Titelblad

Titel:	**Overførsel af personoplysninger til tredjelande**
Vejleder:	**Søren Sandfeld Jakobsen**
Afleveringsdato:	**10. august 2017**
Studieretning:	**Jura – 10. semester**
Sted:	**Aalborg Universitet**
Studienummer:	**20031324**

Helle Dollerup Mortensen

Transfer of personal data to third countries

Denmark as all the other member states of the European Union has implemented directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Danish Act on Processing of Personal Data was passed in year 2000 to implement directive 95/46/EC and is still in force. – however the new EU General Data Protection Regulation which will come into force on May 25, 2018 will have a huge impact on how companies work with personal data right now. In Denmark it is fair to say that the companies probably has not had a lot of focus on if their handling of person data is in compliance with the Danish Act on Processing of Personal Data due to the insignificant penalty level. The new EU General Data Protection Regulation will change this with maximum penalties up to 4 % of the company's group turnover. Now Danish companies are being forced to take handling of personal data serious.

A Danish company with subsidiaries in all parts of the world, including the United States of America will most likely have a need to transfer personal data from one entity to another. As the head quarter is in Denmark and the data will be transferred from Denmark to the other entities, the Danish law will regulate the transfer. However, what is personal data and what are the requirements for a legal transfer of the personal data to countries outside the European Union?

A framework between the European Union and the United States of America was set up and decided upon by the European Commission in year 2000, called the Safe Harbor decision which determined that the United States of America ensured adequate level of protection of personal data cf. article 25 in directive 95/46/EC, meaning that personal data due to the adequate level of protection of personal data could be transferred from companies within the European Union to companies in the United States of America. The companies in the United States of America had to follow the principles in the Safe Harbor framework and join the framework electronically. This decision was in the Safe Harbor Ruling declared invalid by the European Court of Justice due to it has not been established if the United Stated of America itself ensured an adequate level of protection of the personal data transferred to companies within the U.S.A. It had been concluded that the Safe Harbor decision had been made on a fragile foundation and had not been prepared thoroughly.

With the Safe Harbor decision ruled invalid, the European companies needed another possibility of transferring personal data to the United Stated of America. Shortly after the Safe Harbor ruling, the Privacy Shield Framework was decided upon in July 2016 by the European Commission and is still in force

today. – but will it still be compliant with European law after May 25th 2018 when the EU General Data Protection Regulation will come into force?

The thesis contains a description of current law in Denmark and EU regarding transfer of personal data to third countries – a description of the new rules in the EU General Data Protection Regulation in regards to the transfer of personal data to third countries. The Safe Harbor ruling will be analyzed and especially in regards to "ensuring adequate protection of personal data". The Privacy Shied framework which followed the Safe Harbor framework will be analyzed in regards to "ensuring adequate protection of personal data". Is the Privacy Shield Framework enough or will it be deemed invalid next year in May? Lastly, other options of transferring personal data to third counties will be reviewed.

Indholdsfortegnelse

Definitioner

Chartret: Den europæiske unions charter om grundlæggende rettigheder

Dataansvarlig: Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger.[1]

Databehandleren: Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne.[2]

Databeskyttelsesdirektivet: Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

Databeskyttelsesforordningen: 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.

Domstolen: Den Europæiske Unions domstol.

Modtager: Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, hvortil oplysningerne meddeles, uanset om der er tale om en tredjemand. Myndigheder, som vil kunne få meddelt oplysninger som led i en isoleret forespørgsel, betragtes ikke som modtagere.[3]

Overførsel: Samlet betegnelse for videregivelse og overladelse/intern anvendelse.

Persondataloven: Lov om behandling af personoplysninger.

Den registrerede: en identificeret eller identificerbar fysisk person.

Unionen: Den Europæiske Union.

[1] Lov om behandling af personoplysninger, § 3, stk. 1, nr. 4
[2] Lov om behandling af personoplysninger, § 3, stk. 1, nr. 5
[3] Lov om behandling af personoplysninger, § 3, stk. 1, nr. 6

1. Indledning

I slutningen af 1970'erne blev de første reelle love omhandlende beskyttelse af personoplysninger vedtaget i Danmark (Registerlovene). Siden 1970'erne har udvikling af den digitale teknologi taget fart og det har været nødvendig med yderligere regulering for at beskytte personoplysningerne. I og med at vi nu befinder os i en særdeles foranderlig digital verden, hvor teknologien muliggør endeløse udvekslinger af data på tværs af landegrænser, så er behovet for beskyttelse af personoplysninger steget. Lov om behandling af personoplysninger, der blev vedtaget i år 2000, implementerer Databeskyttelsesdirektivet og er den nuværende gældende lovgivning på området.

Den Europæiske Union har ved Databeskyttelsesdirektivet indført minimumsregler for håndtering af personoplysninger i alle medlemsstater og ved vedtagelsen af den nye Databeskyttelsesforordning EU 2016/679, er den allerede eksisterende lovgivning blevet moderniseret og en række nye tiltag introduceret. EU har generelt søgt, at personoplysninger skulle beskyttes bedst muligt og med direktivet fra 1995 og den nye forordning fra sidste år, så har medlemsstaterne i EU et højt beskyttelsesniveau. Det er for så vidt fint nok, at medlemsstaterne i EU har et højt beskyttelsesniveau, men hvad med de europæiske virksomheder, som har behov for at overføre personoplysninger til virksomheder i lande uden for EU, de såkaldte tredjelande?

Et stort dansk moderselskab med datterselskaber (koncernen) i mange forskellige lande vil alt andet lige have et uundværligt behov for at kunne dele identificerede eller identificerbare personoplysninger med sine koncernforbundne selskaber og vice versa – og når en sådan deling sker, så er den underlagt den persondataretlig regulering, uanset om der er blot er tale om et identificerbart billede, der bliver uploadet på et intranet, som hele koncernen har adgang til. Har et moderselskab et datterselskab uden for EU og det er nødvendigt at overføre identificerede/identificerbare personoplysninger, så er overførslen underlagt den i EU vedtagne regulering.

Bødeniveauet for overtrædelse af Databeskyttelsesforordningen er markant højere[4] end bødeniveauet i den gældende lovgivning, hvor en privat virksomheds ulovlig behandling af personoplysninger er blevet afgjort med bøder på max. 10.000 kr.[5] Overtræder en virksomhed bestemmelserne i den nye Databeskyttelsesforordning efter den er trådt i kraft (25. maj 2018), så kan virksomheden i værste fald blive idømt en bøde på op EUR 20.000.000 eller til 4 % af Koncernens samlede globale årlige omsætning,

[4] Databeskyttelsesforordningen, artikel 83
[5] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 663

hvis dette er højere[6]. Det er en mærkbar forskel, som har medvirket til, at fokus på korrekt behandling af personoplysninger i de danske virksomheder er steget.

Hvor det tidligere kunne antages, at virksomheder qua det lave bødeforlæg ikke har vist interesse for at ændre interne procedurer, der var i strid med lovgivning om behandling af personoplysninger, er der grundet risikoen for at blive pålagt en væsentlig større bøde (EUR 20.0000 eller 4 % af årlig koncernomsætning) en højere grad af interesse for, at virksomheden får indført procedurer, der sikrer dennes compliance med Databeskyttelsesforordningen.

Så hvordan sikrer et moderselskab, at overførsel af identificerede/identificerbare personoplysninger til et datterselskab uden for EU er lovligt efter den nuværende og kommende lovgivning og hvordan defineres disse identificerede/identificerbare personoplysninger?

1.1 Problemformulering

Hvilke muligheder har en virksomhed jf. gældende lovgivning for at overføre personoplysninger fra Danmark til tredjelande og i særdeleshed til USA? – set i lyset af Safe Harbor-dommen.

1.2 Afgrænsning

Afhandlingen vil omfatte de grundlæggende principper i persondateretten, men kun i det omfang at det bidrager til forståelsen og er inden for afhandlingens problemstilling. Derudover er afhandlingen afgrænset til kun at omhandle den private sektor, dog vil reglerne for det offentlige bliver berørt, når det tjener til at forstå de persondataretlige begreber og problemstillinger.

Selvom problemformuleringen omhandler overførsel af personoplysninger til USA, så vil den amerikanske lovgivning ikke blive gennemgået, da afhandlingen beskæftiger sig med den EU-retlige regulering i og med, at Danmark er medlem af EU. Gennemgang af relevant og kommende lovgivning er afgrænset til at indeholde de afsnit, som er relevante i forhold til problemformuleringen. Afhandlingen vil derfor ikke indeholde en fuldstændig gennemgang af hele den persondataretlige lovgivning.

[6] Databeskyttelsesforordningen, artikel 83, nr. 5 og 6

2. Metode

Afhandlingen vil for at fastlægge den lovlige overførsel af personoplysninger fra Danmark til tredjelande anvende den retsdogmatiske metode, som er systematisk beskrivelse og fortolkning af eksisterende regler på området.[7]

Afhandlingen vil indledningsvis indeholde en gennemgang af den gældende og kommende lovgivning på området og specifikt en udførlig analyse af begrebet personoplysninger, herunder inddragelse af udtalelser og retspraksis på området. Der vil i afhandlingen bliver lagt stor vægt på både national og europæisk ret. I Danmark ender langt de fleste sager ikke ved domstolene, men ved Datatilsynet, og derfor tillægges Datatilsynets udtalelser og skrivelser stor værdi. Derudover vil artikel 29- gruppens udtalelser og skrivelser ligeledes indgå til vurdering af relevant fortolkning og praksis i forbindelse med afhandlingen.

Afhandlingen fokuserer på overførsel af personoplysninger til tredjeland og i særdeleshed USA, og derfor analyseres den vedtagne Privacy Shield- ordning og Safe Harbour-dommen. Safe Harbour-dommen analyseres tillige med bidrag fra Generaladvokatens forslag til afgørelse. Analyse af Safe Harbour-dommen skal bidrage til forståelse af, hvorfor ordningen blev forkastet og om Privacy Shield-ordning lever op til kravene.

Afslutningsvis indeholder afhandlingen en praktisk gennemgang af, hvilke muligheder en dansk virksomhed har for at overføre personoplysninger til tredjelande på nuværende tidspunkt. Herudover indeholder afhandlingen en kortere gennemgang af de trin en dansk virksomhed bør overveje, såfremt virksomheden ikke allerede overholder persondatalovens regler med hensyn til behandling af personoplysninger.

