr. 104. Kommissionen skal ikke blot tage hensyn til tredjelandet specifikke persondataretlige regler, men skal også tage hensyn til den retlige regulering i det pågældende tredjeland og dets internationale forpligtelser. Man ser fx på tredjelandets forhold til retsstatsprincippet, menneskerettighederne og grundlæggende frihedsrettigheder samt hvorvidt der er tilstedeværelse af flere velfungerende uafhængige myndigheder. Bestemmelsen lægger også vægt på, at det skal indgås i vurderingen, hvorvidt tredjelandet regulerer videreoverførsel til andre tredjelande. Dette må siges at være et særligt vigtigt moment, da forordningen ellers ville virke illusorisk, hvis tredjelandet uden videre kan videreoverføre til et nyt tredjeland som ikke har et tilstrækkeligt beskyttelsesniveau.

Afgørelsen om et tredjelands beskyttelsesniveau træffes ved en gennemførelsesretsakt som skal være genstand for revision hvert fjerde år jf. forordningens artikel 45 stk.3. Blume anfører, at dette er en sympatisk regel, men kan virke belastende.[31] Det må dog siges, at man ved at tage retsakterne til

[29] C-362/14 Schrems mod Data Protection Commissioner, præmis 45.
[30] Dan Jerker B. Svantesson: The Regulation of Cross-border Data Flows, International Data Privacy Law, Vol. 1, No.3, 2011.
[31] Peter Blume: Persondataretlige Grundfigurer, 1. udgave, 2017, s. 118, note 3.

revision hvert fjerde år, undgår den uheldige situation som var grundlag for underkendelsen af Safe Harbor. Her havde beskyttelsesniveauet i USA udviklet sig negativt i løbet af årene som afsløret af Edward Snowden. Gennem den gentagende revision sikrer man sig, at retsakten er udtryk for en tidssvarende tiltrækkelighedsbedømmelse af tredjelandet. Det kan dog diskuteres, hvorvidt revisionsperioden bør være længere end 4 år.

2.2.2. Overførsler omfattet af fornødne garantier

I visse tilfælde ønsker en virksomhed i EU at overføre persondata til et tredjeland, der ikke er blevet vurderet til at have et tilstrækkeligt beskyttelsesniveau. Dette er muligt efter persondataforordningens artikel 46-49 ved anvendelse af enten generelle ordninger, der har indbygget de nødvendige garantier eller overførsler som er baseret på enkeltstående hjemmelsgrundlag, der bruges specifikt med henblik på en bestemt dataoverførsel.

Artikel 46 opstiller flere ordninger som giver tilladelse til overførsler, hvis dataeksportøren giver de fornødne garantier, og på betingelse af at rettigheder, som kan håndhæves, og effektive retsmidler for registrerede er tilgængelige.

2.2.2.1. Bindende virksomhedsregler

Det følger af persondataforordningens artikel 46 stk.2 (b), at der uden krav om specifik godkendelse fra en tilsynsmyndighed kan sikres fornødne garantier gennem bindende virksomhedsregler (BVR) i overensstemmelse med artikel 47.

BVR er et sæt retligt bindende regler i koncerner, som fastsætter principper og procedurer for behandling af persondata på tværs af koncernen og som tildeler den registrerede bestemte rettigheder, der kan håndhæves jf. forordningens artikel 47 stk.1 (a-b). BVR er specifikke i forhold til koncernernes behov. Der findes derfor ikke en standard sæt BVR som en koncern kan anvende. Koncernen må i stedet udforme sit eget.[32]

Den kompetente tilsynsmyndighed skal i overensstemmelse med den sammenhængsmekanisme, der er omhandlet i artikel 63 godkende bindende virksomhedsregler. Sammenhængsmekanismen går ud på at tilsynsmyndighederne samarbejder med hinanden og eventuelt Kommissionen med henblik på at bidrage til en ensartet anvendelse af forordningen i hele EU. Dette giver i sig selv god mening, da BVR især anvendes i større koncerner som kan have aktiviteter og filialer i flere europæiske lande såvel som i USA. Behov for en sammenhængsmekanisme inden for BVR-godkendelser kan fx være nyttigt når en koncern etableret i EU anvender et call center, som er placeret i et tredjeland.[33]

2.2.2.2. Kontrakt- og standardbestemmelser

Fornødne garantier kan også sikres gennem en kontraktindgåelse mellem dataeksportøren og dataimportøren. Det står parterne frit selv at udfærdige en kontrakt, der kan tjene som grundlag for en dataoverførsel til et tredjeland jf. forordningens artikel 46 stk.3 (a) med forbehold af godkendelse fra den kompetence tilsynsmyndighed.

Det følger også af forordningens artikel 46 stk.2 (c-d), at der kan sikres fornødne garantier gennem standardbestemmelser om databeskyttelse vedtaget og godkendt af henholdsvis en tilsynsmyndighed og Kommissionen efter proceduren i artikel 93 stk.2. Denne bestemmelse henviser til reglerne om undersøgelsesproceduren i forordning 182/2011 EU artikel 5, som ikke vil behandles i denne afhandling.

[32] Peter Blume: Persondataretlige Grundfigurer, 1. udgave, 2017, s. 140.
[33] Peter Blume: Retlig Regulering af Internationale Persondataoverførsler, 1. udgave, 2006, side 138, note 28.

Pr. juli 2017 har Kommissionen vedtaget 3 sæt standardkontrakter.[34] Det følger af persondataforordningens artikel 46 stk.5, at Kommissionens standardkontrakter fortsat er gældende indtil de ændre, erstattes eller ophæves. Dette kan meget muligt blive tilfældet inden for de nærmeste par år, da standardkontrakterne er udformet før forordningens tid og på baggrund af persondatadirektivets artikel 26 stk.4. Det kan derfor argumenteres for, at standardkontrakterne ikke lever op til det beskyttelsesniveau som nutidig europæisk databeskyttelsesret kræver. Dette er også baggrunden for Maximillian Schrems indgivelse af en fornyet klage (Schrems II) til den irske databeskyttelseskommissær om gyldigheden af Kommissionens standardkontrakter. Som følge af underkendelsen af Safe Harbor vælger Facebook Irland at anvende Kommissionens standardkontrakter til at overføre persondata til Facebook USA. Schrems nye klage er fortsat, at USA's lovgivning ikke sikrer en tilstrækkelig beskyttelse af europæiske borgeres personoplysninger. En underkendelse af standardkontrakterne kan også få en negativ indflydelse på Privacy Shield-ordningen, da spørgsmålet om standardkontraktens gyldighed blandt andet beror på, hvorvidt USA's lovgivning yder et tilstrækkeligt beskyttelsesniveau, hvilket er en forudsætning for Privacy Shields eksistens.[35]

De første høringer blev foretaget i februar 2017 for den irske Højesteret og det er endnu uvist, hvorvidt sagen tages til EU-domstolen.[36] Schrems II er derfor værd at nævne, grundet dens mulige indflydelse på Privacy Shield, men vil ikke være genstand for yderligere behandling i afhandlingen.

2.2.3. Individuelle overførsler

Såfremt der ikke foreligger en tilstrækkelighedsvurdering af et tredjeland, kan der også ske singulære dataoverførsler uden at det er på baggrund af en generel ordning.

Det er først og fremmest værd at nævne persondataforordningens artikel 48 som tillader overførsler eller videregivelse uden hjemmel i EU-retten.

Her kan den dataansvarlige eller databehandleren i EU blive pålagt at overføre personoplysninger til brug for en verserende retssag eller administrativ sag i et tredjeland. Artikel 48 bestemmer, at en sådan overførsel kun tillades, når den ligger inden for en international aftale. Artikel 48 må læses i sammenhæng med undtagelsen i artikel 49 stk.1 (e), som siger, at overførsler kan finde sted, hvis de er nødvendige for, at retskrav kan fastlægges, gøres gældende eller forsvares.

Artikel 49 er en undtagelse til hovedreglen om, at overførsler til tredjelande kun kan ske, hvis der foreligger et tilstrækkeligt beskyttelsesniveau. Artiklens stk.1 (a-g) oplister de undtagelser som kan danne grundlag for en individuel overførsel. Her kræves der blandt andet, at der foreligger et informeret samtykke fra den registrerede, overførslen er nødvendig af hensyn til opfyldelse af en kontrakt, nødvendig af hensyn til vigtige samfundsinteresser eller nødvendig af hensyn til at beskytte personens vitale interesser såfremt personen ikke er i stand til at give samtykke.

Artikel 49 stk.1 2. afsnit siger, at såfremt ingen af betingelserne i stk.1 (a-g) er opfyldt, kan der alligevel ske overførsler i helt særlige situationer. Dette forudsætter, at der er tale om en singulær overførsel, som kun vedrør et begrænset antal personer og er nødvendig af hensyn til legitime interesser

[34] Link: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm, besøgt d. 24.07.2017, kl. 14.00.
[35] Web-blog: Paolo Balboni: ‘’The Case of Standard Contractual Clauses: The Irish Data Protection Commissioner and Max Schrems’’, 12.03.2017, www.Paolobalboni.eu, besøgt d. 25.09.2017, kl. 14.30.
[36] Link: https://www.dataprotection.ie/docs/16-03-2017-Update-on-Litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm, besøgt d. 25.07.2017, kl. 14.15.

som ikke overrumples af frihedsrettighederne. Den dataansvarlige skal herudover underrette tilsynsmyndighederne og vurdere alle omstændigheder i forbindelse med overførslen. Målet med disse betingelser er at sikre, at der gives passende garantier for beskyttelse af personoplysningerne.

Undtagelsesbestemmelserne i artikel 49 skal fortolkes snævert og restriktivt.[37] Artikel 29-gruppen anbefaler, at man alene benytter artikel 49, hvis de øvrige overførselsmuligheder umuligt kan opfyldes og at man benytter dem som sidste udvej.[38] Grunden til Artikel 29-Gruppens skepsis er at dataeksportøren ikke er forpligtet til at beskytte persondata i tredjelandet, ligesom eksportøren ikke er forpligtet til at indhente forudgående tilladelse fra den relevante tilsynsmyndighed.[39]

Blume anfører, at undtagelsen ikke vil kunne anvendes af mindre dataansvarlige, men vil bruges i større kommercielle sammenhænge, og at det derfor er misvisende, at de bestemmelser som artiklen omfatter betegnes som undtagelser.[40] Dette er i tråd med Artikel 29-Gruppens udtalelse om, at undtagelserne er uegnede til at fungere som grundlag for overførsler af betydelige størrelser.[41]

3. Forholdet til USA

USA er EU's vigtigste handelspartner. Halvdelen af verdens BNP samt en tredjedel af al verdenshandel udspringer fra handelen mellem EU og USA.[42] Det kan derfor virke helt naturligt, at der findes en særlig ordning mellem USA og EU. Dette ændrer dog ikke på, at USA er et tredjeland som ethvert andet tredjeland og det giver anledning til diskussion om, hvorvidt overførsler til USA bør behandles anderledes end overførsler til et andet tredjeland.

3.1. Grundlaget for vurderingen af USA som et tilstrækkeligt tredjeland

Det er som nævnt oven for i afsnit 2.2.1 Kommissionen som træffer afgørelse om et tredjelands tilstrækkelighedsvurdering. Pr. september 2017 er 12 lande blevet vurderet at have et tilstrækkeligt beskyttelsesniveau, herunder USA med vedtagelsen af Privacy Shield, hvilket fremgår af oplistningen på Kommissionens egen hjemmeside.[43] USA's placering på listen giver dog anledning til en interessant overvejelse om, hvorvidt USA burde være placeret på listen.

Blume udtrykker, at Kommissionen har hjemmel i persondataforordningens artikel 45 stk.1 og 3 og i persondatadirektivets artikel 26 stk.5 til at beslutte, at et tredjeland har et tilstrækkeligt beskyttelsesniveau.[44] Det kan derfor i første omgang formodes, at Privacy Shield er en sådan tilstrækkelighedsvurdering af USA, da man ved vedtagelsen af denne ordning generelt antager, at USA's lovgivning sikrer en tilstrækkelig beskyttelse. Blume anfører dog samtidig, at Privacy Shield er en helt speciel ordning mellem USA og EU, og at USA næppe nogensinde vil anmode om en tilstrækkelighedsvurdering, hvorefter han pointerer USA's rolle som global økonomisk og politisk supermagt.[45] Derudover anfører Blume det problematiske ved at foretage en tilstrækkelighedsvurdering af et føderalt land med forskellige sektorer.[46] Netop på grund af USA's globale status og dataoverførslers nødvendighed må det forstås sådan, at den tilstrækkelighedsvurdering, som ligger til grund for Privacy

[37] Article 29 Working Party: Transfers of personal data to third countries, side 24.
[38] Article 29 Working Party: Working document: Article 26(1), side 9.
[39] Ibid., side 6.
[40] Peter Blume: Den Nye Persondataret, 1. udgave, 2016, s. 142.
[41] Article 29 Working Party: Working document: Article 26(1), side 9.
[42] Link: http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states, besøgt d. 25.07.2017, kl.17.00.
[43] Link: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm, besøgt d. 20.09.2017, kl. 15.30.
[44] Peter Blume: Den Nye Persondataret, 1. udgave, 2016, s. 144, og Persondataretlige Grundfigurer 1. udgave, 2017, side 121.
[45] Peter Blume: Persondataretlige Grundfigurer 1. udgave, 2017, side 121-122.
[46] Peter Blume: Retlig Regulering af Internationale Persondataoverførsler, 1. udgave, 2006, side 91-92.

Shield, ikke nødvendigvis har fulgt samme grad af intensitet som de øvrige lande på Kommissionens ovennævnte liste. Tilstrækkelighedsvurderingen har derimod i højere grad været båret af EU-USA dataoverførslers nødvendighed.

Forordningens artikel 45 om tilstrækkelighedsvurdering kræver, at tredjelandets nationale lovgivning inddrages som et moment i afvejningen. USA har dog ikke nogen specifik national databeskyttelseslov. I stedet har de amerikanske delstater deres egen databeskyttelseslovgivning med hver deres grad af beskyttelsesniveauer.[47] Dette taler for, at der ikke er foretaget en egentlig tilstrækkelighedsvurdering af USA, men at man i stedet har vurderet USA på baggrund af landets status og behovet for en særlig aftale, og at derfor er tale om en form for modificeret tilstrækkelighedsafgørelse.

Dette understøttes af, at forordningens artikel 50 og betragtning nr. 116 i pålægger Kommissionen og de nationale datatilsyn at etablere de nødvendige kontakter til tredjelande med henblik på globalt samarbejde og gensidig bistand for at sikre databeskyttelsen. Der kan derfor argumenteres for, at Privacy Shield ikke er en tilstrækkelighedsvurdering af USA, men derimod en særlig ordning af hensyn til det globale samarbejde med hjemmel i forordningens artikel 50. Denne særlige ordning skyldes altså USA's særlige status og de væsentlige forskelle mellem den europæiske og amerikanske opfattelse af databeskyttelsesret (afsnit 3.2).

3.2. Amerikansk databeskyttelsesret kontra persondataforordningen

For at undersøge den generelle retstilling i amerikansk datebeskyttelsesret må man forstå landets generelle opfattelse af privatlivsbeskyttelse. Den overordnede retskilde som giver grundlag for privatlivsbeskyttelse er den amerikanske forfatnings 4. tillægsprotokol, der giver borgere beskyttelse mod vilkårlige indgreb på deres person, hjem, papir og aktiver. Dette omfatter ligeledes telefon- og bankoplysninger. Beskyttelsen sikres dog kun, hvis individet har en legitim forventning om at få beskyttet sit privatliv. Såfremt individet frivilligt har overgivet persondata til en tredjepart, vil der formentlig ikke være en sådan legitim forventning. Det betyder, at forfatningen fx sikrer en ringe privatlivsbeskyttelse på internettet. Derudover sikrer forfatningen generelt set kun privatlivsbeskyttelse for amerikanske statsborgere og udlændinge som er lovligt bosatte i USA.[48] Dette er en væsentlig forskel på persondataforordningen, der i artikel 3 stk.2 beskytter enhver, der befinder sig i EU, uanset om man er statsborger i EU eller ej.

Det tætteste USA kommer på en national databeskyttelseslov på national plan er Privacy Act 1974, som regulerer persondatabehandling i USA. Loven er rettet mod offentlige myndigheder i USA og angår ikke private myndigheder.[49] Dette skyldes amerikanernes opfattelse af, at menneskerettighederne alene vedrører forholdet mellem stat og individ, og at den private sektor i høj grad overgives til den databeskyttelsesregulering, der determineres af markedet og konkurrenceforholdene.[50] Dette gør, at USA er meget sektorbaseret i sin regulering af databeskyttelsesretten inden for den private sektor, som i overvejende grad er bygget op af branchemæssig selvregulering.[51] Derimod kan man på delstatsniveau have en databeskyttelseslovgivning, der efter persondataforordningens vil opfylde

[47] IT Governance Privacy Team (Alan Calder, Richard Campo, Adrian Ross): EU General Data Protection Regulation (GDPR), An Implementation and Compliance Guideline, 2016, side 229.
[48] Directorate-General for Internal Policies, Policy Department C – Citizens' Rights and Constitutional Affairs: ''A Comparison between US and EU Data Protection Legislation for Law Enforcement'', study for LIBE, 2015, side 51.
[49] Directorate-General for Internal Policies, Policy Department C – Citizens' Rights and Constitutional Affairs: ''A Comparison between US and EU Data Protection Legislation for Law Enforcement'', study for LIBE, 2015, side 52-53.
[50] Peter Blume: Retlig Regulering af Internationale Persondataoverførsler, 1. udgave, 2006, side 91.
[51] Dan Jerker B. Svantesson: ''The Regulation of Cross-border Data Flows'', International Data Privacy Law, Vol. 1, No.3, 2011, side 185-186.

en tilstrækkelighedsvurdering, men hvor man risikere, at der sker en reeksport inden for samme tredjeland til en delstat, som har et ringe beskyttelsesniveau. Dette er fx tilfældet med USA.[52]

USA's særlige betydning og landets sektorbaserede databeskyttelsesregulering kan siges at have haft en betydning for udformningen af persondataforordningen. Fx giver persondataforordningens kapitel 5 nu mulighed for at overføre persondata til organisationer eller bestemte sektorer til tredjelande. Dette var ikke tilfældet med persondatadirektivet, men det må dog bemærkes at både Safe Harbor og Privacy Shields udformning var påvirket af USA's sektorbaserede lovgivning og særlige status. Begge ordninger have nemlig en opt-in mulighed for amerikanske virksomheder til at tilslutte sig ordningen. Dette indikerer, at der ikke var tale om en beslutning om et generelt tilstrækkelighedsniveau, da der ellers ikke ville have været en sådan opt-in mulighed. Spørgsmålet er, om dette er nok til at opretholde Privacy Shield i sin nuværende form.

4. Privacy Shield

Som nævnt i denne afhandlings kapitel 3 er der vedtaget en særlig overførselsordning mellem EU og USA, Privacy Shield. Denne særlige ordning skyldes en kombination af USA's særlige status og landets specielle forhold til databeskyttelsesret og privatlivsbeskyttelse. Det skal bemærkes, at Privacy Shield er udformet efter persondatadirektivets regler og ikke persondataforordningen, hvorfor det er tiltænkt, at ordningen skal revideres inden forordningen træder i kraft i maj 2018 og direktivet formelt tilbagetrækkes.[53]

I det følgende vil der redegøres for Privacy Shield princippernes anvendelse i praksis, og vurderes, hvorvidt de harmonerer med henholdsvis persondataforordningens principper samt de principper som kan udledes af retspraksis.

4.1. Privacy Shield principperne kontra persondataforordningen

Privacy Shield blev vedtaget d. 12. juli 2016. Ordningen administreres af det amerikanske handelsministerium (Handelsministeriet), og indeholder en opt-in selv-certificeringssystem for amerikanske virksomheder.[54] I august 2017 havde ca. 2400 amerikanske virksomheder tilsluttet sig ordningen.[55] Når amerikanske virksomheder har tilsluttet sig ordningen bliver de straks underkastet principperne, med en enkel undtagelse i forbindelse med videreoverførsel,[56] som gennemgås neden for.

Privacy Shield består af 7 principper og 16 supplerende principper. Principperne vedrør (1) oplysningspligt, (2) valgfrihed, (3) ansvar for videreoverførsler, (4) sikkerhed, (5) dataintegritet og formålsbegrænsning, (6) indsigt samt (7) klageadgang, håndhævelse og ansvar.[57] De supplerende principper vil ikke være genstand for selvstændig behandling i denne afhandling, men vil inddrages i det omfang de findes relevante til at understøtte forståelsen af de 7 hovedprincipper.

4.1.1. Princippet om oplysningspligt

Under princippet om oplysningspligt er virksomheder forpligtet til at give den registrerede informationer om en række nøgleelementer vedrørende databehandlingen. Det kan vedrør oplysning om, hvilke typer data er indsamlet, formålet med indsamlingen og behandlingen samt oplyse om rettigheder, herunder ret til indsigt og valgfrihed. Virksomheder skal oplyse om deres privatlivspolitik ved at

[52] Peter Blume: Retlig Regulering af Internationale Persondataoverførsler, 1. udgave, 2006, side 93, note 23.
[53] IT Governance Privacy Team (Alan Calder, Richard Campo, Adrian Ross): EU General Data Protection Regulation (GDPR), An Implementation and Compliance Guideline, 2016, side 234.
[54] Commission Implementing Decision (2016) 4176 final, punkt 2, (14) og (18).
[55] Link: https://www.privacyshield.gov/list, besøgt d. 14.08.2017, kl. 09.30.
[56] Commission Implementing Decision (2016) 4176 final, punkt 2, (17).
[57] Ibid., punkt 2.1.

gøre dem tilgængelige for offentligheden, og henvise til Handelsministeriets hjemmeside, Privacy Shield Listen og hjemmesiden for det relevante tvisteløsningsorgan.[58] Oplysningen skal angive den myndighed, der har håndhævelsesbeføjelserne i forhold til overholdelse af principperne. Det kræves også, at virksomheden oplyser om identiteten af en eventuel tredjepart, hvis denne tredjepart har fået videregivet oplysningerne, samt om formålet bag videregivelsen.[59]

4.1.1.1. Princippets sammenspil med forordningen

Princippet om oplysningspligt er i persondataforordningen delt op i to situationer. På den ene side, hvor indsamlingen af personoplysninger sker direkte hos den registrerede (artikel 13), og på den anden side, hvor indsamlingen af personoplysninger sker andre steder end hos den registrerede (artikel 14). Denne sondring lader ikke til at være tilfældet i Privacy Shield. Fordele og ulemper ved en sådan sondring kan diskuteres, men det kan siges, at grundet den teknologiske udviklings indflydelse på måden for indsamling af oplysninger er det mest hensigtsmæssigt at samle situationerne i én bestemmelse og dermed ikke foretage en sondring. Dette skyldes at det i høj grad er muligt at identificere personer på baggrund af oplysninger, der i forvejen er offentligt tilgængelige flere steder, og uden at den registrerede selv aktivt har givet oplysningerne.[60] Grænserne for direkte og indirekte indsamling er flydende, og det er derfor ikke nødvendigvis en ulempe og en svækkelse af transparens, at Privacy Shield ikke ligesom persondataforordningen sondrer mellem de to situationer. Det skal alligevel bemærkes, at forordningens artikel 13 og 14 er meget mere detaljeret end Privacy Shield i sine krav til oplysningspligtens indhold. En sammenligning mellem ordlyden i artikel 13 og 14 og Privacy Shield princippet om oplysningspligt viser, at persondataforordningen stiller det krav, at oplysningspligten skal opfyldes på det tidspunkt, der sker indsamling af personoplysningen (enten direkte eller indirekte). Derimod nævner Privacy Shield bilag 2.I.b, at oplysningspligten skal gives på det tidspunkt den registrerede anmodes om at give personoplysningerne til virksomheden (direkte). Ud fra en ordlydsfortolkning må det siges, at oplysningspligten i Privacy Shield ikke kræves opfyldt ved indirekte indsamlinger, eftersom den slet ikke nævner disse situationer eller ovennævnte sondring. Dette kan være problematisk da indirekte indsamlinger er højt forekommende i især den offentlige sektor,[61] og det var især indirekte indsamling af personlige oplysninger af den amerikanske efterretningstjeneste, der var grundlaget for Schrems-dommen.[62]

Derudover indeholder Privacy Shield ikke en bestemmelse om, at den registrerede skal have oplysninger om eventuelle datasikkerhedsbrud. Dette er derimod indehold i forordningens artikel 34, hvilket må siges at være begrundet i ønsket om større transparens.