2.1 Historik

I 1979 var Danmark et af de første lande, der indførte regler (Registerlovene), som skulle beskytte personoplysninger – dog var der også andre vesteuropæiske lande, som Sverige, Norge, Vesttyskland og Frankrig, der indførte lignende regler i slut halvfjerdserne.[8]

I 1995 blev Databeskyttelsesdirektivet vedtaget med en implementeringsfrist på 3 år og fik virkning i Danmark i juli 2000 via lov om behandling af personoplysninger.[9] Selve vejen fra vedtagelsen af

[7] http://www.juraplexus.dk/juridisk-leksikon/id.retsdogmatik/i.html - sidst aktiveret den 03.06.2017
[8] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 67
[9] Blume, Persondataretlige grundfigurer, 2017, side 23

direktivet i 1995 og til den danske lov om behandling af personoplysninger var knudret og langvarig. Lovforslaget, som skulle implementere direktivet, blev forberedt af Registerlovsudvalget og forelagt i 1997 i Betænkning 1345.[10] I modsætning til registerlovene (lov om offentlige registre og lov om private registre) af 1979, så ville anvendelsesområdet for den danske lov, der skal implementere Databeskyttelsesdirektivet indeholde en udvidelse, da både manuelle registre og elektronisk behandling af personoplysninger er omfattet.[11] Udvalget anbefalede endvidere at den nye lov burde gælde for både den offentlig og private sektor.[12] Dermed ville to love blive samlet i én og en højere grad af gennemskuelighed sikret.

Efter forlæggelsen af Betænkningen fulgte det første lovforslag (L 82) den 30. april 1998.[13] Lovforslaget nåede aldrig til 2. behandling. Det blev derimod genfremsat som lovforslag (L44),[14] hvor der var foretaget enkelte ændringer og præciseringer – ej heller dette forslag nåede til 2. behandling.[15] Tredje gang var lykkens gang – den 9. december 1999 blev lovforslag (L 147) fremsat, igen med småændringer og præciseringer.[16] Lovforslaget blev den 26. maj 2000 ved. 3.-behandlingen vedtaget med bredt flertal.[17]

Da lov nr. 429 af 31. maj 2000 om behandling af personoplysninger trådte i kraft, bortfaldt de to registerlove samtidigt. Ligeledes vil Databeskyttelsesdirektivet blive ophævet samtidig med at Databeskyttelsesforordningen træder i kraft i 2018.

Den nye betænkning nr. 1565 om Databeskyttelsesforordning 2016/679 indeholder en beskrivelse af, hvordan de nye regler om databeskyttelse skal forstås. Formålet med betænkningen er at sikre, at dansk lovgivning pr. 25. maj 2018 er indrettet i overensstemmelse med Databeskyttelsesforordningens bestemmelser.[18] – selvfølgelig med henblik på at det i løbet af efteråret 2017 er muligt at fremsætte et lovforslag på et oplyst og gennemarbejdet grundlag, så netop dansk lovgivning er i overensstemmelse med forordningen og at forordningens indhold bliver korrekt gennemført. Uanset om Danmark når at vedtage en ny persondatalov, så kan der støttes ret på Databeskyttelsesforordningen fra ikrafttrædelsesdatoen, da en forordning er umiddelbar anvendelig. Er der derimod tale om et direktiv, så skal dette implementeres i dansk lovgivning inden for en given frist og først når implementeringen er sket, kan der støttes ret på direktivet.

[10] Blume, Persondataretlige grundfigurer, 2017, side 19
[11] Betænkning nr. 1345/1997 om behandling af personoplysninger, side 22
[12] Betænkning nr. 1345/1997 om behandling af personoplysninger, side 153
[13] Folketingstidende 1997-1998, 2. samling, tillæg A, side 2097
[14] Folketingstidende 1998-1999, tillæg A, side 1095
[15] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 36-37
[16] Folketingstidende 1999-2000, tillæg A, side 3971
[17] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 37-38
[18] Betænkning nr. 1565 om Databeskyttelsesforordningen, side 10

3. Gældende ret

Som tidligere nævnt, så er lov om behandling af personoplysninger (persondataloven) gældende ret i Danmark og denne lov implementerede Databeskyttelsesdirektivet. Hele pointen med lovgivningen på persondatabeskyttelsesområdet er at sikre den enkelte borgers privatliv.[19] – så med vedtagelsen af persondataloven er de generelle regler for behandling af personoplysninger fastsat. Som udgangspunkt defineres begrebet behandling, som værende al behandling der foretages helt eller delvist via elektronisk databehandling.[20] Udover den elektroniske behandling, så er manuel behandling også omfattet, så længe den er eller bliver indeholdt i et register. Den type oplysninger, der er omfattet af loven, er personoplysninger- herved skal forstås *enhver information om en identificeret eller identificerbar fysisk person*. [21] Databeskyttelsesdirektivet indeholder en række definitioner af persondatabeskyttelsesretlige begreber – samtlige af disse definitioner er indføjet i persondataloven. Dog er de ikke overført sprogligt uændret, men snarere præciseret og afkortet.[22]

Den 25. maj 2018 vil det dog ikke længere være Databeskyttelsesdirektivet, som regulerer reglerne for beskyttelse af personoplysninger i Europa – det vil i stedet været Databeskyttelsesforordningen. Som udgangspunkt viderefører Databeskyttelsesforordningen gældende ret samt moderniserer den en smule.

[19] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 75
[20] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 81
[21] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 87
[22] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 133

4. Overførsel af personoplysninger til et tredjeland

I forbindelse med overførsel af personoplysninger til et tredjeland vil dette afsnit indledningsvis definere begrebet personoplysninger. Dernæst følger en gennemgang af reglerne for behandling af personoplysninger, som leder videre til forståelse af, hvilke behandlinger ordet begrebet overførsel af personoplysninger dækker. Slutteligt omhandler afsnittet en definition af begrebet tredjeland.

4.1 Personoplysninger

I henhold til nuværende gældende dansk lovgivning, så er personoplysninger defineret således:

> ***Personoplysninger:***
> ***Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede)***[23]

Definitionen i persondataloven er meget bred og omfatter derfor alle oplysninger, som kan henføres til en fysisk person. Begrebet identificerbar person kan sammenfattes til en person, som enten direkte eller indirekte kan identificeres ved f.eks. et identifikationsnummer. I Databeskyttelsesdirektivet er dette uddybende bemærket.[24]

> ***››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 bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet.***[25]

I Danmark opereres der i persondataloven med 3 grader af personoplysninger; almindelige, følsomme og semi-følsomme. I Databeskyttelsesdirektivet findes kategorien semi-følsomme oplysninger ikke – der opereres kun med almindelige og følsomme personoplysninger. § 7, stk. 1 i persondataloven angiver en udtømmende liste over de personoplysninger, som karakteriseres som følsomme. Det er oplysninger om; racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk baggrund, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold. Disse oplysninger må ikke behandles.

[23] Lov om behandling af personoplysninger § 3, stk. 1, nr. 1
[24] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 136
[25] Databeskyttelsesdirektivet, artikel 2 (a)

4.1.1 Hvilke oplysninger er omfattet af personoplysningsbegrebet?

For at en oplysninger er omfattet af § 3, stk. 1 i persondataloven, så kan dette ske, hvis f.eks. navn eller adresse er erstattet med en kode og denne kan føres tilbage til den oprindelige individuelle personoplysning. Så længe der kan foretages identifikation, så er måden den foretages på, underordnet. Lønoplysninger er bl.a. omfattet af begrebet personlysninger.[26] Personoplysninger, som er blevet anonymiseret er ikke omfattet af begrebet, så længe det ikke er muligt at identificere den registrerede igen. For at afgøre, om en person er identificerbar, så skal der ved vurderingen medregnes alle de hjælpemidler, som med rimelighed kan forventes anvendt af den dataansvarlige eller enhver anden fysisk person.[27] Datatilsynet blev af Radio- og tv-nævnet anmodet om at tage stilling til et tv-projekt, som indebar, at der ville blive sendt en live-dokumentar fra Vollsmose-området i Odense. Der skulle transmitteres billeder fra et indkøbscenter dagligt til beboelsesområder endvidere ville billederen blive gengivet på storskærm i indkøbscentret. Billedzonen i centret ville blive tydeligt opmærket og kameraerne tydeligt markeret, så det var muligt for den enkelte person at færdes i indkøbscentret uden at blive filmet. Sagen blev behandlet i Datarådet og Datatilsynet udtalte herefter, at hvis der er tale om et billede og der ikke foreligger yderligere oplysninger end selve fotografiet til at identificere den pågældende, så vil billedet være omfattet af persondataloven, da det vil blive betragtet som personhenførbart. – men dog kun hvis det bliver forevist til person, som kan genkende den pågældende person. I og med, at der var tale om en transmission fra et lokalt indkøbscenter til et beboelsesområde i nærheden af centret samt gengivelsen på storskærmen i indkøbscentret, så var det sandsynligt, at nogen vil kunne genkende de filmede personer.[28] Fotos er derfor omfattet af begrebet personoplysninger.

I forbindelse med anvendelse af fingeraftryk til identifikation modtog Datatilsynet en forespørgsel fra BornholmsTrafikken. De havde indført et ny person id-rabatkort "Bornholmerkortet", som var et chipkort, som indeholdte kundens fingeraftryk. Ved ansøgning om erhvervelse af et Bornholmerkort skulle kunden oplyse relevant data om kundens dankort samt underskrive en formular. Ved udstedelse af kortet blev der på grundlag af 19 målepunkter af kundens fingeraftryk udregnet en værdi – og denne værdi lå sammen med kundens kundenummer i chipkortet. Kundenummeret fandtes ligeledes i BornholmTrafikkens bookingsystem. Kundens fingeraftryk lå ikke i chipkortet. BornholmsTrafikken havde ikke en central database, hvor alle de udregnede værdier for kunderne blev opbevaret, de lå alene på kortet. Datatilsynet vurderede, at den udregnede værdi af kundens fingeraftryk, som er lagret i

[26] C-465/00, C-138/01 og C-139/01 – (Österreichischer Rundfunk)
[27] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 136 og Databeskyttelsesforordningen, betragtning 26
[28] Datatilsynets journalnummer 2002-321-0155 – Datatilsynets årsberetning 2002, side 42-43

kundens eget personlige Bornholmerkort betragtes som en personoplysning.[29] Den udregnede værdi af et fingeraftryk er derfor omfattet af begrebet personoplysninger. Det slås endvidere fast i C-291/12 (Michael Schwarz) præmis 26 og 27, at fingeraftryk er omfattet af begrebet personoplysninger.