4.1.1.2. Kritikpunkter fra Artikel 29-Gruppen

Artikel 29-Gruppen anfører, at princippet mangler krav om oplysning af øvrige rettigheder end de rettigheder Privacy Shield nævnte. Princippet skal være mere eksplicit og endvidere henvise til retten til at rette og slette oplysninger.[63] Privacy Shields uoverskuelighed og manglende klarhed i sin ordlyd er et generelt kritikpunkt fra Gruppens side.[64]

Gruppen anfører ligeledes et kritikpunkt vedrørende kravet om tidspunktet for opfyldelse af oplysningspligten. Det fremgår af Privacy Shield bilag 2, II.1.b, at oplysning først skal gives når individer bliver bedt om at give personlige oplysninger til virksomheden eller umiddelbart i forlængelse heraf.

---

[58] Ibid., punkt 2.1, (20).
[59] Ibid., Bilag 2.II.1.
[60] Peter Blume: Persondataretlige Grundfigurer, 1. udgave, 2017, s. 100.
[61] Ibid.
[62] C-362/14 Schrems mod Data Protection Commissioner, præmis 26-30.
[63] 16/EN WP 238: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, punkt 2.2.1.a.
[64] Ibid., punkt 1.2.2.

Under alle omstændigheder skal oplysninger gives før virksomheden bruger sådanne oplysninger til et andet formål end det oprindelige formål eller før der sker videregivelse. Kritikken går på, at princippet ikke tager højde for, at den amerikanske virksomhed modtager disse personoplysninger fra en europæisk virksomhed, og ikke selv kontakter den registrerede og beder denne om at give oplysninger. Privacy Shield virksomhederne foretager dermed ikke en direkte indsamling af persondata fra den registrerede. Tidspunktet for oplysningspligten burde derfor være det tidspunkt Privacy Shield virksomheden registrerer/indsamler personoplysningen, uanset om dette sker direkte eller indirekte.[65]

4.1.1.3. Afhandlingens anbefaling til revideringen

I forbindelse med den første årlige revidering må Kommissionen nå frem til, at det i Privacy Shield skal præciseres, at oplysningspligten skal opfyldes på det tidspunkt virksomheden registrerer/indsamler personoplysningen om borgeren, uanset at der er tale om en direkte eller indirekte registrering.

4.1.2. Princippet om valgfrihed

Under princippet om valgfrihed skal virksomheder tilbyde den registrerede muligheden for at vælge, hvorvidt deres personlige oplysninger tilgængeliggøres for en tredjepart eller bruges til et andet formål end det formål der oprindeligt blev oplyst til og godkendt af den registrerede. Dette princip udtrykker den registreredes ret til opt-out.[66] Modsat princippet om oplysningspligt indeholder princippet om valgfrihed ikke nogen krav om at den registrerede skal have mulighed for opt-out når der sker videregivelse til en tredjepart. Denne modsætning gælder kun i de tilfælde tredjeparten fungerer som en mellemmand, der udfører opgaver på vegne af virksomheden og hvor virksomheden har ledelsesretten over mellemmanden.[67] Dette kan skyldes, at ledelsesretten, som omtalt i afsnit 2.1.1, kan indikere, at der ikke er sket en egentlig overførsel i persondataforordningens forstand.

Princippet indeholder også en opt-in mulighed for den registrerede, når der er tale om behandling af følsomme oplysninger (oplysninger der vedrør medicin, helbred, race, etnicitet, seksualitet, politiske anskuelser, religiøs overbevisning og fagforeningsmedlemsskab). I sådanne tilfælde skal virksomheder indhente samtykke til behandlingen, hvis sådanne følsomme oplysninger tilgængeliggøres for en tredjepart eller bruges til et andet formål end det oprindeligt oplyste.[68]

Valgfrihedsprincippet indeholder således en opt-out mulighed, hvor den registrerede kan modsætte sig en behandling, og en opt-in mulighed, hvor den registrerede i visse tilfælde skal tillade en behandling før den lovligt kan fuldføres.

4.1.2.1. Princippets sammenspil med forordningen

Princippet om valgfrihed suppleres af det supplerende Princip 12, der siger at borgere altid har ret til opt-out i forbindelse med direkte markedsføring – dog med den undtagelse at man må tåle en vis tidsfrist.

Persondataforordningens artikel 21 stk.2 og artikel 22 stk.1 tillader den registrerede at fravælge muligheden for både at være genstand for direkte markedsføring og en automatiseret individuel afgørelse, herunder i form af profilering. Privacy Shield anvender derimod ikke udtrykket *profilering*, men anvender i stedet kun formuleringen *direkte markedsføring.* Privacy Shields opt-out mulighed i valgfrihedsprincippet er dermed kun en rettighed for borgeren til at fravælge at være genstand for direkte markedsføring. Rettigheden gælder, modsat i persondataforordningen, ikke ved profilering.

---

[65] Ibid., punkt 2.2.1. a.
[66] Commission Implementing Decision (2016) 4176 final, punkt 2.1, (22).
[67] Commission Implementing Decision (2016) 4176 final, Bilag 2, punkt II.2.
[68] Ibid., Bilag 2 punkt II.2.b.

4.1.2.2. Kritikpunkter fra Artikel 29-Gruppen

Gruppen bemærker at opt-out muligheden, udover i forbindelse med direkte markedsføring, ikke giver nogle detaljerede beskrivelser af, hvornår og hvordan sådan en opt-out mulighed skal udnyttes. Gruppen anfører, at virksomheden aktivt bør tilbyde den registrerede at anvende sin opt-out mulighed før genbrugen af oplysningerne eller før videregivelsen.[69] I sådanne tilfælde har den registrerede mulighed for at give et specifikt samtykke, der direkte tager stilling den konkrete databehandling og dermed i højere grad opfylder samtykke definitionen i persondataforordningens artikel 4 stk. nr.11, hvorefter et samtykke skal være frivilligt, specifikt, informeret og utvetydigt. Hvis samtykket til databehandlingen først blev givet på tidspunktet for oplysningspligtens opfyldelse, og dermed før opt-out muligheden blev praktisk aktuel, ville samtykket have rettet sig mod databehandlingen i sin helhed og ikke specifikt til videregivelsen eller det nye formål.

Gruppens kritik skal også ses i sammenhæng med den generelle kritik om, at Privacy Shield ikke er klar i sin ordlyd og flere steder nøjes med blot at nævne hvilke rettigheder den registrerede har, men uden at beskrive hvordan rettighederne udnyttes. Gruppen udtaler fx, at det er uvist og uklart, hvornår et formål er materielt uforeneligt med det oprindelige formål. Løsningen herpå kunne være at indsætte et krav om, at det nye formål skal være sammenligneligt og foreneligt med det oprindelige formål.[70]

4.1.2.3. Afhandlingens anbefaling til revideringen

Kommissionen må nå frem til, at valgfrihedsprincippet også gælder ved profilering og ikke kun ved direkte markedsføring. Dermed tager man højde for at borgeren ikke skal være genstand for automatiserede afgørelser baseret på sine personoplysninger. Derudover bør man indføre reglen om, at opt-out muligheden skal tilbydes før der sker genbrug eller videreoverførsel af personoplysninger, da man i så fald vil være tættere på at overholde samtykkekravet i persondataforordningen.

4.1.3. Princippet om ansvar for videreoverførsler

Princippet om ansvar for videreoverførsler indebærer, at en virksomhed er ansvarlig for at tredjeparten overholder Privacy Shield principperne.[71]

I bilagene til Privacy Shield har Handelsministeriet præciseret kravet til opfyldelse af princippet. Handelsministeriet sondrer mellem videreoverførsler til en tredjepart, der handler som en selvstændig dataansvarlig, og videreoverførsler til en tredjepart, der handler som en mellemmand på vegne af Privacy Shield virksomheden.[72]

I første situation, videreoverførsler til en ny dataansvarlig, kræves det, at virksomheden i forbindelse med videreoverførsler skal overholde princippet om oplysningspligt og valgfrihed. Virksomheden skal ved kontraktindgåelse forpligte tredjeparten til at foretage databehandling i overensstemmelse med datasubjektets samtykke og stille garanti for, at kontrakten opfylder samme beskyttelsesniveau som Privacy Shield principperne. Kontrakten mellem virksomheden og tredjeparten skal også forpligte tredjeparten til at underrette virksomheden i tilfælde af, at tredjeparten konkluderer, at denne ikke længere kan opfylde principperne. Kontrakten skal i sådanne tilfælde indeholde adgang til foranstaltninger, der kan bringe behandlingen til ophør eller tage nødvendige og rimelige remedier i brug.[73]

I den anden situation, videreoverførsler til en mellemmand, må virksomheden kun overføre personoplysninger til begrænsede og specifikke formål, og garantere at mellemmanden er forpligtet til at

[69] 16/EN WP 238: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, punkt 2.2.2.
[70] 16/EN WP 238: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, punkt 2.2.2.
[71] Commission Implementing Decision (2016) 4176 final, punkt 2.1, (28).
[72] Ibid., Bilag 2, punkt II, nr.3.
[73] Commission Implementing Decision (2016) 4176 final, Bilag 2, punkt II.3.a.

yde mindst samme beskyttelsesniveau som Privacy Shield. Derudover skal virksomheden sørge for, at mellemmanden tager rimelige og nødvendige foranstaltninger i brug for at sikre at mellemmanden effektivt behandler oplysningerne på en måde, der er forenelig med virksomhedens forpligtelser under Privacy Shield. Virksomheden skal forpligte mellemmanden at underrette virksomheden i tilfælde af manglende overholdelse af principperne. Mellemmanden skal også kræves at tage nødvendige og rimelige foranstaltninger i brug for at stoppe en uautoriseret databehandling, og tilvejebringe en gengivelse eller kopi af relevante bestemmelser i kontrakten til Handelsministeriet ved ministeriets anmodning.[74]

Den væsentlige forskel mellem de to situationer er således, at mellemmanden ikke er forpligtet til at foretage en databehandling i overensstemmelse med den registreredes samtykke. Der kan altså ske databehandling til opfyldelse af et andet formål end det formål, der oprindelige blev samtykket til. Der er dog fortsat et krav om, at der skal være et specifikt og begrænset formål i kontrakten mellem Privacy Shield virksomheden og mellemmanden. Grundet til denne forskel er som nævnt oven for under princippet om valgfrihed, at ledelsesretten taler imod, at der er sket en egentlig overførsel, men derimod en videregivelse til en mellemmand, som er under virksomhedens ledelsesret. Det er dog uvist, hvordan den registrerede står i tilfælde af videregivelse af personfølsomme oplysninger til en mellemmand, og om der i disse tilfælde gælder en opt-in mulighed.

Kommissionen skriver, at princippet om ansvar for videreoverførsel skal læses i sammenhæng med princippet om oplysningspligt og valgfrihed. Det kan derfor tænkes, at opt-in muligheden ved behandling af personfølsomme oplysninger også gælder ved videregivelse af oplysninger til en mellemmand eftersom mellemmandens behandling ikke forudsætter, at denne opfylder præcist samme formål som der oprindeligt blev samtykket til, men forudsætter derimod at opfylde et begrænset og specifikt formål aftalt mellem mellemmanden og virksomheden.

Som nævnt under punkt 4.1 er det klare udgangspunkt, at Privacy Shield principperne gælder straks efter selvcertificeringen, og at der findes en særlig undtagelse ved videregivelse af personoplysninger. I sådanne tilfælde, videregivelse af oplysninger, vil Privacy Shield virksomheden og tredjeparten typisk have tidligere kommercielle kontrakter imellem sig, og det kan tage tid at få disse kontrakter harmoneret med Privacy Shield principperne. Derfor tillader man en tidsperiode på maksimum 9 måneder for at tredjeparten kan rette sig efter principperne. Under denne tidsperiode er virksomheden dog forpligtet til at opfylde sin oplysningspligt og princippet om valgfrihed, sådan at den registrerede kan tage stilling til, om man vil acceptere overførslen. På denne måde sikres på den ene side den registreredes databeskyttelsesret og på anden side virksomhedernes behov for en rimelig tidsfrist til at harmonere interne politikker og eksterne kommercielle forhold med Privacy Shield.[75]

4.1.3.1. Princippets sammenspil med forordningen

Privacy Shield er som nævnt skrevet på baggrund af persondatadirektivet. Følgende vil Privacy Shield princippet om ansvar for videreoverførsler dog læses i sammenhæng med persondataforordningens regler om overførsler i forordningens kapitel 5, der er nærmere gennemgået i denne afhandlings afsnit 2.2, med henblik på at klargør, i hvilket omfang princippets praktiske anvendelse harmonerer med princippets anvendelse i persondataforordningen.

Det er i denne forbindelse værd at henvise til forordningens artikel 44, der fastsætter det generelle princip, at enhver overførsel, herunder videreoverførsler, til et tredjeland kun må finde sted, hvis forordningens øvrige betingelser er opfyldt, og hvis der trods videreoverførslen kan garanteres et

[74] Ibid., Bilag 2, punkt II.3.b.
[75] Commission Implementing Decision (2016) 4176 final, punkt 2, (17).

tilstrækkeligt beskyttelsesniveau. I tilfælde af, at videreoverførslen sker fra Privacy Shield virksomheden til et tredjeland, der mangler afgørelse om tilstrækkeligheden af beskyttelsesniveau, kan videreoverførslen til dette tredjeland kun finde sted, hvis betingelserne i artikel 49 er opfyldt. Mest relevant i denne sammenhæng er betingelsen om, at den registrerede skal have givet sit samtykke til selve overførslen jf. artikel 49 stk. 1 (a). Dette er modsat Privacy Shield, hvori kravet er, at videreoverførsler kan ske ved en aftale mellem virksomheden og tredjeparten om, at behandlingen skal ske i overensstemmelse med den registreredes oprindelige samtykke. Der kræves i Privacy Shield således ikke, at der indhentes selvstændigt samtykke til videreoverførsler. Man tager i stedet udgangspunkt i den registreredes oprindelige samtykke, mens der i forordningen kræves et nyt samtykke til (videre)overførslen.

4.1.3.2. Kritikpunkter fra Artikel 29-Gruppen

Artikel 29-Gruppen har kritiseret princippet om ansvar for videreoverførsler med at princippets anvendelse afhænger af, hvorvidt der sker videreoverførsler til henholdsvis en ny dataansvarlig (controller) eller en databehandler (processor/agent). Kritikken retter sig særligt mod, at der stilles forskellige krav for, hvornår en videreoverførsel accepteres, alt efter om det er en dataansvarlig eller databehandler, der modtager overførslen.

4.1.3.2.1. Bekymringer i forhold til videreoverførsler til en dataansvarlig

Ved videreoverførsler til et tredjeland uden for EU til en ny dataansvarlig i dette tredjeland udtales det, at man bør indsætte en klar henvisning til formålsbegrænsningsprincippet. Dermed gøres det klart, at videreoverførsler ikke tillades hvor tredjeparten (den dataansvarlige i tredjelandet) har til hensigt at behandle personoplysningerne med et inkompatibelt formål. Det er en klar forbedring i forhold til den dagældende Safe Harbor, at der nu kræves en kontrakt før der tillades videreoverførsler.[76] Det kan dog være problematisk, at sådan en kontrakt ikke kræves ved koncerninterne overførsler. I sådanne situationer henvises der til BVR eller andre koncerninstrumenter såsom compliance- og kontrol programmer.[77] Sådanne andre instrumenter garanterer ikke et retligt bindende instrument med hjemmel i europæisk databeskyttelsesret. Det kan derfor tænkes, at Privacy Shields henvisning til andre koncerninstrumenter vil bruges til at undvige kravet om et retligt bindende instrument.[78]

4.1.3.2.2. Bekymringer i forhold til videreoverførsler til en databehandler

Ved videreoverførsler til en databehandler i et tredjeland kræves der også en kontrakt, uanset om databehandleren er underlagt Privacy Shield eller en anden tilstrækkelighedsvurdering. Gruppen kritiserer dog den utilstrækkelige rækkevidde af Privacy Shields regler om ansvar for databehandleren. Det er særligt kritisabelt, at ordningens Bilag 2, II.7.b, som fastlægger virksomhedens ansvar for databehandlerens skadevoldende handlinger, ikke finder anvendelse i de tilfælde virksomheden har valgt at samarbejde med en databeskyttelsesmyndighed jf. Bilag 2, III.5.a. in fine. En sådan undtagelse virker ubegrundet.[79]

Princippet mangler en klar henvisning til formålsbegrænsningsprincippet, der skal klargøre, at databehandlerens formål skal være kompatibelt med virksomhedens oprindelige formål. Det bør dermed ikke være tilstrækkeligt, at formålet skal være specifikt og begrænset, men skal ligeledes være kompatibelt med Privacy Shield virksomhedens oprindelige formål.

En særlig situation opstår, hvor Privacy Shield virksomheden agerer som en databehandler på vegne af den europæiske virksomhed. Her skal det være klart for den nye databehandler i tredjelandet, der

[76] 16/EN WP 238: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, punkt 2.2.3.b.
[77] Commission Implementing Decision (2016) 4176 final, Bilag 2, punkt III.10.B.
[78] 16/EN WP 238: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, punkt 2.2.3.b.
[79] Ibid., punkt 2.2.3.c.

modtager oplysningerne, at det er kontrakten mellem Privacy Shield virksomheden og EU-virksomheden der giver hjemmel for videreoverførslen. Tredjeparten vil naturligvis have den formodning, at Privacy Shield virksomheden har kompetence til at videreoverføre persondata af egen fri vilje. Dette brister EU-virksomhedens ledelsesret. Der mangler derfor klare regler for at lukke denne form for smuthul, hvilket vil gøre det klart for tredjeparten, at det er EU-virksomheden, der er ansvarlig for videreoverførslen og ikke Privacy Shield virksomheden.[80]

4.1.3.3. Afhandlingens anbefaling til revideringen

Kommissionen bør revidere princippet til, at der skal gives nyt samtykke til videreoverførslen i stedet for, at man læner sig op ad det oprindelige samtykke, der blev givet til overførslen til USA. Derudover bør der indsættes et krav om, at formålet med videreoverførslen skal være kompatibelt med det oprindelige formål og ikke blot at formålet skal være specifikt og begrænset. Med sådan en revidering vil der i højere grad være tale om et informeret, specifikt og utvetydigt samtykke fra den registreredes side.

4.1.4. Princippet om sikkerhed

Under princippet om sikkerhed skal virksomheder, taget den store risiko og karakteren af personoplysningerne i betragtning, tage nødvendige og rimelige sikkerhedsforanstaltning i brug. Dette er med henblik på at hindre tab, misbrug og uautoriseret behandling, afsløring, ændring og destruering.[81]

4.1.4.1. Princippets sammenspil med forordningen og afhandlingens anbefaling til revideringen

Persondataforordningen stiller ligeledes krav til virksomhedernes sikkerhedsforanstaltninger. Modsat Privacy Shield stilles der i forordningens artikel 35 og betragtning nr. 84 krav om at foretage en konsekvensanalyse af databehandlingen. Resultatet heraf skal tages i betragtning inden der besluttes en sikkerhedsforanstaltning. Viser resultatet at der er en høj risiko for databrud og brud på den registreredes rettigheder og friheder skal tilsynsmyndighederne høres. Kommissionen bør derfor revidere princippet til, at tilsynsmyndigheder skal inddrages i forbindelse med igangsættelse af sikkerhedsforanstaltninger.

4.1.4.2. Kritikpunkter fra Artikel 29-Gruppen og afhandlingens anbefaling til revideringen

Modsat se øvrige principper har Gruppen ikke taget dette princip til særskilt behandling i sin udtalelse. Det må dog siges, at Gruppens generelle kritik om, at Privacy Shield ikke er klar nok i sin ordlyd og ofte nøjes med at nævne rettigheder i stedet for at uddybe og stille krav til rettighedernes anvendelse, også kan rettes mod princippet om sikkerhed. Ordningen behandler ikke spørgsmålet om, hvornår en sikkerhedsforanstaltning er rimelig og nødvendig, og om der stilles skærpede krav til sikkerhedsforanstaltninger ved særlige personfølsomme oplysninger. Der mangler krav om konsekvensanalyse og henvisning til datamyndighedernes rolle, hvilket Kommissionen bør inddrage i revideringen.

4.1.5. Princippet om dataintegritet og formålsbegrænsning

Indholdet af personlige oplysninger skal begrænses til det indhold der er relevant for formålet bag behandlingen. En virksomhed må ikke foretage en databehandling på en måde, der er uforeneligt med det formål som den registrerede har samtykket til. Virksomheden skal træffe nødvendige foranstaltninger for at sikre, at personoplysningerne er anvendelige og passende til det tilsigtede brug, at de er korrekte, fuldstændige og retvisende. En virksomhed skal overholde principperne så længe den er i besiddelse af personoplysningerne. Princippet forhindrer ikke virksomheder i at fortsætte databehandlingen i en længere periode, når det oprindelige formål er opnået. Dette gælder dog kun i tilfælde

[80] 16/EN WP 238: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, punkt 2.2.3.c.
[81] Commission Implementing Decision (2016) 4176 final, Bilag 2, punkt II.4.

af arkivering i den offentlige interesse, journalistik, litteratur og kunst, videnskabs- og historieforskning samt til statistisk og analytisk brug. De øvrige principper finder dog fortsat anvendelse i sådanne situationer.[82]

4.1.5.1. Princippets sammenspil med forordningen

Princippet om dataintegritet og formålsbestemthed findes i persondataforordningens artikel 5. Princippet tager sigte på at sikre transparens forstået på den måde, at den registrerede skal have mulighed for at forudse, hvad personoplysningerne bliver brugt til.[83] Den registreredes forudberegnelighed er altså med til at sikre transparensen. Denne forudberegnelighed må siges i højere grad at være sikret i persondataforordningen end i Privacy Shield. Forordningens artikel 5 stk.1 (c) angiver princippet om dataminimering. Bestemmelsen siger, at personoplysninger skal være tilstrækkelige, relevante og begrænses til hvad der er *nødvendigt* i forhold til det oprindelige behandlingsformål. Privacy Shield princippet indeholder ikke et krav om nødvendighed, men et krav om at personoplysninger skal være relevante. Dette må siges at give en lavere grad af forudberegnelighed for den registrerede, end hvad der kræves i persondataforordningen.

Persondataforordningens regel om arkiveringsformål i artikel 5 stk.1 (e) kræver, at der kun må opbevares personoplysninger til arkiveringsformål, hvis arkiveringen alene sker i samfundets interesse eller øvrige hensyn, som er oplistet i bestemmelsen. Privacy Shield opstiller det samme krav, men modsat persondataforordningen stiller Privacy Shield ikke krav om, at der implementeres passende tekniske og organisatoriske foranstaltninger for at sikre den registreredes rettigheder og friheder.

4.1.5.2. Kritikpunkter fra Artikel 29-Gruppen

Selvom en virksomhed opfylder principperne om oplysning og valgfrihed kan databehandlingen alligevel være i strid med proportionalitetsprincippet.[84] Kravet om, at personoplysninger skal begrænses til, hvad der er relevant for behandlingen giver ikke den registrerede en stærk nok beskyttelse mod uproportionelle databehandlinger.[85] Kravet bør i stedet ændres til, at personoplysninger begrænses til hvad der er nødvendigt for databehandlingen. Dette understøttes af, at proportionalitetsprincippet i både EMRK artikel 8 og Charteret artikel 8 specifikt indeholder krav om nødvendighed.

Artikel 29-Gruppen kritiserer særligt den forvirrende og inkonsistente ordvalg i dataintegritet & formålsbegrænsningsprincippet og valgfrihedsprincippet. Formålsbegrænsningsprincip siger, at persondata ikke må behandles på en måde, der er uforeneligt med det oprindelige formål, mens valgfrihedsprincippet stiller en opt-out mulighed for den registrerede, hvis dette er tilfældet. Dette kunne skabe troen, at valgfrihedsprincippet er en undtagelse til formålsbegrænsningsprincippet, hvilket ikke er tilfældet, og ville i så fald autorisere en videre adgang til inkompatible databehandlinger, end hvad der var tiltænkt med principperne.[86]

4.1.5.3. Afhandlingens anbefaling til revideringen

For at sikre mest muligt transparens og forudberegnelighed bør Kommissionen indføre reglen om dataminimering som i persondataforordningens artikel 5 strk.1 (c), der angiver, at personoplysninger begrænses til, hvad der er nødvendigt for det oprindelige behandlingsformål, og ikke blot hvad der er relevant. Dermed gøres princippet ikke bare konformt med persondataforordningen, men også med EMRK og Charteret.

---

[82] Commission Implementing Decision (2016) 4176 final, punkt 2.1, (23).
[83] Peter Blume: Den Nye Persondataret, 1. udgave, 2016, s. 71.
[84] WP 29 letter to Vice-President Redin, 10 April 2014, side 8.
[85] 16/EN WP 238: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, punkt 2.2.4.a.
[86] Ibid, punkt 2.2.4.c.