Personoplysningsbegrebet er "med vilje" fastlagt bredt, dette for at beskytte de oplysninger, som lægger i grænseområdet og som bør beskyttes. Selv en IP-adresse er en personoplysning.[30]

Selvom en person kun er en biperson i forbindelse med behandling af personoplysninger, så er disse personoplysninger også omfattet af begrebet personoplysninger.[31] Som eksempel kan nævnes den situation, hvor en kvinde får kræft. Oplysningerne om kræftforløbet registreres i sygehusets edb-system. Her registreres også oplysninger om hendes nærmeste pårørende (det kunne være hendes mand). Hendes mand har kun en tilknytning til kræftforløbet og registreres i egenskab af at være hendes pårørende. Hans personoplysninger, som er registreret i sygehusets edb-system, er også omfattet af begrebet personoplysninger.[32]

I og med at begrebet personoplysninger er begrænset til kun at omfatte fysiske personer, så omfatter det selvsagt ikke juridiske personer – herunder aktieselskaber, anpartsselskaber osv. Dog er oplysninger om enkeltmandsvirksomheder omfattet af definitionen. Det må derfor kunne udledes, at virksomhedsoplysninger, der kan identificere enkeltpersonen falder ind under definitionen.[33]

I forbindelse med en vurdering af, om oplysninger om afdøde personer er omfattet af begrebet personoplysninger, så er det ikke udtrykkeligt reguleret i Databeskyttelsesdirektivet – det er derimod overladt til medlemsstaterne selv at beslutte i hvilken udstrækning, direktivet finder anvendelse på afdøde personer. Sådanne oplysninger er i Danmark omfattet af persondatalovens regler, det betyder bl.a. at registrerede oplysninger om en person, fortsat vil være omfattet af loven efter personens død. Indsamling og behandling af personlige oplysninger om en afdød person, skal derfor ske i overensstemmelse med lovens bestemmelser. Følgelig kan en række af lovens bestemmelser ikke anvendes, da nogle af lovens regler forudsætter samtykke fra den registrerede person. – det i sig selv er jo en umulighed. Problemer, der måtte opstå hermed er overladt til løsning hos tilsynsmyndighederne, som gennem praksis fastlægger grænserne for lovens anvendelse på døde personer.[34] Datatilsynet slår i Datatilsynets afgørelse: journal nummer 2007-321-0039 fast, at oplysninger om afdøde anses som værende personoplysninger og de skal behandles herefter. Sagen omhandlede Frilandsmuseets

[29] Datatilsynets journalnummer 2003-212-0143 – Datatilsynets årsberetning 2003, side 85-86
[30] Blume, Persondataretten – i en brydningstid, 2014, side 71
[31] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 141
[32] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 141
[33] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 142
[34] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 142-143

forespørgsel angående lovligheden af at oprette en database over modstandsfolk under Danmarks besættelsen og denne skulle publiceres på internettet. Som forudsætning for oprettelse af databasen skulle Frilandsmuseet indhente samtykke fra de levende modstandsfolk og de afdøde kunne først optages i databasen 10 år efter deres død. Derudover skulle Frilandsmuseet fjerne oplysninger om den pågældende afdøde modstandsmand, såfremt nære slægtninge anmodede herom.[35]

Om oplysninger om fostre er omfattet af begrebet personoplysninger, er mere uklart, da det ikke fremgår af persondataloven eller forarbejderne hertil. Et foster har arverettigheder jf. arveloven § 94 og der er ikke fastsat en tidsgrænse for, hvor tidligt i en graviditet at et foster kan betragtes som en registreret.[36] Artikel 29-gruppen har endvidere ved deres vurdering af persondatabegrebet pointeret, at det er op til de nationale retssystemer at afgøre, om oplysninger om fostre er omfattet af persondatabegrebet.[37] Datatilsynet har endnu ikke afgjort sager omhandlende oplysninger om fostre og mangler derfor endnu at fastsætte, hvad og i hvilken udstrækning begrebet personlysninger omfatter.[38]

4.1.2 Personoplysningsbegrebet i den nye databeskyttelsesforordning

I henhold til artikel 4 (1) i Databeskyttelsesforordningen, så skal personoplysninger forstås således:

> ***››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.***

De eneste ændringer i forhold til definitionen af personoplysninger i Databeskyttelsesdirektivet er at; lokaliseringsdata, en onlineidentifikator og genetiske identitet er blevet tilføjet.

Uagtet disse tilføjelser, så anses de ikke for at være en udvidelse af personoplysningsbegrebet, snarere en præcisering, da Artikel 29-gruppen i deres Udtalelse nr. 4/2007 om begrebet personoplysninger,[39] allerede har taget højde for tilføjelserne – de er blot nu skrevet ind i bestemmelsen.

[35] https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/offentliggoerelse-af-oplysninger-om-modstandsfolk-paa-internettet-ii/ - sidst aktiveret den 27.07.2017
[36] Blume, Personoplysningsloven, 2000, side 43
[37] Artikel 29-gruppens udtalelse nr. 4/2007 om begrebet personoplysninger (WP 136), s. 23
[38] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 145
[39] Artikel 29-gruppens udtalelse nr. 4/2007 om begrebet personoplysninger (WP 136), s. 9,11 og 14

4.2 Behandling af personoplysninger

Behandling af personoplysninger defineres som følger:

> ***2) Behandling:***
> ***Enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for.***[40]

I henhold til persondatalovens § 5, stk. 1, så skal personoplysninger behandles i overensstemmelse med god databehandlingsskik.[41] Databeskyttelsesdirektivet indeholder ikke en definition af god databehandlingsskik, men fastsætter dog regler i artikel 6 (1) om, at medlemsstaterne skal fastsætte bestemmelser om, at personoplysninger skal behandles rimeligt og lovligt. Direktivet indeholder i betragtning 38 en slags definition af ***rimelig behandling***; det forudsætter, at de registrerede til enhver tid kan få kendskab til, at der sker en behandling og få oplyst hvad denne behandling omfatter. "God databehandlingsskik", det er det krav, som der i Danmark lægges vægt på, når der skal ske en rimelig behandling af persondata. I Datatilsynets afgørelse: Journalnummer 2007-219-0043, gjorde Datatilsynet det klart, at tv-overvågning af et kollegies fælleskøkken var i strid med princippet om god databehandlingsskik. Formålet med tv-overvågningen var at opklare, hvem der stjal mad fra køkkenet. Fælleskøkkenet kunne efter Datatilsynets opfattelse anses som værende en del af beboernes mere private opholdsrum på kollegiet – især også fordi madlavning på værelserne var forbudt. I forbindelse med at en kommune ved en fejl videregav oplysninger om hemmelige adresser til brug for en vejviser, fandt Datatilsynet, at dette var i strid med god databehandlerskik.[42] Kravet om god databehandlerskik skal vurderes i forhold til den person oplysningerne angår.[43] Ofte vil der ved vurderingen af om kravet om god databehandlerskik er overholdt indgå flere elementer.

Selve indsamlingen af oplysningerne skal ske til udtrykkeligt angivne og saglige formål og en senere behandling af oplysningerne må ikke være uforeneligt med det oprindelige formål jf. § 5, stk. 2 i persondataloven. Artikel 6 (1) litra b i Databeskyttelsesdirektivet indeholder på samme måde denne formålsbestemthed – også kaldet **finalité-princippet**. Formålet med indsamlingen skal være præcist og tilstrækkeligt velfunderet. – og den dataansvarlige må ikke indsamle oplysninger, som han ikke har brug for.[44] – det betyder at den dataansvarlige ikke må indsamle oplysninger, som han måske får brug for i fremtiden. I Datatilsynets afgørelse: Journalnummer 2008-632-0034 havde Forsvarets Personeltjeneste

[40] Lov om behandling af personoplysninger § 3, stk. 1 nr. 2
[41] Lov om behandling af personoplysninger § 5, stk. 1
[42] Datatilsynets journalnummer 2007-632-0006
[43] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 196
[44] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 197

uden samtykke fra medarbejderne videregivet oplysninger om medarbejderens navne, stillingsbetegnelser og privatadresser til Topdanmark. Topdanmark ville anvende oplysningerne til markedsføring, som ville give medarbejderne mulighed for tegne forsikring hos dem. I henhold til § 5, stk. 2, skal indsamlingen af oplysninger ske til et udtrykkeligt angivet og sagligt formål og en senere behandling må ikke være uforeneligt med dette (**finalité-princippet)** – i og med at medarbejderne ikke havde givet deres samtykke til Forsvarets Personeltjeneste til at videregive deres oplysninger til Topdanmark, så er dette klart i strid med § 5, stk. 2. Dog kan indsamlede oplysninger anvendes til senere behandling i historisk, statistisk eller videnskabeligt øjemed, selvom det ikke er foreneligt med det oprindelige formål, når blot det har hjemmel i § 10 i persondataloven.[45]

I henhold til § 5, stk. 3, så skal de oplysninger, der behandles være relevante og tilstrækkelige, og skal ikke indeholde mere end det kræves til opfyldelse af formålet – altså et såkaldt **proportionalitetsprincip**. Databeskyttelsesdirektivet indeholder i artikel 6 (1) litra c identisk ordlyd. I Datatilsynets afgørelse: Journalnummer 2009-631-0099 foretog en fitnesscenter ejer tv-overvågning af herrernes omklædningsrum. Dette med henblik på at minimere/opklare gentagne tyverier/indbrud i de skabe, hvor herrerne opbevarede deres tøj og værdigenstande, mens de var inde og træne. Overvågningen var begrænset til områderne omkring skabene og dermed ikke toilet -og badområderne. Først gør Datatilsynet klart, at personoplysninger skal behandles i overensstemmelse med god databehandlerskik jf. § 5, stk. 1. Derudover pointeres Datatilsynet, at de oplysninger, som behandles skal være relevante og tilstrækkeligt og må ikke omfatte mere end hvad der kræves til opfyldes af det formål. Altså et proportionalitetskrav – dette krav føret til, at det i første gang om overvejes, om der findes mindre indgribende midler end tv-overvågning til at opklare, hvem der stjæler fra omklædningsrummet.