4.1.6. Princippet om indsigt

Den registrerede skal have mulighed for at få indsigt i de personlige oplysninger, der vedrør den registrerede, og som virksomheden er i besiddelse af. De skal have mulighed for at korrigere, tilføje og slette oplysninger, hvor disse er ukorrekte eller har været genstand for en krænkende databehandling. Dette kan dog ikke ske, hvis udgifterne forbundet med indsigt vil være uproportionelle i forhold til risikoen for at krænke den registreredes ret til privatliv. Et hvert andet afslag på indsigt skal begrundes i helt særlige omstændigheder. Her har virksomheden bevisbyrden. I USA anvendes forskellige lovgivninger inden for specifikke sektorer, som regulerer virksomhedernes beslutninger om at tillade indsigt. Kommissionen har givet udtryk for, at den anerkender problemer med mangelfuld amerikansk lovgivning på dette område. Man påpeger, at sektorlovgivningens regler om indsigt ikke er holdbar taget den moderne digitale økonomi i betragtning, og at reglerne om indsigt er en af de første områder, som skal revideres.[87]

4.1.6.1. Princippets sammenspil med forordningen

Persondataforordningens regler om indsigt findes i artikel 15. Bestemmelsen angiver hvilke oplysninger den registrerede kan kræve at få indsigt i. Den indeholder undtagelser til indsigtsretten. Undtagelserne til artikel 17 om retten til sletning bliver dog relevante for indsigtsretten, da ønsket om at få slettet oplysninger typisk først vil blive aktuelt efter at den registrerede, som følge af indsigten, er blevet bekendt med hvilke oplysninger virksomheden er i besiddelse af. Privacy Shields undtagelse til indsigt ved uproportionelle udgifter er dermed uforeneligt med forordningen, da denne undtagelse hverken er nævnt i forordningens artikel 15 om indsigt, artikel 16 om berigtigelse eller artikel 17 om sletning.

En særlig bestemmelse er forordningens artikel 15 stk.3. Denne indeholder reglen om, at den registrerede har ret til at modtage en kopi af de oplysninger virksomheden er i besiddelse af. Reglen skal ses i sammenhæng med den nye rettighed i persondataforordningen, retten til dataportabilitet i artikel 20. Retten til dataportabilitet er ikke en rettighed i Privacy Shield, hvilket er et af de væsentligste forskelle mellem de to regelsæt.

4.1.6.2. Kritikpunkter fra Artikel 29-Gruppen

Et væsentligt kritikpunkt fra Gruppen retter sig mod det supplerende Princip 8, der siger, at indsigt kun gives i personoplysninger, der opbevares af virksomheden. Gruppen anbefaler at ændre ordlyden sådan at det gøres klart, at der gives indsigt i oplysninger, der på enhver måde blevet behandlet og ikke blot opbevaret.[88] Taget den digitale tidsalder i betragtning lader dette til at være et fornuftigt tiltag i forbindelse med revideringen, da personoplysninger flyver tværs over landegrænser på internettet og ikke nødvendigvis opbevares i et register.

Gruppen anbefaler ligeledes, at man ved næste revidering af ordningen overvejer indførelsen af princippet om dataportabilitet.[89] Blume anfører dog, at retten til dataportabilitet er en symbolsk forbedring af databeskyttelsen for forbrugere, der kun sjældent vil udnyttes grundet rettens begrænsede anvendelsesområde og undtagelser.[90]

---

[87] Commission Implementing Decision (2016) 4176 final, punkt 2.1, (25).
[88] 16/EN WP 238: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, punkt 2.2.5.
[89] Ibid., punkt 1.2.4, side 15.
[90] Peter Blume: Den Nye Persondataret, 1. udgave, 2016, s. 144, og Persondataretlige Grundfigurer 1. udgave, 2017, side 105.

4.1.6.3. Afhandlingens anbefaling til revideringen

Privacy Shield indeholder ingen regel om dataportabilitet, men da denne rettighed formentlig ikke vil udnyttes i et betydeligt omfang, og kun betragtes som værende af symbolsk karakter, bør Kommissionen rette fokus et andet sted. En indførelse af retten til dataportabilitet vil overordnet ikke udgøre en væsentlig forbedret retsstilling for den registrerede.

Kommissionen bør fjerne undtagelsen om uproportionelle udgifter i forbindelse med indsigt og samtidig indføre en regel om, at der gives indsigt i enhver oplysning, der er blevet behandlet, og ikke blot opbevaret.

4.1.7. Princippet om klageadgang, håndhævelse og ansvar

Princippet om klageadgang, håndhævelse og ansvar relaterer sig til den registreredes adgang til effektive retsmidler i forbindelse med sikring af sin databeskyttelse. Dette princip er et af de vigtigste principper i Privacy Shield, da hele spørgsmålet om adgang til effektive retsmidler var et væsentligt moment for underkendelsen af Safe Harbor ordningen i Schrems-dommen.[91]

4.1.7.1. Virksomhedernes ansvar og forpligtelser

Når en virksomhed frivilligt har certificeret sig selv bliver den automatisk forpligtet til at sørge for effektiv overholdelse af Privacy Shield. En amerikansk virksomhed kan kun fortsætte med at modtage persondata fra europæiske virksomheder i medfør af Privacy Shield, hvis den årligt gencertificerer sig selv.[92] Gencertificeringen følger samme regler og formkrav som den originale selvcertificering. Her skal angives oplysninger om virksomheden og en beskrivelse af virksomhedens privatlivspolitikker. Der skal angive en kontaktperson i forbindelse med behandling af klager, anmodninger om indsigt og andre spørgsmål, der relaterer sig til Privacy Shield.[93]

Virksomheden skal også angive den anvendte metode for verifikation af sin Privacy Shield-compliance og overholdelse af princippet om klageadgang, håndhævelse og ansvar. Dette kan ske gennem selv-evaluering eller gennem en objektiv tilsyns- og stikprøvekontrol. Verifikation skal indikere at virksomhedens privatlivspolitikker er nøjagtige, omfattende, fremtrædende vist, komplet implementeret og tilgængelige. Evalueringen skal også indikere at virksomhedens privatlivspolitikker er i overensstemmelse med Privacy Shield, at de registrerede er informerede om ethvert internt arrangement for klagebehandling og om hvilke uafhængige mekanismer en registrerede kan benytte i forbindelse med indgivelse af klager.[94]

Hvis virksomheden frivilligt trækker sig ud af Privacy Shield eller ikke længere er omfattet af ordningen, fordi den ikke opfylder reglerne ved gencertificeringen er den fortsat underlagt Handelsministeriets tilsynsmyndighed. Formålet hermed er at verificere, hvorvidt virksomheden agter at returnerer, slette eller beholde personoplysningerne. Hvis virksomheden beholder oplysningerne er den fortsat forpligtet af Privacy Shield principperne. I de tilfælde Handelsministeriet har fjernet en virksomhed fra Privacy Shield Listen pga. virksomhedens manglende overholdelse af principperne vil Handelsministeriet sikre at virksomheden returnerer eller sletter personoplysningerne.[95]

4.1.7.2. Klagemuligheder

Den registrerede kan i første omgang klage direkte til den pågældende virksomhed. Virksomheden skal tilrettelægge en effektiv procedure i forbindelse med modtagelse af en klage. Ved modtagelse af

[91] C-362/14 Schrems mod Data Protection Commissioner, præmis 90 og 95.
[92] Commission Implementing Decision (2016) 4176 final, punkt 2.1, (26).
[93] Ibid., Bilag 2, punkt III.6.B.
[94] Ibid., Bilag 2, punkt III.7.
[95] Ibid., punkt 2.2, (34).

en klage skal virksomheden informere den registrerede om, hvem den rette kontaktperson/kontaktmyndighed er, som tager sig af klagen.[96] Virksomheder skal besvare klagen inden for 45 dage og besvarelsen skal indeholde en vurdering af klagens berettigelse og oplysninger om, hvordan virksomheden vil løse problemet.[97]

Den registrerede kan også klage direkte til et uafhængigt tvisteløsningsorgan, der er udpeget af virksomheden til at undersøge og afgøre individuelle seriøse og ikke åbenbart ugrundede klager. Organet kan enten befinde sig i EU eller USA. Organet skal have mulighed for at stille effektive sanktioner ved overtrædelser, og virksomheder skal informere Handelsministeriets hvis de ikke agter at følge organets afgørelse, med risiko for at Handelsministeriet fjerner virksomheden fra Privacy Shield Listen.[98]

Den registrerede kan som en tredje mulighed klage til en national databeskyttelsesmyndighed. Her følger almindelige forvaltningsretlige regler og virksomheder er forpligtet til at samarbejde med myndigheden. Følger virksomheden ikke myndighedens afgørelse inden for 25 dage skal myndigheden underrette Handelsministeriet, og virksomheden risikerer at blive ekskluderet fra Privacy Shield Listen.[99]

En klage kan som fjerde og femte mulighed behandles i henholdsvis Handelsministeriet eller FTC. Handelsministeriet kan behandle klager ex officio efter anmodning eller ved henvendelse fra en national uafhængig databeskyttelsesmyndighed. Her følger særlige procedurer. Handelsministeriets kompetence er, som nævnt oven for, at ekskludere virksomheder fra Privacy Shield Listen. Handelsministeriet kan også henvise virksomheder til den anden håndhævelsesmyndighed, FTC, hvis virksomheden fastholder, at det overholder Privacy Shield principperne. FTC træffer i deres undersøgelses- og håndhævelsesbeføjelser afgørelser om, hvorvidt Section 5 i Federal Trade Commision Act[100] er overtrådt ved brud på Privacy Shield principperne. FTC har ikke kompetence til at foretage in-house kontrol, men har beføjelser til at kræve dokumenter udleveret og indhente vidneinterviews. FTC kan gennem administrative afgørelser håndhæve overholdelsen, og vil systematisk overvåge overholdelsen af disse afgørelser. Hvis virksomheden ikke følger afgørelsen kan FTC henvise sagen til den kompetence domstol.[101]

Som en sjette og sidste mulighed kan den registrerede udnytte en bindende voldgiftklausul hos Privacy Shield Panelet. Muligheden herfor skal også fremgå i opfyldelsen af princippet om oplysningspligten. Panelet består af voldgiftsmænd udpeget af Handelsministeriet og Kommissionen. I forbindelse med voldgiften gælder almindelige voldgiftsretlige regler. Selv om klageren har mulighed for at udnytte andre klagemidler kan Panelet acceptere voldgift, hvis den finder de øvrige klagemidler for utilstrækkelige i den konkrete sag.[102] Voldgiften kan derfor ses som en slags generalklausul eller sikkerhedsventil.

[96] Ibid., punkt 2.3, (43).
[97] Commission Implementing Decision (2016) 4176 final, punkt 2.3, (44).
[98] Ibid., punkt 2.3, (45) og (47).
[99] Ibid., punkt 2.3, (48) og (49).
[100] Section 5 forbyder virksomheder at engagere sig i uretfærdige eller vildledende handlinger eller praksis i ''interstate commerce''.
[101] Commission Implementing Decision (2016) 4176 final, punkt 2.3, (52-55).
[102] Commission Implementing Decision (2016) 4176 final, punkt 2.3, (56-58).

Som noget helt nyt kan EU-borgere henvende sig til en national databeskyttelsesmyndighed, der på borgerens vegne indgiver en klage til en Privacy Shield Ombudsmand, der er en amerikansk databeskyttelsesmyndighed, som varetager klager og bekymringer over efterretningstjenesternes indsamling af persondata.[103]

Det skal også nævnes, at der findes oprejsningsmuligheder i de forskellige staters og sektorers lovgivninger, som indeholder bestemmelser om retsmidler under erstatningsretten og i forbindelse med brud på forbruger eller markedsretlige forhold.[104]

Det er som nævnt Handelsministeriet, der administrerer Privacy Shield, og på baggrund af ovennævnte klagemuligheder og tilsynskontrollen har Kommissionen vurderet, at USA i sin helhed sikrer et niveau af persondatabeskyttelse, der i det væsentlige svarer til det niveau, der er garanteret ved de grundlæggende principper i persondatadirektivet. Spørgsmålet er dog, i hvor stort et omfang beskyttelsesniveauet i det væsentlige svarer til det niveau, der er garanteret ved de grundlæggende principper i persondataforordningen.

4.1.7.3. Princippets sammenspil med forordningen

Persondataforordningens tilsyns- og håndhævelsesregler findes i forordningens kapitel 6 og 7. Forordningens artikel 51 kræver, at den enkelte medlemsstat etablerer et eller flere uafhængige datatilsyn. De enkelte datatilsyn er forpligtet til at fremme den harmonisering, der er en af forordningens målsætninger jf. forordningens betragtning nr.123. Der er i afsnit 4.1.7.2 redegjort for de forskellige tilsyns- og klagemuligheder i USA. USA's mange datatilsyn skyldes landets føderale system.[105] Forordningen kræver i sådanne tilfælde, at et af disse datatilsyn skal være kontaktpunkt i forhold til EU jf. forordningens betragtning nr.119. I USA er dette tilfældet for Privacy Shield Ombudsmanden, der modtager klager fra EU-staters nationale tilsynsmyndigheder på vegne af EU-borgere. Dette gør sig også gældende for klager til Handelsministeriet. Forskellen mellem disse to myndigheder ligger i deres kompetencer.