I henhold til § 5, stk. 4, så skal behandling af oplysninger tilrettelægges således, at der skal ske fornøden ajourføring af oplysningerne (**datakvalitet**). Sammenlignelig ordlyd findes i Databeskyttelsesdirektivet artikel 6 (1) litra d. om ajourføringen. Den fornødne kontrol, der kan kræves af databehandleren afhænger klart af oplysningernes karakter. Det er også muligt for den registrerede selv at rette henvendelse til databehandleren for at få slettet, rettet eller blokeret oplysninger jf. § 37 i persondataloven, hvis oplysningerne er urigtige eller vildledende.[46] I forbindelse med Datatilsynets afgørelse: Journalnummer 2008-313-0113, havde en registreret ved hjemkomst til Danmark informeret en kommune om sin nye adresse. I forbindelse med modtagelse af ejendomsspecifikation 3 måneder efter adresseændringen, var den registrerede stadig registreret med den tidligere udenlandske adresse.

[45] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 206
[46] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 207-208

Godt nok modtog den registrerede ejendomsspecifikationen på den korrekte adresse, men på selve specifikationen stod den tidligere adresse. Rykkerskrivelser blev sendt til den tidligere adresse i udlandet. Datatilsynet udtaler, at det er kommunens ansvar at ajourføre den registreredes adresse jf. persondatalovens § 5, stk. 4. Derfor blev kommunen anmodet om at ændre sine procedurer.

I henhold til § 5, stk. 5, så må indsamlede oplysninger ikke opbevares på en måde, der kan identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles[47]. Sammenlignelig ordlyd findes i direktivet artikel 6 (1) litra e. Denne opbevaringsbegrænsning beror på en vurdering af den enkelte situation. I Datatilsynets afgørelse: Journalnummer 2003-313-0180, klagede en registreret over, at et parkeringsselskab (Parkering-København) stadig behandlede oplysninger om ham, selvom han havde betalt sin bøde. Parkering-København forklarede, at de opbevarede oplysningerne i maksimum 5 år, før de blev slettet. Datatilsynet udtalte at; "Det er ikke muligt generelt at beskrive, for hvilke tidsrum opbevaring af identificerbare oplysninger vil kunne ske. Dette afhænger af en konkret vurdering i den enkelte situation" – og at Parkering-København var en del af den offentlige forvaltning og derfor er underlagt forpligtelser med hensyn til opbevaring af sagsakter og registre. Derudover har Parkering-Danmark brug for oplysninger i forbindelse med eventuelle klagesager. Derfor fandt Datatilsynet, at opbevaring af den registreredes oplysninger i op til 5 år ikke var uforeneligt med opbevaringsbegrænsninger i § 5, stk. 5.

4.2.2 Behandlingsbegrebet i den nye databeskyttelsesforordning

I henhold til Databeskyttelsesforordningen skal behandling forstås således:

> ***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*.**[48]

Umiddelbart er artikel 5 i forordningen sammenlignelig med artikel 6 i direktiv 95/96/EF og § 5 i persondataloven. – men der er dog sket visse forandringer, de følger under artikel 5 i forordningen.

[47] Høilund, Persondataloven, en indføring, side 29
[48] Databeskyttelsesforordningen, artikel 4 (2)

Artikel 5

Principper for behandling af personoplysninger

1. Personoplysninger skal:

a) behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«)

b) indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål (»formålsbegrænsning«)

c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (»dataminimering«)

d) være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges (»rigtighed«)

e) opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder (»opbevaringsbegrænsning«)

f) behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

2. Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes (»ansvarlighed«).

Artikel 5 (1) litra a i Databeskyttelsesforordningen er næsten identisk med artikel 6 (1) litra a i Databeskyttelsesdirektivet og som tidligere anført, så er persondataloven baseret på Databeskyttelsesdirektivet og det må derfor antages, at god databehandlerskik fortsat er et udtryk for gældende ret. Ud over den næsten identiske ordlyd i forhold til Databeskyttelsesdirektivet, så indeholder artikel 5 (1) litra a i Databeskyttelsesdirektivet et krav om gennemsigtighed, som er nærmere defineret i betragtning 39 hertil. Gennemsigtighed kræver, at enhver information og kommunikation vedrørende behandling af personoplysninger, skal være lettilgængelige og letforståelige. Der skal benyttes et klart og tydeligt sprog. Gennemsigtighedsprincippet ved navnlig oplysninger om den dataansvarlige og formålet med behandlingen.[49]

Artikel 5 (1) litra b i Databeskyttelsesforordningen er næsten identisk med Databeskyttelsesdirektivet, da ordlyden er næsten ens og det må derfor antages, at der ikke sker ændringer i forståelsen af denne i forbindelse med en ny persondatalov. Dog er der mulighed for viderebehandling til arkivformål i samfundets interesse. Dette er en udvidelse i forhold til de statistiske, videnskabelige eller historiske forskningsformål, som var angivet i Databeskyttelsesdirektivet. Såfremt behandlingen er et led i en retlig forpligtelse, så er der ikke noget i vejen for, at der sker viderebehandling til arkiv formål i samfundets interesse.[50]

Databeskyttelsesforordningen indeholder endvidere i artikel 6 (4) en præcisering af, at der er tre muligheder hvorved en lovlig viderebehandling jf. artikel 5 (1) litra b kan ske. Der er tale om *enten* et samtykke fra den registrerede, *eller* EU-retten eller medlemsstatens nationale ret i overensstemmelse med artikel 23 (1) (begrænsninger af hensyn til statens sikkerhed, forsvaret osv.) *eller* hvis det nye formål ikke er uforeneligt med det oprindelige jf. artikel 6 (4) litra a-e.[51]

Artikel 5 (1) litra c i Databeskyttelsesforordningen er stort set identisk med både § 5 stk. 3 i persondataloven og artikel 6 (1) litra c i Databeskyttelsesdirektivet – dog er ordet senere ikke med i Databeskyttelsesforordningen, men dette er ikke grund til at antage, at der ved den kommende persondatalov, sker ændringer i forståelse af dataminimeringsprincippet. Det kræves at perioden for opbevaring ikke er længere end strengt nødvendigt.[52]

Artikel 5 (1) litra d i Databeskyttelsesforordningen er stort set identisk med artikel 6 (1) litra d i Databeskyttelsesdirektivet. Persondatalovens § 5, stk. 4 er også stort set identisk med artikel 5 (1) litra c i Databeskyttelsesforordningen og det giver derfor ikke anledning til at tro, at der vil ske en ændring af

[49] Databeskyttelsesforordningen, betragtning 39
[50] Databeskyttelsesforordningen, betragtning 45
[51] Betænkning nr. 1565 om Databeskyttelsesforordningen, side 94
[52] Databeskyttelsesforordningen, betragtning 39

forståelsen af denne i den nye persondatalov. Dog benytter der i Databeskyttelsesforordningens artikel 5 (1) litra c en ordlyd, som henviser til, at urigtige oplysninger skal slettes straks og hvor der i persondatalovens § 5, stk. 4 er anført, at sådanne oplysninger skal slettes snarest muligt. Derfor vil sletning af sådanne oplysninger efter ikrafttræden af den nye persondatalov skulle ske straks.

Artikel 5 (1) litra e i Databeskyttelsesforordningen er identisk med § 5, stk. 5 persondataloven og artikel 6 (1) litra e i Databeskyttelsesdirektivet, selvom ordene er opført i ændret rækkefølge, så er det de samme ord, der bliver anvendt og der sker derfor ikke ændringer af denne i forbindelse med den nye persondatalov.

Artikel 5 (1) litra f i Databeskyttelsesforordningen indeholder et nye princip, der sikrer tilstrækkelig fortrolighed og sikkerhed for de pågældende personoplysninger. Hverken Databeskyttelsesdirektivet eller persondataloven indeholder en lignende bestemmelse. I og med dette nye princip er indført, så bliver der sendt et tydeligt tegn om, at sikkerhed omkring behandling af personoplysninger skal være i top.

Artikel 5 (2) i Databeskyttelsesforordningen indeholder en pligt for den dataansvarlige til at kunne påvise, at bestemmelserne i artikel 5 (1) i Databeskyttelsesforordningen overholdes. Det er derved den dataansvarliges ansvar og han skal bevise det.

Der er ikke mange ændringer i Databeskyttelsesforordningens artikel 5 i forhold til gældende lovgivning og de ændringer der er, udvider beskyttelsen af den registrerede og giver den dataansvarlige ansvaret for at reglerne i artikel 5 bliver fulgt.

4.3 Overførsel af personoplysninger

I henhold til § 27 i persondataloven, så kan der kun ske overførelse af personoplysninger til et tredjeland, såfremt dette tredjeland garanterer et tilstrækkeligt beskyttelsesniveau. Men hvordan defineres overførelse? Overførsel skal forstås som videregivelse eller overladelse af oplysninger til modtagere i tredjelande. Videregivelse forstås som overførsel af oplysninger til enhver anden end den registrerede, den dataansvarlige, databehandleren og personer under den dataansvarliges og databehandlerens direkte myndighed. Overladelse forstås som en overførsel til en databehandler eller person under databehandlerens direkte myndighed. Overførsel omfatter også den dataansvarliges

interne anvendelse af oplysningerne. Så overførsel er en samlet betegnelse for overladelse, videregivelse og intern anvendelse.[53]

4.4 Overførsel af personoplysninger til tredjeland

4.4.1 Definition af tredjeland

Persondataloven indeholder en definition af tredjeland

> ***Tredjeland:***
> ***En stat, som ikke indgår i Det Europæiske Fællesskab, og som ikke har gennemført aftaler, der er indgået med Det Europæiske Fællesskab, og som indeholder regler svarende til 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.[54]***

Reglerne om overførsel af personoplysninger findes i artikel 25 og 26 i Databeskyttelsesdirektivet og i § 27 i persondataloven – gengivet nedenfor.

Det vil sige, at en overførsel til et tredjeland (lande uden for EU) skal ske med hjemmel i persondatalovens § 27 og selve behandlingen af personoplysninger med hjemmel i behandlingsafsnittene i persondataloven.