4.1.7.4. Kritikpunkter fra Artikel 29-Gruppen

Gruppen anbefaler at lade europæiske databeskyttelsesmyndigheder repræsentere borgerne i voldgiftssager, og kritiserer, at Privacy Shield generelt mangler faste og mere klare regler om de europæiske databeskyttelsesmyndigheders rolle og funktion i forhold til de amerikanske myndigheder. Det er også kritisabelt at Privacy Shield ikke giver et svar på, hvad de amerikanske myndigheder præcist har af beføjelse i forhold til stikprøvekontroller (on-site investigations).[106] Gruppen anerkender USA's detaljerede håndhævelsesregler, men kritiserer, at disse ikke retter sig mod USA's overvågningsprogram, som var grundlaget for underkendelsen af Safe Harbor.[107]

EMD har tidligere udtalt, enhver europæisk borger skal have mulighed for at gå rettens vej, hvis der er anledning til at tro at der er sket en krænkelse af deres fundamentale rettigheder.[108] Derfor er det særligt kritisabelt, at amerikansk privatlivsbeskyttelse på føderalt niveau ikke beskytter ikke-amerikanske statsborgere eller personer som ikke er fast bosatte i USA.[109] Dette er med til at skærpe kravet om effektive retsmidler, og der må derfor være særlige omstændigheder til stede for at tolerere USA som et tilstrækkeligt tredjeland. Derfor anses det som positivt, at der er oprettet en Privacy Shield

[103] Ibid., Bilag 3, A.
[104] Ibid., punkt 2.3, (59) analogt.
[105] Peter Blume: Den Nye Persondataret, 1. udgave, 2016, s. 146.
[106] 16/EN WP 238: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, punkt 2.2.6.c, side 29.
[107] Ibid., punkt 3.3.4, side 42.
[108] Zakharov mod Rusland, 47143/06, 04.12.2015, præmis 171.
[109] 16/EN WP 238: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, punkt 3.5.1.1, side 43.

Ombudsmand, som er den største nyskabelse til spørgsmålet om retsmidler sammenlignet med Safe Harbor. Det er dog uklart i ordningens ordlyd, hvor langt Ombudsmandens kompetence rækker og om det kun er EU-borgere, der kan klage til Ombudsmanden via deres nationale databeskyttelsesmyndigheder. Dette ville Gruppen i så fald finde uacceptabelt.[110] Derudover er Gruppen skeptiske omkring Ombudsmandens uafhængighed grundet proceduren for dennes udvælgelse og afskedigelse.[111] Det er samtidig uklart, hvor stor en adgang til relevante oplysninger Ombudsmanden kan tiltvinge sig hos de forskellige myndigheder og virksomheder i forbindelse med behandling af en klage.[112] Ombudsmanden må anses at for være et meget mere effektivt retsmiddel, hvis denne havde mulighed for at tiltvinge sig adgang til dokumenter og oplysninger, end hvis der skulle træffes en afgørelse på baggrund af klagerens forelagte beviser. Derudover er det tvivlsomt om Ombudsmanden overhovedet har beføjelser til at håndhæve sanktioner i forbindelse med brud på Privacy Shield reglerne.[113]

4.1.7.5. Afhandlingens overvejelser i forhold til revideringen

I september 2017 foretog FTC for første gang en kontrol Privacy Shield reglerne, og udstedte administrative bøder til tre amerikanske virksomheder for at have vildledt forbrugere om deres deltagelse i Privacy Shield.[114] Eftersom virksomhederne gik med til et forlig i forbindelse med forhandlingen med FTC, kunne det tyde, at FTC rent faktisk er et effektivt retsmiddel til overholdelse af Privacy Shield. Det skal dog bemærkes, at der var tale om tre relativt ukendte virksomheder, og det kan ikke afvises, at en større virksomhed ville modgå FTC og tage sagen i retten i stedet for at acceptere FTCs bøde. Det er derfor fortsat uvist, hvordan FTC forholder sig til de store virksomheder. Det er dog positivt, at man har kompetencen til at indgå forlig med virksomhederne og udstede bøder som straf for overtrædelse.

Persondataforordningen tillader, at der er flere klagemuligheder og tilsyn jf. artikel 51 stk.1. Der er derfor intet i vejen med, at USA, grundet dets føderale system, har flere klagemuligheder og tilsyn med forskellige kompetencer. Kommissionen bør dog præcisere tilsynsmyndighedernes kompetencer, særligt Privacy Shield Ombudsmanden, samt præcisere de europæiske tilsynsmyndigheders rolle og beføjelser over for de amerikanske myndigheder. Privacy Shield Ombudsmanden er en nyskabelse i Privacy Shield, og Ombudsmanden kompetence, eller mangel på samme, og betydningen for revideringen vil gennemgås i afsnit 4.2.2.2.

4.2. Privacy Shield kontra retspraksis

Enhver, der har bopæl på Unionens område, og som ønsker at anvende det sociale netværk, Facebook, er i forbindelse med sin registrering forpligtet til at indgå en aftale med Facebook Irland, som er et datterselskab til Facebook USA. Aftalen går på helt eller delvist at overføre personoplysninger til servere, der tilhører Facebook USA, og som befinder sig i USA, hvor de er genstand for behandling. Maximillian Schrems indgav en klage til Commissioner, hvori han anmodede denne om at udøve sine vedtægtsmæssige beføjelser til at forbyde Facebook Irland at videregive hans personoplysninger til USA. Dette var på baggrund af Edward Snowdens afsløringer af NSAs masseovervågning af europæiske borgere. Klagen blev afvist med henvisning til, at Kommissionen med Safe Harbor-ordningen allerede har slået fast, at USA er et tilstrækkeligt tredjeland.[115] Sagen kom for den irske højesteret,

[110] Ibid., punkt 3.5.3.4, side 47.
[111] Ibid., punkt 3.5.3.6, side 49.
[112] Ibid., punkt 3.5.3.7, side 50.
[113] 16/EN WP 238: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, punkt 3.5.4, side 51.
[114] Link: https://www.ftc.gov/news-events/press-releases/2017/09/three-companies-agree-settle-ftc-charges-they-falsely-claimed, besøgt d. 21.09.2017, kl. 16.30.
[115] C-362/14 Schrems mod Data Protection Commissioner, præmis 26-30.

som anmodede EU-domstolen om at tage stilling til, hvorvidt Commissioner var bundet af Kommissionens tilstrækkelighedsbeslutning, og hvorvidt de nye afsløringer kan danne grundlag for Commissioner at foretage en egen undersøgelse af forholdene i USA.[116]

EU-Domstolen besvarede det præjudicielle spørgsmål og nåede frem til, at nationale tilsynsmyndigheder, herunder Commissioner, som omhandlede i persondatadirektivets artikel 28, i medfør af charterets artikel 7, 8 og 47 ikke er hindret i at foretage en konkret vurdering af Schrems' klage.[117] Dette skyldtes, at Schrems gjorde gældende, at USA's lovgivning og praksis ikke sikrede et tilstrækkeligt beskyttelsesniveau. Commissioner burde derfor have behandlet klagen.

Domstolen vurderede også, at Schrems' klage i virkeligheden rettede sig mod Safe Harbor-ordningens gyldighed og ikke specifikt mod Facebook Irlands overførsel til Facebook USA.[118] Domstolens besvarelse af de præjudicielle spørgsmål vil derfor ikke behandles yderligere. I stedet vil afhandlingen gennemgå Domstolens behandling af Safe Harbor ordningens gyldighed på baggrund af påstanden om, at USA ikke sikrer et tilstrækkeligt beskyttelsesniveau som påkrævet i både persondatadirektivets artikel 26 stk.6 og Charteret. Underkendelsen af Safe Harbor havde baggrund i manglende privatlivsbeskyttelse og manglende adgang til effektive retsmidler på trods af, at Safe Harbors artikel 1 fastslog et tilstrækkeligt beskyttelsesniveau i USA.

4.2.1. Krav til privatlivsbeskyttelse

Safe Harbors artikel 1 skal læses i sammenhæng med persondatadirektivets artikel 25 stk.6, der kræver, at overførsler skal ske til et tredjeland, der i det væsentlige sikrer et tilsvarende beskyttelsesniveau som krævet i direktivet. Artikel 1 i Safe Harbor siger, at Safe Harbor principperne *''formodes''* at *''sikre''* et tilstrækkeligt beskyttelsesniveau i USA i overensstemmelse med kravene i persondatadirektivet.

Domstolen bemærker, at Safe Harbor udelukkende stiller krav til selvcertificerende amerikanske foretagender, og ikke offentlige amerikanske myndigheder.[119] Domstolen bemærker også, at Safe Harbors Bilag 1, 4. afsnit giver mulighed for, blandt andet ved lov og administrative forskrifter, at begrænse anvendelsen af Safe Harbor principperne til et niveau, der er tilstrækkeligt for at opfylde kravene med hensyn til statens sikkerhed, almenvellet eller opretholdelsen af lov og orden.[120] Derudover har amerikansk lovgivning ved opfyldelse af disse krav til blandt andet statens sikkerhed forrang for Safe Harbor principperne.[121] Domstolen kritiserer særligt, at undtagelserne i Bilag 1, 4.afsnit er af så generel karakter, at der åbnes op for indgreb i europæiske borgeres grundlæggende rettigheder og friheder. Domstolen udtaler også, at et indgreb i retten til privatliv ikke er betinget af, at videregivne oplysninger er af personfølsomme karakter, eller at videregivelsen har medført ubehageligheder for den berørte. Kritikken understøttes også af, at der ikke på statsligt niveau i USA er regler, der tilsigter at begrænse indgreb i grundlæggende rettigheder for de registrerede i tilfælde af indgreb, der forfølger legitime formål, såsom statens sikkerhed.[122]

Ovenstående blev brugt af Domstolen til at statuere, at artikel 1 i Safe Harbor tilsidesættes som ugyldig, fordi den blandt andet ikke sikrer et tilstrækkeligt beskyttelsesniveau i form af blandt andet en

[116] Ibid., præmis 36.
[117] Ibid., præmis 66.
[118] Ibid., præmis 67.
[119] Ibid., præmis 82.
[120] C-362/14 Schrems mod Data Protection Commissioner, præmis 84.
[121] Ibid., præmis 85-86.
[122] Ibid., præmis 87-88.

beskyttelse af retten til respekt for privatlivet, som er sikret i både EMRK artikel 8 og Charteret artikel 7.

4.2.1.1. Indgreb i privatlivet

Domstolens bemærkninger har støtte i Generalsekretær Bots forslag til afgørelsen.

Bot starter med at slå fast, at PRISM-programmet, som blev brugt til masseovervågning af blandt andet europæiske borgere udgør et indgreb i retten til beskyttelse af privatlivet.[123] Dette har støtte i EMD-praksis, hvor det er slået fast, at systematisk indsamling og opbevaring af persondata i offentlige myndigheders registre i sig selv er tilstrækkeligt til at udgøre et indgreb i retten til privatliv efter EMRK artikel 8.[124] I Leander-dommen fik Leander ikke medhold i sin klage til EMD, selvom der blev statueret et indgreb i retten til privatliv efter artikel 8 stk.1. EMD fandt, at undtagelserne i artikel 8 stk.2 var opfyldt.[125] Artikel 8 stk.2 kræver, at indgrebet skal være foreskrevet ved lov, forfølge legitime hensyn og være nødvendigt i et demokratisk samfund.