Persondatalovens § 27

> ***§ 27. Der må kun overføres oplysninger til et tredjeland, såfremt dette land sikrer et tilstrækkeligt beskyttelsesniveau, jf. dog stk. 3.***
>
> ***Stk. 2. Vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, sker på grundlag af samtlige de forhold, der har indflydelse på en overførsel, herunder navnlig oplysningernes art, behandlingens formål og varighed, oprindelseslandet og det endelige bestemmelsesland, samt de retsregler, regler for god forretningsskik og sikkerhedsforanstaltninger, som gælder i tredjelandet.***
>
> ***Stk. 3. Ud over de i stk. 1 nævnte tilfælde kan der overføres oplysninger til et tredjeland, såfremt***
>
> ***1) den registrerede har givet udtrykkeligt samtykke,***
>
> ***2) overførsel er nødvendig af hensyn til opfyldelsen af en aftale mellem den registrerede og den dataansvarlige eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en sådan aftale,***

[53] https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/spoergsmaal-om-behandling-af-personoplysninger-i-forbindelse-med-whistleblowing/, sidst aktiveret den 30.07.2017
[54] Persondataloven § 3, stk. 1, nr. 9

3) overførsel er nødvendig af hensyn til indgåelsen eller udførelsen af en aftale, der i den registreredes interesse er indgået mellem den dataansvarlige og tredjemand,

4) overførsel er nødvendig eller følger af lov eller bestemmelser fastsat i henhold til lov for at beskytte en vigtig samfundsmæssig interesse eller for, at et retskrav kan fastlægges, gøres gældende eller forsvares,

5) overførsel er nødvendig for at beskytte den registreredes vitale interesser,

6) overførsel finder sted fra et register, der ifølge lov eller bestemmelser fastsat i henhold til lov er tilgængeligt for offentligheden eller for personer, der kan godtgøre at have en berettiget interesse heri, i det omfang de i lovgivningen fastsatte betingelser for offentlig tilgængelighed er opfyldt i det specifikke tilfælde,

7) overførsel er nødvendig af hensyn til forebyggelse, efterforskning og forfølgning af strafbare forhold samt straffuldbyrdelse og beskyttelse af sigtede, vidner eller andre i sager om strafferetlig forfølgning eller

8) overførsel er nødvendig af hensyn til den offentlige sikkerhed, rigets forsvar eller statens sikkerhed.

Stk. 4. Uden for de i stk. 3 nævnte tilfælde kan tilsynsmyndigheden give tilladelse til, at der overføres oplysninger til tredjelande, som ikke opfylder stk. 1, såfremt den dataansvarlige yder tilstrækkelige garantier for beskyttelse af de registreredes rettigheder. Der kan fastsættes nærmere vilkår for overførslen. Tilsynsmyndigheden underretter Europa-Kommissionen og de øvrige medlemsstater om tilladelser meddelt i henhold til denne bestemmelse.

Stk. 5. Reglerne i denne lov finder i øvrigt anvendelse ved overførsel af oplysninger til tredjelande efter stk. 1, 3 og 4.

Persondatalovens § 27 tager udgangspunkt i Databeskyttelsesdirektivets artikel 25 og 26.

Databeskyttelsesforordningen artikel 44 indeholder et generelt princip for overførsler.

Enhver overførsel af personoplysninger, som underkastes behandling eller planlægges behandlet efter overførsel til et tredjeland eller en international organisation, må kun finde sted, hvis betingelserne i dette kapitel med forbehold af de øvrige bestemmelser i denne forordning opfyldes af den dataansvarlige og databehandleren, herunder ved videreoverførsel af personoplysninger fra det pågældende tredjeland eller den pågældende internationale organisation til et andet tredjeland eller en anden international organisation. Alle bestemmelserne i dette kapitel anvendes for at sikre, at det beskyttelsesniveau, som fysiske personer garanteres i medfør af denne forordning, ikke undermineres.

Forskellen på princippet i Databeskyttelsesforordningens artikel 44 og principperne i Databeskyttelsesdirektivets artikel 25 er, at i Databeskyttelsesforordningen er det specifikt nævnt, at internationale organisationer er omfattet samt der anvendes ordet overførsel frem for videregivelse, som anvendes i Databeskyttelsesdirektivet. Persondatalovens § 27 anvender også ordet overførsel. At internationale organisationer er omfattet anses ikke som værende en ændring, blot en præcisering af

ordlyden.[55] Uanset, at der anvendes ordet videregivelse for "overførsel" til tredjelandet, så ændrer det ikke på den måde, hvorpå begrebet skal forstås. Overførsel er en samlet betegnelse for videregivelse, overladelse og intern anvendelse.[56]

Både persondataloven og Databeskyttelsesdirektivets bestemmelser om overførsel af personoplysninger til tredjelande har vist sig at være formuleret på en måde, som har krævet en del retspraksis for at fastlægge rækkevidden af, hvad der skal til for et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau. Se nærmere herom i afsnit 5 Safe Harbor og 6.1 Privacy Shield. I øjeblikket sikrer følgende tredjelande et tilstrækkeligt beskyttelsesniveau: Andorra, Argentina, Australien, Canada, Færøerne, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Schweiz, Uruguay, USA – dog flere med visse begrænsninger.[57] Disse lande betegnes de såkaldte sikre tredjelande.

Derudover er det relevant at se på, hvornår der reelt set er sket en overførsel til et tredjeland. Sagen C-101/01 Lindquist omhandlede en svensk kvinde (Bodil Lindquist), der beskæftigede sig med forberedelse af konfirmander. Hun oprettede en hjemmeside, hvor både hendes egne og 18 andre kollegaerne oplysninger fremgik – herunder oplysninger om arbejdsopgaver, navne, efternavne, telefonnumre, familieforhold og i et en enkelt tilfælde oplysninger om en kvinde, som var sygemeldt pga. en fodskade. Bodil Lindquist havde hverken oplyst om eksistensen af hjemmesiden til de opførte personer eller indhentet samtykke fra de opførte personer på hjemmesiden[58]. Spørgsmålet var, om der forelå overdragelse af personoplysninger til et tredjeland i og med at oplysningerne var tilgængelige på en hjemmeside og kan tilgås af personer i tredjelande?[59] Domstolen afviste, at der skulle foreligge videregivelse til et tredjeland, når der blev lagt oplysninger op på internettet i en medlemsstat i EU.[60]

Med den nye Databeskyttelsesforordnings § 45 er der fastlagt hvilke elementer, som skal indgå i forbindelse med vurdering af om tredjelandets beskyttelsesniveau er tilstrækkeligt.

De er;

- ***Retsstatsprincippet, respekt for menneskerettighederne og de grundlæggende frihedsrettigheder...***
- ***Tilstedeværelse af en eller flere velfungerende uafhængige tilsynsmyndigheder i tredjelandet...***

[55] Betænkning nr. 1565 om Databeskyttelsesforordningen, side 638
[56] Betænkning nr. 1565 om Databeskyttelsesforordningen, side 631
[57] https://www.datatilsynet.dk/erhverv/tredjelande/sikre-tredjelande/, sidst aktiveret den 02.08.2017
[58] C-101/01 (Lindquist), præmis 12, 13 og 14
[59] C-101/01 (Lindquist), præmis 52
[60] C-101/01 (Lindquist), præmis 171

- ***De internationale forpligtelser, som tredjelandet har påtaget sig i forbindelse med beskyttelse af personoplysninger…***[61]

4.2 Sammenfatning om overførsel af personoplysninger til tredjelande

En personoplysning er enhver oplysning, som enten har identificeret eller kan identificere en fysisk person. En oplysning, der kan identificere en fysisk person, kan være; et billede, en kodet adresse – hvis den kan afkodes igen, et fingeraftryk, DNA, lønoplysninger, en IP-adresse osv. Den fysiske person er afgrænset til at være den registrerede selv, bipersoner, afdøde personer og fostre og i forbindelse med juridiske personer; enkeltmandsvirksomheder. Det vil sige, at persondataloven kun finder anvendelse på denne personkreds.

Behandling af personoplysninger skal ske under iagttagelse af god databehandlerskik og selve skal ske til udtrykkeligt angivne og saglige formål og en senere behandling af oplysningerne må ikke være uforeneligt med det oprindelige formål – også kaldet **finalité-princippet.** De oplysninger, der behandles skal være relevante og tilstrækkelige, og skal ikke indeholde mere end det kræves til opfyldelse af formålet – altså det såkaldte **proportionalitetsprincip**. Endvidere skal behandling af oplysninger tilrettelægges således, at der skal ske fornøden ajourføring af oplysningerne (**datakvalitet**).

Overførsel er en samlet betegnelse for videregivelse, overladelse og intern anvendelse.

Et tredjeland er enhver stat uden for EU. Overførsel til et tredjeland forudsætter, at tredjelandet kan sikre et tilstrækkeligt beskyttelsesniveau af de overførte personoplysninger.

Generelt er overførsel af personoplysninger til tredjelandet med ændringerne i Databeskyttelsesforordningen en videreudvikling og præcisering af allerede gældende ret. Det er kapitel 5 i Databeskyttelsesforordningen, som indeholder de forskellige overførselsgrundlag, som kan anvendes i forbindelse med overførsel af personoplysninger til tredjelande. Blandt andet så indeholder Databeskyttelsesforordningens artikel 47 regler for Binding Corporate Rules og artikel 46 (2) litra b for Standardkontrakter, som vil blive gennemgået i afsnit 6.2.

[61] Databeskyttelsesforordningen, artikel 45, (2) litra a, b og c

5. Safe Harbor-ordningen

Før Privacy Shield-ordningen blev vedtaget, var Safe Harbor-ordningen gældende. Ordningen tillod at virksomheder inden for EU kunne overføre personoplysninger til virksomheder i USA, såfremt disse havde tilsluttet sig ordningen.

5.1 Før Safe Harbor-dommen

Vedtagelsen af Databeskyttelsesdirektivet førte et krav fra USA om særlovgivning med sig. USA var af den overbevisning, at direktivet ville resultere i handelsbarrierer mellem EU og USA, da det efter USA's mening medførte en uacceptabel begrænsning af den frie handel. USA havde på intet tidspunkt ytrer, at de ville implementere national lovgivning, som svarer til det i direktivet.[62] USA fremsatte derimod krav om særlovgivning – havde det været en lille land i stedet for en supermagt, der havde fremsat dette krav, ville det sikkert ikke blive imødekommet. Safe Harbor–ordningen blev hermed født – det er grundlæggende en aftale, som alt andet lige diskriminerer andre tredjelande – da de ikke har mulighed for at indgå en sådan aftale.[63]

Ordningen er hjemlet i artikel 25 (1) i Databeskyttelsesdirektivet, hvor Kommissionen traf beslutning om dataeksport til USA. Amerikanske private virksomheder kunne frit vælge, om de ville tilslutte sig Safe Harbor-ordningen – valgte en virksomhed at gøre dette, så skulle virksomheden efterleve Safe Harbor-principperne. [64] Virksomheden ville hermed blive en såkaldt *sikker havn* – hvor virksomheden levede op til betingelsen i artikel 25 (1) i Databeskyttelsesdirektivet om et tilstrækkeligt beskyttelsesniveau af persondataoplysningerne. Safe Harbor-principperne, som virksomheden skulle overholde, var 7 hovedprincipper: oplysningspligt, valgfrihed, videre overførsel, sikkerhed, data-integritet, indsigt og håndhævelse. – og i sammenspil med 15 FAQ (frequently asked questions) dannede de rammen for ordningen. Særligt relevant i principperne var virksomhedernes pligt til at oplyse fysiske personer om formålet med indsamling af personoplysningerne samt anvendelsen heraf, klagevejledning, muligheder for begrænsning af anvendelse eller videregivelse af personoplysningerne.[65] – Herudover skulle der af virksomheden indhentes udtrykkelig godkendelse fra den registrede forud for behandling af følsomme personoplysninger.[66] Uanset at virksomhederne forpligtede sig til at overholde de i beslutning 2000/520/EF principper, så kunne der være modstridende forpligtelser, som medvirkede til, at hensyn til

[62] Blume, Retlig regulering af internationale persondataoverførsler, 2006, side 144-145
[63] Blume, Retlig regulering af internationale persondataoverførsler, 2006, side 145
[64] Kommissionens beslutning af 26. juli 2000 (2000/520/EF) i henhold til Europa-Parlamentets og Rådets direktiv 95/46EF, side 10, bilag 1 – afsnit 3
[65] Kommissionens beslutning af 26. juli 2000 (2000/520/EF i henhold til Europa-Parlamentets og Rådets direktiv 95/46EF, side 11, bilag 1 – afsnit 4
[66] Kommissionens beslutning af 26. juli 2000 (2000/520/EF i henhold til Europa-Parlamentets og Rådets direktiv 95/46EF, side 11, bilag 1 – afsnit 6

statens sikkerhed, almenvellet eller opretholdelse af lov og orden begrænsede overholdelse af principperne.[67]

Safe Harbor-ordningen anses ikke for at have været en ubetinget succes, da mange amerikanske virksomheder fandt det svært at bruge ordningen.[68]

5.2 Safe Harbor-dommen

5.2.1 Sagens omstædigheder

Maximillian Schrems var en østrigsk statsborger, som boede i Østrig og som havde været bruger af Facebook (socialt medie) siden 2008. For at en person kunne gøre brug af Facebook som borger i en medlemsstat i EU, var brugeren forpligtet til at indgå en aftale med Facebook Ireland, som var et datterselskab til Facebook Inc., der havde hjemsted i USA. Personoplysninger, der vedrører de Facebook-brugere, som havde bopæl i en medlemsstat overførtes helt eller delvist til servere i USA, som tilhørte Facebook Inc. – og her var personoplysningerne genstand for en behandling.[69]

Maximillian Schrems indgav den 25. juni 2013 en klage til den irske tilsynsmyndighed, hvor han gjorde gældende i lyset af Edward Snowdens afsløringer, at amerikansk ret og praksis ikke beskytter de data, som opbevares i USA. Af Snowdens afsløringer fremgik det, at NSA havde iværksat et program (PRISM), som gav NSA fri adgang til alt data, som blev opbevaret på servere i USA.[70]

Den irske tilsynsmyndighed afviste klagen på baggrund af Kommissionens beslutning 2000/520 – hvor det var blevet fastslået, at USA sikrede et tilstrækkeligt beskyttelsesniveau, så længe virksomheden havde tiltrådt Safe Harbor-ordningen og det havde Facebook. [71] Maximillian Schrems anlagde herefter sag ved High Court i Irland, som valgte at forelægge to præjudicielle spørgsmål for Domstolen.

> ***1, Er en uafhængig person – der ved lov er tillagt opgaven med administration og håndhævelse af databeskyttelseslovgivningen – ved vurderingen af en klage, der er blevet indgivet til den pågældende, over, at personoplysninger overføres til et tredjeland (i dette tilfælde USA), hvis lovgivning og praksis det påstås ikke indeholder tilstrækkelig beskyttelse for datasubjektet, fuldstændigt bundet af konklusionen i en fælleskabsundersøgelse, hvor det konkluderes det modsatte, og som er indeholdt i beslutning***

[67] Kommissionens beslutning af 26. juli 2000 (2000/520/EF i henhold til Europa-Parlamentets og Rådets direktiv 95/46EF, side 10, bilag 1 – afsnit 4
[68] Blume, Retlig regulering af internationale persondataoverførsler, 2006, side 147
[69] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 26 og 27
[70] Forslag til afgørelse fra generaladvokat Y. Bot fremsat den 23. september 2015 i sag C-362/14 (Safe Harbor), præmis 25 og 26
[71] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 29

2000/520, henset til chartrets artikel 7, […] 8 og […] 47, og dette trods bestemmelserne i artikel 25, stk. 6 i direktiv 95/46?

2, Eller alternativt kan og/eller skal den person, der varetager hvervet, foretage en egen undersøgelse af forholdet i lyset af den mellemliggende udvikling i de faktiske omstændigheder, der har fundet sted, siden Kommissionens beslutning blev offentliggjort? [72]

Sammenfattende, så bad den irske High Court Domstolen om at tage stilling til, om i det tilfælde, hvor der er truffet en beslutning af Kommissionen (2000/520) om at overførsel af personoplysninger til et tredjeland er tilstrækkeligt sikret, forhindrerede det så, at den nationale domstol/tilsynsmyndigheder kunne behandle en persons anmodning om prøvelse af denne beslutning. – de præjudicielle spørgsmål angår derved rækkevidden af *de nationale databeskyttelsesmyndigheders undersøgelsesbeføjelser, når Kommissionen har vedtaget en tilstrækkelighedsbeslutning.* [73]

5.2.2 Domstolens argumentation for efterprøvelse af Kommissionens beslutning (Safe Harbor)

I henhold til Databeskyttelsesdirektivets artikel 25, (1), så må personoplysninger kun videregives til et tredjeland, såfremt dette tredjeland sikrer et tilstrækkeligt beskyttelsesniveau. I betragtning 57 til Databeskyttelsesdirektivet bliver det endvidere præciseret, at såfremt et tredjeland ikke kan sikre et tilstrækkeligt beskyttelsesniveau, så forbydes videregivelse af personoplysninger til dette tredjeland. Kommissionen kan med hjemmel i artikel 25, (6) vedtage en afgørelse, hvor det fastslås, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau.[74]

Artikel 25 (6)

Kommissionen kan efter proceduren i artikel 31, stk. 2, fastslå. At et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med denne artikels stk. 2, på grundlag af dets nationale lovgivning eller dets internationale forpligtelser med henblik på at beskytte privatlivet og personers grundlæggende rettigheder og frihedsrettigheder, herunder de forpligtelser, der er indgået efter de i stik 5 nævnte forhandlinger.

Medlemsstaterne træffer de foranstaltninger, der er nødvendige for at efterkomme Kommissionens afgørelse.

Artikel 25 (6) indeholdt ifølge Domstolen følgende generelle krav:

[72] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 36
[73] Forslag til afgørelse fra generaladvokat Y. Bot fremsat den 23. september 2015 i sag C-362/14 (Safe Harbor), præmis 57
[74] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 51

1, tredjelandet skal sikre et tilstrækkeligt beskyttelsesniveau på grundlag af dets nationale lovgivning eller dets internationale forpligtelser.

2, vurderingen af, om beskyttelsesniveauet i tredjelandet, sker med henblik på beskyttelse af personers grundlæggende rettigheder og frihedsrettigheder og privatlivet. [75]

3, Sikre et fortsat højt niveau for beskyttelse af personoplysninger, som er fastsat i chartrets artikel 8, stk. 1 ved gennemføres ved denne forpligtelse i artikel 25 (6).[76]

Domstolen anførte endvidere, at selvom artikel 25 (6) i Databeskyttelsesdirektivet ikke indeholder et krav om, at et tredjeland skal sikre et beskyttelsesniveau, som er identisk med det, som er gældende i Unionen, så skal udtrykket tilstrækkeligt beskyttelsesniveau, forstås således, at et tredjeland skal sikre et beskyttelsesniveau for frihedsrettighederne og de grundlæggende rettigheder, som i det væsentligste svarer til det i Unionen.[77] Domstolen anførte herudover også, at selvom tredjelandet anvender andre midler end en medlemsstat i Unionen til overholdelse af de krav, som følger af Databeskyttelsesdirektivet, så skal tredjelandets midler være effektive, så de sikrer en beskyttelse af personoplysninger, som svarer til den, der er gældende i Unionen.[78]

En afgørelse vedtaget af Kommissionen i henhold til artikel 25 (6) i Databeskyttelsesdirektivet skal revurderes med jævne mellemrum for at sikre, at der til stadighed er et tilstrækkeligt beskyttelsesniveau af personoplysningerne i tredjelandet.[79] – derudover skal vurderingen af gyldigheden af Kommissionens afgørelse i henhold til artikel 25 (6) i direktiv 95/46 også omfatte begivenheder, der indtruffet efter vedtagelsen af afgørelsen.[80] –slutteligt anførete Domstolen, at efterprøvelsen skal vurderes strengt.[81]

5.2.3 Domstolens efterprøvelse af Safe Harbor

Selve prøvelsen af Safe Harbor-beslutningen indledtes med en gennemgang af artikel 1 (1) i beslutning 2000/520, hvor Kommissionen anførte, at de i bilag 2 til beslutningen omhandlede FAQ sikrer et tilstrækkeligt beskyttelsesniveau af personoplysninger, som videregives fra Unionen til USA.[82] En virksomhed i USA, som ønskede at tilslutte sig til Safe Harbor-ordningen, skulle gøres dette på grundlag af et selvcertificeringssystem. At Safe Harbor-ordningen var baseret på et selvcertificeringssystem, var i