Bot udtaler, at der foreligger et særligt intensivt indgreb som blandt andet begrundes i, at Facebook brugerne ikke oplyses om, at deres personoplysninger gøres almindeligt tilgængelige for de amerikanske sikkerhedsmyndigheder.[126] Dette har støtte i EMD-praksis, der slår fast, at EMRK artikel 8 om retten til privatliv blandt andet indeholder processuelle retsgarantier, som skal opfyldes for at sikre en beskyttelse af borgernes ret til privatliv, herunder retten til at blive hørt og blive oplyst om beslutninger, der påvirker ens retsstilling.[127]

4.2.1.2. Brud på proportionalitetsprincippet

Bot kritiserer, at de *''legitime interesser''* i Bilag 1, 4. afsnit ikke præciseres nærmere, og at der foreligger usikkerhed om omfanget af undtagelsernes anvendelsesområde. Derudover kritiseres det, at der alene foretages en generel henvisning til amerikansk lovgivning i stedet for at henvise til en direkte lovhjemmel. Ovenstående er nogle af årsagerne til, at Bot betragter undtagelserne i Bilag 1, 4. afsnit som værende i strid med Charterets artikel 7 (privatliv), 8 (databeskyttelse) og 52 (rækkevidden af de sikrede rettigheder).[128] Bot betragter masseovervågningen som værende i strid med proportionalitetsprincippet, i det en så massiv og vilkårlig overvågning i sagens natur er uforholdsmæssig og udgør et uberettiget indgreb i de rettigheder, der sikres ved Charterets artikel 7 og 8. EU-lovgiver og medlemsstaterne har ikke mulighed for at vedtage lovbestemmelser, der foreskriver massiv og vilkårlig overvågning i strid med Charteret. Dette må betyde, at tredjelande under ingen omstændigheder kan anses for at sikre et tilstrækkeligt beskyttelsesniveau for EU-borgeres personoplysninger, når tredjelandets lovgivning faktisk tillader massiv og vilkårlig overvågning og opfangning af personoplysninger, som tilfældet er med USA.[129]

Samme kritik kan rettes mod Privacy Shield. Artikel 29-Gruppen anerkender, at Privacy Shield nu også omfatter offentlige myndigheders behandlings og indhentelse af personoplysninger. Gruppen kritiserer dog fortsat, at ordningen ikke omfatter den amerikanske efterretningstjeneste, selvom statens sikkerhed altid er et legitimt hensyn. Gruppen anfører, at massiv og vilkårlig overvågning af individer aldrig kan være proportionelt og nødvendigt i et demokratisk samfund.[130] Denne kritik er aktivisten Max Schrems enig i, og han anser Privacy Shield som et godt alternativ til Safe Harbor,

[123] Forslag til afgørelse C-362/14 fra Generalsekretær Y. Bot, 23.09.2015, præmis 170.
[124] Leander mod Sverige, 9248/81, 26.03.1987, præmis 48.
[125] Ibid., præmis 67.
[126] Forslag til afgørelse C-362/14 fra Generalsekretær Y. Bot, 23.09.2015, præmis 172.
[127] Shtukaturov mod Rusland, 44009/05, 27.03.2008, præmis 91.
[128] Forslag til afgørelse C-362/14 fra Generalsekretær Y. Bot, 23.09.2015, præmis 178-183.
[129] Ibid., præmis 200-201.
[130] 16/EN WP 238: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, side 4.

men kritiserer, at ordningen ikke tager højde for amerikanske efterretningstjenesters masseovervågning af borgerne, hvilket var grunden til, at sagen mod Facebook Irland overhovedet blev påklaget til Commissioner i første omgang.[131]

4.2.1.3. Betragtninger til revideringen

Ikke det helt store lader sig til at være ændret ved den amerikanske lovgivning som var grundlag for underkendelsen af Safe Harbor, hvilket må siges at være Privacy Shields svaghed, når det kommer til privatlivsbeskyttelse. Max Schrems anfører, at der ikke er så meget EU kan gøre på lige netop dette område, men at det må komme fra USA selv, nærmere bestemt det amerikanske forretningsliv, der selv har en interesse i, at Privacy Shield opretholdes. Dette kan ske ved at virksomhederne i Silicon Valley gennem lobbyarbejder presser de amerikanske lovgivere til en ændret lovgivning, der i højere grad respekterer privatlivet og databeskyttelsen for ikke bare amerikanske borgere, men også europæere.[132] Det må dog siges, at Kommissionen, ud fra retspraksis behandling af de processuelle retsgarantier, der er indeholdt i privatlivsbeskyttelsen, ikke kan løbe fra, at retten til at blive hørt og retten til at blive oplyst er en vigtig del af privatlivsbeskyttelsen. Disse rettigheder må derfor have særlig fokus i forbindelse med revideringen af Privacy Shield.

4.2.2. Krav til effektive retsmidler

Det er slået fast at underkendelsen af Safe Harbor blandt andet var begrundet i manglende beskyttelse af retten til privatlivet. Underkendelsen var dog også begrundet i manglende beskyttelse af retten til effektive retsmidler.

Akkurat som EMRK artikel 8 indeholder processuelle retsgarantier, selvom dette ikke eksplicit fremgår af ordlyden jf. afsnit 4.2.1.1, udleder EU-Domstolen, at persondatadirektivets artikel 25 indeholder sådanne processuelle retsgarantier, der er med til at sikre adgang til effektiv domstolsprøvelse.[133] Adgang til effektive retsmidler er en grundlæggende rettighed som fremgår af EMRK artikel 13 og Charterets artikel 45.

Domstolen finder frem til, at amerikansk lovgivning ikke indeholder adgang til effektive retsmidler, der tillader den registrerede adgang til berigtigelse, sletning eller effektiv domstolsprøvelse og klageadgang.[134] Dette omfatter også manglende adgang til indsigt.[135]

Domstolen henviser til generalsekretær Bots udtalelse om, at Safe Harbors regler om private voldgiftsmekanismer og FTCs kompetence, der kun behandler handelstvister, ikke kan benyttes som effektiv klageadgang mod de amerikanske efterretningstjenesters adgang til personoplysninger, der overføres fra EU. FTCs kompetence dækker ikke ikke-kommercielle forhold og er, modsat medlemsstaternes tilsynsmyndigheder, ikke oprettet for at beskytte borgeres ret til privatliv, men derimod oprettet for at skabe bedre handelsvilkår.[136] Bot kritiserer, at hverken FTC eller de private voldgiftsmekanismer har kompetence til at kontrollere eventuelle overtrædelser af principperne om beskyttelse af personoplysninger, som begås af offentlige aktører såsom efterretningstjenesterne. En sådan kompetence anser Bot og Domstolen som værende afgørende for at sikre retten til effektiv beskyttelse af

[131] Link: https://www.youtube.com/watch?v=EdCmpmL1UJk (Europa Parlamentets officielle Youtube kanal) 'Privacy Shield: Safe Harbor with teeny tiny changes' - Max Schrems, 18.03.2016, besøgt d. 30.08.2017, kl. 14.15.
[132] Ibid.
[133] C-362/14, Schrems mod Data Protection Commissioner, præmis 53 og 99.
[134] Ibid., præmis 95.
[135] Forslag til afgørelse C-362/14 fra Generalsekretær Y. Bot, 23.09.2015, præmis 212.
[136] C-362/14, præmis 89 jf. Forslag til afgørelse C-362/14 fra Generalsekretær Y. Bot, 23.09.2015, præmis 204-206.

personoplysninger. Safe Harbor sikrer derfor ikke en tilstrækkelig beskyttelse af den ret, der tillægges ved Charterets artikel 8 stk.3 om databeskyttelse ved en uafhængig tilsynsmyndighed.[137]

Det er hermed fastslået, at de tilgængelige retsmidler i Safe Harbor ikke har været effektive, og dette skyldes blandt andet myndighedernes manglende uafhængighed. Netop uafhængigheden var en afgørende faktor i Leander-dommen, hvis præmisser kan anvendes i denne sag og bruges til en sammenligning med de nye retsmidler i Privacy Shield.

4.2.2.1. Leander-dommen og betydningen af uafhængige tilsynsmyndigheder

Sagen angik svenske efterretningstjenesters persondata registrering af en svensk borger. Leander blev ansat på et museum ved en marinestation. Der blev foretaget en undersøgelse af Leanders fortid i et hemmeligt politiregister, hvilket førte til, at han blev afskediget.[138]

Det skal for en god ordens skyld nævnes, at Leander ikke blev hørt i forbindelse med databehandlingen, akkurat som de registrerede ikke blev i forbindelse med overførsler efter Safe Harbor principperne. EMD nåede frem til at der forelå et indgreb i retten til privatliv,[139] men man nåede dog også frem til, at der alligevel ikke forelå en krænkelse af retten til privatliv, da der forelå klare regler for indgrebet og da indgrebet var nødvendigt i et demokratisk samfund og var begrundet i statens sikkerhed.[140]

Udover påstanden om krænkelse af EMRK artikel 8 om retten til privatliv påstod Leander, at hans ret til effektive retsmidler efter EMRK artikel 13 var blevet krænket. Det er i afsnit 4.2.1.1 nævnt, hvordan artikel 8 indeholder processuelle retsgarantier, som kan have en indvirkning på, hvorledes der foreligger en krænkelse af retten til privatliv. EMD nåede frem til at der ikke var sket en krænkelse af retten til effektive retsmidler i artikel 13.

EMD startede med at fastslå det generelle princip, at EMRK artikel 13 er opfyldt, hvis de enkelte retsmidler samlet set er tilstrækkelige. Flere enkeltvise utilstrækkelige retsmidler kan således samlet set udgøre en opfyldelse af EMRK artikel 13.[141]

Afgørende for resultatet var, at Leander havde adgang til faktisk uafhængige effektive retsmidler hos både parlamentets Ombudsmand og Justitskansleren.[142]

EMD anerkendte, at Ombudsmanden og Justitskansleren formelt set var afhængige af henholdsvis parlamentet og regeringen,[143] og ikke havde kompetence til at udstede retligt bindende afgørelser.[144] Umiddelbart ville dette betyde, at disse retsmidler ikke er effektive i EMRKs forstand. EMD påpege dog, at Sverige har en så stærk tradition med Ombudsmanden og Justitskansleren, at disses afgørelser, selvom de ikke er retligt bindende, utvivlsomt vil følges af myndighederne. Disse to retsmidler er derfor begge faktisk uafhængige tilsynsmyndigheder som kan konstituere et effektivt retsmiddel i overensstemmelse med EMRK artikel 13.

4.2.2.2. Privacy Shield Ombudsmandens kompetencer

Det er nu slået fast, at et lands retssystem er effektivt, hvis landet har faktisk uafhængige tilsynsmyndigheder. Det overlader spørgsmålet, hvorledes Schrems-dommens præmisser, og for den sags skyld

[137] Forslag til afgørelse C-362/14 fra Generalsekretær Y. Bot, 23.09.2015, præmis 207.
[138] Leander mod Sverige, 9248/81, 26.03.1987, punkt I.
[139] Ibid., præmis 48.
[140] Ibid., præmis 67.
[141] Leander mod Sverige, 9248/81, 26.03.87, præmis 77 (C).
[142] Ibid., præmis 81 og 84.
[143] Ibid., præmis 38 jf. 81-82 og præmis 36 jf. 81-82.
[144] Ibid., præmis 82.

Leander-dommen, kan anvendes i forbindelse med Privacy Shields regler om navnlig håndhævelse og retsmidler. Der er nu oprettet en Privacy Shield Ombudsmand, og det er yderst relevant at sammenligne dennes kompetence med Ombudsmandens kompetence i Leander-dommen.

Ombudsmandsrollen er pålagt Seniorkoordinatoren i det amerikanske udenrigsministerium, og er uafhængig af de amerikanske efterretningstjenester. Som nævnt i afsnit 4.1.7.4 kritiserer Artikel 29-Gruppen, at Privacy Shield ikke går nærmere ind og beskriver Ombudsmandens kompetencer. Ordningen siger kun, at Ombudsmandens skal give den EU-klageinstansen, der har klaget på vegne af borgeren, et svar, hvori det bekræftes at klagen er blevet behørigt undersøgt, at amerikanske love, agenturers politikker og præsidentielle dekreter og direktiver er blevet overholdt, og i modsat fald, at den manglende overholdelse er blevet afhjulpet. Ombudsmanden kan hverken bekræfte eller afkræfte, hvorvidt borgeren er udsat for overvågning af den amerikanske efterretningstjeneste i forbindelse med den påklagede databehandling, og oplyser heller ikke hvilket retsmiddel der blev anvendt.[145] Der oplyses altså ikke hvilke muligheder for aktindsigt og håndhævelse Ombudsmanden besidder. Ordningen kræver alene at Ombudsmanden oplyser, hvorvidt fejlen er afværget, men ikke om det er Ombudsmanden der skal gennemtvinge afværgelsen. Det kan umiddelbart tyde, at Ombudsmanden fungerer som kommunikationsenhed mellem USA og EU, og ikke som et retsmiddel til håndhævelse af databeskyttelsesreglerne. Dette kan understøttes af, at Privacy Shield Ombudsmanden ikke er en selvstændig institution, sådan som vi kender det i Norden, herunder Ombudsmanden i Leander-dommen. Privacy Shield Ombudsmanden er derimod en person, der på viceministerniveau er ansat i det amerikanske udenrigsministerium, der fungerer som kontaktperson.[146] Dette kan først og fremmest ikke siges at opfylde graden af uafhængighed, der blev fastsat i Leander-dommen.