[75] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 71
[76] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 72
[77] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 73
[78] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 74
[79] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 76
[80] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 77
[81] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 78
[82] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 79

sig selv ikke grund til at USA ikke sikrede tilstrækkeligt beskyttelsesniveau af personoplysninger, så længe at kontrolforanstaltninger muliggjorde sanktioner af eventuelle tilsidesættelser af reglerne om et tilstrækkeligt beskyttelsesniveau.[83] I og med at Safe Harbor-ordningen kun fandte anvendelse for virksomheder i USA, som modtog personoplysninger fra EU, så var ingen af Safe Harbor-principperne gældende for amerikanske offentlige myndigheder, da de ikke havde mulighed for at tilslutte sig ordningen. Derfor var de amerikanske offentlige myndigheder ikke underlagt kravene i Safe Harbor-ordningen.[84]

Domstolen pointerede endvidere, at artikel 2 i beslutning 2000/520 kun vedrørte tilstrækkeligheden af beskyttelsesniveauet af personoplysninger i USA, mens den amerikanske retsorden ikke blev omtalt. – herunder, hvilke tiltag, som USA havde besluttet at indføre, for at sikre et tilstrækkeligt beskyttelsesniveau af personoplysninger.[85] Det var endvidere anført i fjerde afsnit til bilag 1 i beslutning 2000/520, at Safe Harbor-principperne kunne begrænses til et niveau, som er sekundært i forhold til *statens sikkerhed, almenvellet eller opretholdelsen af lov og orden.*[86] – hvilket jo helt firkantet betyder, at statens sikkerhed, almenvellet eller opretholdelsen af lov og orden havde forrang for principperne i Safe Harbor-ordningen, og at disse skulle vige, såfremt de er uforenelige med statens sikkerhed, almenvellet eller opretholdelsen af lov og orden.[87] Domstolen påpegede endvidere, at det i beslutning 2000/520 ikke fremgår, om der i USA fandtes regler af statslig karakter, som begrænsede eventuelle indgreb i de grundlæggende rettigheder hos de EU-borgere, hvis oplysninger blev videregivet fra EU til USA. – samt hvilke indgreb, som de statslige myndigheder i USA havde beføjelse til at foretage, når der forfulgtes legitime mål, som fx statens sikkerhed.[88] Slutteligt vedrørende beslutning 2000/520 tilføjede Domstolen, at det ikke fremgik, at USA havde en effektiv domstolsbeskyttelse mod indgreb i de grundlæggende rettigheder hos de personer, hvis oplysninger blev videregivet til USA fra Unionen. – voldgiftsreglerne, der var anført i beslutning 2000/520 angår handelstvister og ikke tvister om lovligheden af de indgreb i de grundlæggende rettigheder, der følger af statslige foranstaltninger.[89]

Domstolen havde i sin analyse fastslået, at amerikansk lovgivning har forrang for Safe Harbor-principperne, og dermed havde de amerikanske myndigheder mulighed for at få adgang til de fra EU til USA videregivne personoplysninger. Dette var helt i tråd med Kommissionens egen vurdering, hvor Kommissionen også fastslog, at myndighederne i USA havde mulighed for at behandle de videregivne

[83] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 80-81
[84] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 82
[85] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 83
[86] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 84
[87] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 86
[88] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 88
[89] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 89

personoplysninger i strid med formålet – og behandlingen gik videre ned, hvad der var strengt nødvendigt.[90]

For at beskytte de i chartrets artikel 7 og 8 grundlæggende rettigheder, så skal der fastsættes klare og præcise regler, når EU-lovgivning indebærer et indgreb i disse. Reglerne skal regulere anvendelse og rækkevidden samt opstille mindstekrav for overholdelse, som minimere et misbrug af disse .[91] – endvidere skal beskyttelsen begrænses til det strengt nødvendige.[92]

Kommissionens vedtagelse af en afgørelse i henhold til artikel 25 (6) i Databeskyttelsesdirektivet kræver, at USA sikrede et beskyttelsesniveau for de grundlæggende rettigheder, som i det væsentligste svarer til det niveau, som er sikret i EU.[93] Kommissionen anførte ikke i beslutning 2000/520, at USA sikrede et tilstrækkeligt beskyttelsesniveau.[94]

Domstolen fastslog herefter, at det ikke var nødvendigt at undersøge indholdet af Safe Harbor-principperne, da der allerede i artikel 1 i beslutningen tilsidesættes de krav, som er fastsat i artikel 25 (6) i Databeskyttelsesdirektivet sammenholdt med chartret og at den som følge heraf er ugyldig.[95]

Med hensyn til spørgsmålet om hvorvidt de nationale tilsynsmyndigheder kan behandle enhver anmodning om beskyttelse af en persons grundlæggende rettigheder i forhold til behandling af personoplysninger, så fastsatte artikel 3 (1) første afsnit i beslutning 2000/520 en særlig ordning hertil.[96] Artikel 3 (1) i beslutning 2000/520 fratog de nationale myndigheder beføjelserne til at behandle en anmodning fra en borger, som rejser tvivl om, hvorvidt et tredjeland sikrede et tilstrækkeligt beskyttelsesniveau.[97] – dette er i strid med artikel 25 (6) i Databeskyttelsesdirektivet, da denne ikke giver Kommissionen kompetence til at begrænse de nationale tilsynsmyndigheders beføjelser.[98]

Domstolen fastslog, at Kommissionen ved at vedtage artikel 3 i beslutning 2000/520 derfor havde overskredet grænserne for dens kompetence efter artikel 25 (6) i direktiv 95/46 – og bestemmelsen blev som følge heraf erklæret ugyldig.[99]

[90] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 90
[91] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 91
[92] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 92
[93] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 96
[94] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 97
[95] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 98
[96] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 100
[97] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 102
[98] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmiss 103
[99] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 104

Da det ikke var muligt at adskille artikel 1 og 3 fra artikel 2 og 4 i og fra bilagene til beslutning 2000/520, så var hele Safe Harbor-ordningen ugyldig.[100] Domstolen fulgte herved Generaladvokat Y. Bot's forslag til afgørelse. [101]

5.3 Analyse af Safe Harbor-dommen

Domstolen pointerer i den afsagt dom (C-362/14), at der i Databeskyttelsesdirektivet ikke findes en definition af tilstrækkeligt beskyttelsesniveau og at det beror på en vurdering.[102] Imidlertid fremgår det lige herefter i dommen (C-362/14), ***at artikel 25 (6) i direktiv 95/46 kræver, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau på baggrund af dets nationale lovgivning eller dets internationale forpligtelser***. – samt **at *vurderingen af, om beskyttelsesniveauet i tredjelandet er tilstrækkeligt, sker med henblik på at beskytte privatlivet og personers grundlæggende rettigheder og frihedsrettigheder.***[103] Selvom Domstolen gør klart, at det ikke kan kræves, at et tredjeland sikrer et beskyttelsesniveau, der er identisk med det, som er sikret i Unionen, så definerer Domstolen tilstrækkeligt beskyttelsesniveau som følger: ***at der opstiller et krav om, at dette tredjeland på grundlag af dets nationale lovgivning eller dets internationale forpligtelser faktisk sikrer et beskyttelsesniveau for frihedsrettighederne og de grundlæggende rettigheder, som i det væsentlige svarer til det niveau, der er sikret inden for Unionen i medfør af direktiv 95/46 sammenholdt med chartret.*** [104] Ud fra dette analyseres de enkelte elementer i Domstolens definition af indholdet i artikel 25 (6) i Databeskyttelsesdirektivet.

Generaladvokat Y. Bot gør i sit forslag til afgørelse klart, at det kun kan konkluderes, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, såfremt der foretages en helhedsvurdering af gældende ret og praksis i det pågældende tredjeland.[105]

Domstolen forklarer, at Safe Harbor-principperne kun kan anvendes på private virksomheder i USA, som har tilsluttet sig ordningen og derved modtager personoplysninger fra EU. – der er intet krav jf. beslutning 2000/520 om, at de amerikanske offentlige myndigheder overholder principperne.[106] Det gøres endvidere klart, at beslutning 2000/520 kun vedrører beskyttelse, der opnås i USA – men ingen konstateringer af på hvilket grundlag USA i sig selv sikrer et tilstrækkeligt beskyttelsesniveau.[107] Det er

[100] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 105-106
[101] Forslag til afgørelse fra generaladvokat Y. Bot fremsat den 23. september 2015 i sag C-362/14 (Safe Harbor), præmis 237
[102] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 70
[103] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 71
[104] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 73
[105] Forslag til afgørelse fra generaladvokat Y. Bot fremsat den 23. september 2015 i sag C-362/14 (Safe Harbor), præmis 141
[106] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 82
[107] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 83

tidligere slået fast, at vurdering af tilstrækkelig beskyttelsesniveau i henhold til artikel 25 (6) i Databeskyttelsesdirektivet skal ske på baggrund af national lovgivning. Det er derfor problematisk, at Kommissionen i beslutning 2000/520 ikke inddrager USA's nationale lovgivning. Domstolen bemærker derudover, at når et tredjeland anvender et selvcertificeringssystem, så er dette ikke i sig selv i strid med artikel 25 (6) i Databeskyttelsesdirektivet så længe, at der er indført effektive afslørings- og kontrolmekanismer, som sikrer beskyttelse af personoplysninger – og dette er sikret af tredjelandet. [108] Slutteligt, så anfører Domstolen, at beslutning 2000/520 har den betydning, at de begrænsninger, som er anført i bilag 1, 4. afsnit til beslutning 2000/520, har forrang for Safe Harbor-principperne. Det betyder, at de selvcertificerede virksomheder, som har tilsluttet sig ordningen, har pligt til at se bort fra principperne, når hensyn til statens sikkerhed, almenvellet eller opretholdelse af lov og orden i USA taler for det.[109]

For at vurdere, om et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, så er det ikke tilstrækkeligt kun at vurdere reglerne for overførsel af personoplysningerne til et tredjeland er overfyldt – derimod skal det også vurderes, om et effektivt håndhævelsessystem er vedtaget, så reglerne i praksis også bliver overholdt.[110]

Det kan af Domstolens præmisser samt Artikel 29 gruppens udtalelser udledes, at det er tredjelandet som helhed, der skal sikre et tilstrækkeligt beskyttelsesniveau jf. artikel 25 (6) i Databeskyttelsesdirektivet og ikke kun "ordningen" (Safe Harbor). Det er særdeles vigtigt at vurdere tredjelandets nationale lovgivning, så der opnås en forenelighed med kravet om sikring af tilstrækkeligt beskyttelsesniveau af tredjelandet.