I Leander-dommen var en af årsagerne til, at den svenske Ombudsmand blev anset at udgøre et effektivt retsmiddel efter EMRK artikel 13, at denne, udover at være faktisk uafhængig, havde adgang til og kunne kræve relevante oplysninger og dokumenter udleveret med henblik på at foretage en vurdering af, hvorvidt det er sket en lovovertrædelse.[147] Der lægges også vægt på, at den svenske Ombudsmand har kompetence til at indstille en strafferetlig eller disciplinær procedure mod den person, herunder en embedsmand, der har begået lovovertrædelsen.[148]

Til forskel fra den svenske Ombudsmand kan det således siges, at Privacy Shield Ombudsmanden hverken er formelt eller faktisk uafhængig, ikke lader til at kunne gennemtvinge sig adgang til indsigt i offentlige myndigheders dokumenter og ikke har mulighed for at iværksætte foranstaltninger, der skal bringe en overtrædelse til ophør, men alene konstatere, hvorvidt en overtrædelse har fundet sted. Det er ikke til at vide, hvorvidt denne konstatering i sig selv er nok til at lovovertræderen vil bringe overtrædelsen til ophør. Den afgørende forskel mellem USA og Sverige, i spørgsmålet om Ombudsmanden som effektivt retsmiddel, er netop at Ombudsmanden i Sverige og de nordiske lande nyder stor respekt, og at der i høj grad er tradition for at man følger en ombudsmands udtalelse og retter sig efter dennes kritik.[149] Hele konceptet med en ombudsmand er nyt for USA, og der foreligger derfor ikke samme tradition for at følge dennes udtalelse og rette sig efter kritikken.

4.2.2.3. Betragtninger til revideringen

Som nævnt i afsnit 4.2.1.3 er der ikke noget EU kan gøre for at ændre ved amerikansk lovgivning. EU kan ikke pålægge Handelsministeriet eller FTC andre kompetencer, end det som amerikansk lov-

[145] Commission Implementing Decision (2016) 4176 final, Bilag 3, A, punkt 4, e.
[146] Ibid., Bilag 5, punkt d, sidste afsnit.
[147] Leander mod Sverige, 9248/81, 26.03.1987, præmis 81 jf. præmis 38, 39 og 41.
[148] Ibid., præmis 38.
[149] Leander mod Sverige, 9248/81, 26.03.1987, præmis 82.

givning pålægger dem. EU kan derimod præcisere de europæiske myndigheders kompetencer i forhold til de amerikanske myndigheder. I forbindelse med den kommende Privacy Shield revidering er det reglerne om Privacy Shield Ombudsmanden, hvor EU kan have en stor indflydelse. Ombudsmandens uafhængighed kan EU ikke gøre noget ved, da dette forudsætter en ændring i den politiske struktur i USA. Afgørende for EU må derfor være at tildele Privacy Shield Ombudsmanden kompetencen til at kræve indsigt i amerikanske myndigheders dokumenter. Kan dette gøres vil man formentlig se bort fra den manglende grad af uafhængighed mellem Privacy Shield Ombudsmanden og det amerikanske udenrigsministerium.

5. Konklusion

I denne digitale tidsalder udgør borgeres personoplysninger en værdifuld handelsvare på lige fod med fysiske goder. Personoplysningerne er genstand for massiv behandling over hele verden, og der er derfor behov for et særligt regelsæt til at sikre borgerne en tidssvarende data- og privatlivsbeskyttelse, hvilket var grundlaget for skabelsen af persondataforordningen. Der er adgang til fri dataoverførsel inden for EU, men overførsler til et tredjeland skal opfylde reglerne i persondataforordningens kapitel 5. Hvorvidt der er tale om en international persondataoverførsel omfattet af forordningens regler afhænger af en konkret vurdering. Det er dog et krav, at der må foreligge et grænseoverskridende element i forbindelse med overførslen, før der er tale om en persondataoverførsel i forordningens forstand. Hvis der sker videregivelse af personoplysninger inden for en koncern, er der tale om en international persondataoverførsel omfattet af forordningen, såfremt videregivelsen sker fra et selskab i etableret EU til moder- eller datterselskabet etableret i USA.

Netop USA har en særlig vigtig og afgørende status i den internationale handel. Dette er grundlaget for, at Kommissionen har vedtaget en helt særlig ordning, Privacy Shield, til overførsler mellem EU og USA, i stedet for at lave en almindelig tilstrækkelighedsvurdering som man normalt gør med andre tredjelande. En almindelig tilstrækkelighedsvurdering af USA ville formentlig ikke have vurderet USA til at være et tilstrækkeligt tredjeland grundet landets relativt svage databeskyttelseslovgivning på føderalt niveau, og den masseovervågning som NSA foretager af blandt andre europæiske borgere.

Privacy Shield er udformet på baggrund af persondatadirektivet, men med udsigt til senere revidering med henblik på at blive konform med persondataforordningen, der blandt andet har til formål at sikre større transparens. Selvom den dagældende Safe Harbor også havde samme syv principper som Privacy Shield, indeholder Privacy Shield flere positive elementer i forhold til Safe Harbor. Privacy Shield går dog videre og fokuserer på de mere individuelle rettigheder for EU-borgere, og stiller strengere krav til amerikanske virksomheder. Fx er et af de væsentligste forbedringer reglen om ansvar for videreoverførsler. Som noget nyt skal virksomheder nu opfylde princippet om formålsbegrænsning og sikre, at tredjeparten stiller samme beskyttelsesniveau som Privacy Shield, før der kan ske videreoverførsler til en tredjepart.

På trods af de enkelte forbedringer er Privacy Shield med rette genstand for kritik. Kommissionen bør revidere reglen om tidspunktet for oplysningspligtens opfyldelse og droppe sondringen mellem direkte og indirekte registrering. Derudover bør man indføre en regel om, at valgfrihedsprincippet også gælder ved profilering, der er et vigtigt princip i persondataforordningen, og ikke kun ved direkte markedsføring. Derudover bør man se på tiltag, der kan opfylde forordningens samtykkekrav. Det kan fx være et krav om indhentelse af nyt samtykke til videreoverførsler, og en regel om at tilbyde opt-out, før der sker videreoverførsler og genbrug af personoplysninger. Dermed sikres, at der altid gives et informeret, frit og utvetydigt samtykke fra den registrerede.

Privacy Shield bør også indføre reglen om dataminimering, og i den forbindelse gøre det klart, at personoplysninger skal begrænses til, hvad der er nødvendigt, og ikke blot hvad der er relevant.

Den registrerede har i Privacy Shield flere klagemuligheder. Dette kan i sig selv tænkes positivt, men kan også tænkes uoverskueligt. Det er uvist, hvad de forskellige myndigheders kompetencer indebærer, og hvordan deres forhold er med de europæiske håndhævelsesmyndigheder. Positivt er det, at man har oprettet en Privacy Shield Ombudsmand. Her mangler man dog også klare regler for Ombudsmandens kompetencer. Afgørende må være at tildele denne muligheden for at gennemtvinge sig adgang til aktindsigt, hvilket var et afgørende element i Leander-dommen. Tiden må vise, hvad de forskellige håndhævelsesmyndigheder præcist har af kompetencer over for både små og store virksomheder.

Konkluderende må det derfor siges, at Privacy Shield indeholder forbedringer, men går ikke langt nok for at sikre den grad af transparens som persondataforordningen kræver. Privacy Shield går heller ikke langt nok for at sikre de processuelle retsgarantier, der følger af data- og privatlivsbeskyttelsen i Charteret og EMRK, såsom ret til at blive hørt og ret til indsigt. Dette kan løses ved de oven for nævnte tiltag, der kan være med til at styrke samtykkekravet og give den registrerede en større kontrol og medbestemmelse i hvad personoplysningerne bruges til.

6. Litteraturliste

6.1. Bøger

- Christopher Kuner: European Data Protection Law (Corporate Compliance and Regulation, 2nd edition, Oxford, 2007.
- Evald og Schaumburg-Müller: Retsfilosofi, Retsvidenskab og Retskildelære, 1. udgave, Jurist- og økonomforbundets forlag, 2014.
- IT Governance Privacy Team (Alan Calder, Richard Campo, Adrian Ross): EU General Data Protection Regulation (GDPR), An Implementation and Compliance Guideline, 2016.
- Peter Blume: Den Nye Persondataret, 1. udgave, Jurist- og økonomforbundets forlag, 2016.
- Peter Blume: Persondataretlige Grundfigurer, 1. udgave, Jurist- og økonomforbundets forlag, 2017.
- Peter Blume: Retlig Regulering af Internationale Persondataoverførsler, 1. udgave, Jurist- og økonomforbundets forlag, 2006.

6.2. Lovgivning, traktater og konventioner

- 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).
- Den Europæiske Unionens Charter om Grundlæggende Rettigheder (2000/C 364/01).
- Europarådets Konvention nr. 108 af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger.
- 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.
- 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.
- Federal Trade commission act Federal Trade Commission Act 38 Stat. 717 (1914).
- Kommissionens beslutning af 26. juli 2000 (2000/520) EF 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.

- 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 *(meddelt under nummer C (2016) 4176)*.
- Konvention til beskyttelse af Menneskerettigheder og Grundlæggende Frihedsrettigheder, 1953.
- 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.

6.3. Retspraksis

- C-362/14 Schrems mod Data Protection Commissioner.
- C-101/01, straffesag mod Bodil Lindqvist, 6. november 2003.
- Forslag til afgørelse C-362/14 fra Generalsekretær Y. Bot, 23.09.2015.
- Leander mod Sverige, 9248/81, 26.03.1987.
- Zakharov mod Rusland, 47143/06, 04.12.2015.
- Shtukaturov mod Rusland, 44009/05, 27.03.2008.

6.4. Artikler og tidsskrifter

- Dan Jerker B. Svantesson: The Regulation of Cross-border Data Flows, International Data Privacy Law,Vol. 1, No.3, 01.08.2011, Oxford Academic, side 180-198.
- Jon Bing: Overføring av personopplysninger til utlandet – noen grunnleggende problemstillinger, Lov og Rett, vol. 53, 3, 2014, side 127-146.

6.5. Rapporter og vejledninger

- Article 29 Working Party: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016.
- Article 29 Working Party: Opinion 8/2010 on applicable law, adopted on 16 December 2010.
- Article 29 Working Party: Letter to Vice-President Redin, 10 April 2014.
- Article 29 Working Party: Working document on a common interpretation of Article 26(1) of Directive 95/45/EC of October 1995, adopted on 25 November 2005.
- Article 29 Working Party: Working document on Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, adopted by the Working Party on 24. July 1994.
- COM (2017) 611 Final, ‘’Report from the Commission to the European Parliament and The Council on the first annual review of the functioning of the EU-U.S. Privacy Shield, Brussels, 18.10.2017.
- Directorate-General for Internal Policies, Policy Department C – Citizens’ Rights and Constitutional Affairs: ‘’A Comparison between US and EU Data Protection Legislation for Law Enforcement’’, study for LIBE, 2015.

6.6. Websteder

- EU-U.S. data flows and data protection: opportunities and challenges in the digital era -- Speech at the Center for Strategic and International Studies by Věra Jourová, Commissioner for Justice, Consumers and Gender Equality: http://europa.eu/rapid/press-release_SPEECH-17-826_en.htm, besøgt d. 25.09.2017, kl. 14.00.
- Model Contracts for the transfer of personal data to third countries: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm, besøgt d. 24.07.2017, kl. 14.00.

- Update on litigation involving Facebook and Maximilian Schrems: https://www.dataprotection.ie/docs/16-03-2017-Update-on-Litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm, besøgt d. 25.07.2017, kl. 14.15.
- Countries and regions – Trade: http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states, besøgt d. 25.07.2017, kl.17.00.
- Commission decisions on the adequacy of the protection of personal data in third countries: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm, besøgt d. 20.09.2017, kl. 15.30.
- Privacy Shield Listen: https://www.privacyshield.gov/list, besøgt d. 14.08.2017, kl. 09.30.
- Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework: https://www.ftc.gov/news-events/press-releases/2017/09/three-companies-agree-settle-ftc-charges-they-falsely-claimed, besøgt d. 21.09.2017, kl. 16.30.
- 'Privacy Shield: Safe Harbor with teeny tiny changes' - Max Schrems: https://www.youtube.com/watch?v=EdCmpmL1UJk (Europa Parlamentets officielle Youtube kanal), uploadet d. 18.03.2016, besøgt d. 30.08.2017, kl. 14.15.
- ‘’The Case of Standard Contractual Clauses: The Irish Data Protection Commissioner and Max Schrems’’, oprettet d. 12.03.2017, www.Paolobalboni.eu, besøgt d. 25.09.2017, kl. 14.30.