Kommissionen havde i beslutning 2000/520 ej heller konstateret, om der foreligger en effektiv domstolsbeskyttelse, såfremt der foretages indgreb i de grundlæggende rettigheder hos de personer, hvis personoplysninger er blevet videregivet eller kan videregives til USA.[111] Beslutning 2000/520 indeholder kun domstolsregler, såfremt der er tale om illoyal eller vildledende adfærd eller praksis på handelsområdet.[112]

Endvidere har Domstolen fastslået, at grundet det beskyttelsesniveau, som et tredjeland sikrer, kan ændre sig, så er Kommissionen forpligtet til at undersøge med jævne mellemrum at

[108] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 81
[109] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 86
[110] Artikel 29 gruppens arbejdsdokument af den 24. juli 1998 (WP12/1998), side 5, afsnit 2
[111] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 87, 88 og 89
[112] Forslag til afgørelse fra generaladvokat Y. Bot fremsat den 23. september 2015 i sag C-362/14 (Safe Harbor), præmis 205

beskyttelsesniveauet opretholdes og især, hvis det kommer til Kommissionens kendskab, at der er tvivl om opretholdelse af beskyttelsesniveauet.[113]

Generaladvokat Y. Bot gør i sit forslag til afgørelse opmærksom på, at undtagelserne i bilag 1 til beslutning 2000/520 i sig selv udgør et indgreb i de grundlæggende rettigheder, som er beskyttet i Chartrets artikel 7, 8 og 47.[114] Artikel 7 i Chartret indeholder bestemmelser om respekt for privatliv og familieliv, artikel 8; beskyttelse af personoplysninger og artikel 47: adgang til effektive retsmidler og til en upartisk domstol. Dette understøtter generaladvokaten med for det første, at unionsborgere ikke har nogen effektiv høringsret i USA med hensyn til overvågning og indsamling af deres af deres oplysninger, deres føres tilsyn, men dette på et hemmeligt grundlag, som samlet set ikke er i overensstemmelse med Chartrets artikel 47.[115] For det andet anses den brede formulering af begrænsningerne i bilag 1 til beslutning 2000/520, hvorved de amerikanske efterretningstjenester kan få adgang til de overførte oplysninger, som værende en krænkelse af det væsentligste indhold af Chartrets artikel 7 og 8.[116] For det tredje, når nu indgrebet er konstateret og det skal vurderes om det svarer til et mål af almene interesser, så skal indgrebet i henhold til tilladelsen kun overtræde Safe Harbor-principperne i det omfang, som er nødvendigt for at tilgodese legitime interesser.[117] I og med at de legitime interesser ikke præciseres nærmere, så hersker der usikkerhed med hensyn til rækkevidden af anvendelsesområdet for denne undtagelse.[118] Det er derfor generaladvokatens opfattelse, at i og med, at rækkevidden af undtagelsen ikke er præcist fastlagt, at undtagelsen strider imod Chartrets artikel 7 og 8.

Domstolen fulgte generaladvokat Y. Bots argumentation og anførte i dommen (C-362/14), at en lovgivning, hvor intet er til hinder for opbevaring af samtlige personoplysninger fra samtlige personer, hvis oplysninger er blevet videregivet fra Unionen til USA og hvor offentlige myndigheder har mulighed for at få adgang til disse, hvor et veldefineret formål forfølges, er ikke begrænset til det strengt nødvendige.[119]

Derudover pointerede Domstolen, at en lovgivning, som gør det muligt for offentlige myndigheder i et tredjeland at få adgang til personoplysningerne, anses som et indgreb af den grundlæggende ret til respekt for privatlivet, som den er sikret i Chartrets artikel 7.[120] Udover at den nationale lovgivning giver offentlige myndigheder mulighed for at få adgang til personoplysninger, som er overført fra Unionen, så

[113] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 76
[114] Forslag til afgørelse fra generaladvokat Y. Bot fremsat den 23. september 2015 i sag C-362/14 (Safe Harbor), præmis 174
[115] Forslag til afgørelse fra generaladvokat Y. Bot fremsat den 23. september 2015 i sag C-362/14 (Safe Harbor), præmis 173
[116] Forslag til afgørelse fra generaladvokat Y. Bot fremsat den 23. september 2015 i sag C-362/14 (Safe Harbor), præmis 177
[117] Forslag til afgørelse fra generaladvokat Y. Bot fremsat den 23. september 2015 i sag C-362/14 (Safe Harbor), præmis 178
[118] Forslag til afgørelse fra generaladvokat Y. Bot fremsat den 23. september 2015 i sag C-362/14 (Safe Harbor), præmis 179
[119] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 93
[120] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 94

giver den nationale lovgivning i tredjelandet ikke nogen mulighed for retssubjektet til anvende retsmidler til at få oplysningerne berigtiget eller slettet og ej heller mulighed for domstolsbeskyttelse, som er sikret ved Chartrets artikel 47.[121]

Som tidligere pointeret, så slog Domstolen fast, at det ikke kan kræves, at et tredjeland sikrer et beskyttelsesniveau, der er identisk med det, som er sikret i Unionen – men at et tilstrækkeligt beskyttelsesniveau skal forstås således, at tredjelandet skal sikre et beskyttelsesniveau for frihedsrettighederne og de grundlæggende rettigheder, som i det væsentligste svarer det niveau, der er sikret i Unionen. [122]

Generaladvokat Y. Bot henviser i sit forslag til afgørelse til Domstolens dom Digital Rights Ireland m.fl. (C-293/12 og C-594/12) og gør gældende at Domstolen i denne dom fastslog at begrænsningerne af personoplysningernes beskyttelse skal holdes inde for det strengt nødvendige.[123] I henhold til Digital Rights Ireland m.fl. (C-293/12 og C-594/12) gør Domstolen endvidere klart, at EU-lovgivningen skal fastsætte klare og præcise regler, som regulerer både rækkevidden og anvendelsen af den omhandlende foranstaltning, samt opstiller en række mindstekrav, således at de personer, hvis data er blevet lagret, råder over tilstrækkelige garantier, der gør det muligt at beskytte deres personlige oplysninger mod misbrug og ulovlig adgang til og anvendelse af disse oplysninger på en effektiv måde.[124] Slutteligt gør Domstolen det i Digital Rights Ireland m.fl. (C-293/12 og C-594/12) klart, at beskyttelse af personoplysninger, som er fastsat i Chartrets artikel 8 stk. 1, har en særlig betydning for personers ret til respekt for privatlivet jf. Chartrets artikel 7.[125]

5.3.1 – Sammenfatning af Safe Harbor-dommen

Sammenfattende gør Domstolen det klart ved Safe Harbor-dommen, at lovgivningen inden for EU, som udgør et indgreb i Chartrets artikel 7 og 8 jf. ovenfor, først skal holdes inde for det **strengt nødvendige** og skal være baseret på en lovgivning, som fastsætter **klare og præcise regler**, som regulerer **rækkevidden og anvendelsen** af foranstaltning og opstiller mindstekrav, således at de berørte personer råder over **garantier**, som gør det muligt at beskytte deres data mod misbrug og ulovlig adgang.

[121] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 95
[122] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 73
[123] Forslag til afgørelse fra generaladvokat Y. Bot fremsat den 23. september 2015 i sag C-362/14 (Safe Harbor), præmis 191 - Digital Rights Ireland m.fl. (C-293/12 og C-594/12), præmis 52
[124] Domstolens dom af 8. april 2014 i sag C-293/12 og C-594/12 (Digital Rights Ireland m.fl.), præmis 54 samt Forslag til afgørelse fra generaladvokat Y. Bot fremsat den 23. september 2015 i sag C-362/14 (Safe Harbor), præmis 193
[125] Domstolens dom af 8. april 2014 i sag C-293/12 og C-594/12 (Digital Rights Ireland m.fl.), præmis 53 samt Forslag til afgørelse fra generaladvokat Y. Bot fremsat den 23. september 2015 i sag C-362/14 (Safe Harbor), præmis 192

Domstolen valgte at erklære Safe Harbor-ordningen ugyldig på baggrund af, at Kommissionen ikke havde godtgjort, at USA sikrede et tilstrækkeligt beskyttelsesniveau. Ud fra analysen samt Domstolens præmisser i Safe Harbor dommen (C-362/14) og Digital Rights Ireland m.fl. dommen (C-293/12 og C-594/12) kan det udledes, at ***tilstrækkeligt beskyttelsesniveau*** i artikel 25 (6) i Databeskyttelsesdirektivet, skal forstås således:

Et tredjeland skal på **grundlag af sin egen lovgivning** sikre et tilstrækkeligt beskyttelsesniveau, det er derfor ikke selve Safe Harbor-ordningen eller andre lignende ordninger, som skal sikre et tilstrækkeligt beskyttelsesniveau. Det tilstrækkelige beskyttelsesniveau skal i det **væsentligste** svare til det niveau, som er sikret i Unionen jf. Databeskyttelsesdirektivet og de grundlæggende rettigheder i Chartret. Selvom Domstolen i præmis 73 til dom C-362/14 (Safe Harbor) anfører, at beskyttelsesniveauet ikke skal være identisk med det niveau, der er sikret i Unionens retsorden, så fastslår Domstolen alligevel, at et tilstrækkeligt beskyttelsesniveau stort set skal være på niveau med det i Unionen, da Domstolen vælger ordlyden *som i det væsentligste svare til det niveau, der er sikret inden for Unionen…*[126] Endvidere tilslutter Domstolen sig artikel 29-gruppens konstatering af, at et tredjeland for at sikre et tilstrækkeligt beskyttelsesniveau, **skal sikre effektive retsmidler til borgere**, hvis persondataretlige rettigheder er blevet krænkede.

5.4 Konsekvens af Safe Harbor-dommen

10 dage efter at Domstolen afsagde dom i C-362/14 om Safe Harbor-ordningens ugyldighed opfordrede Artikel 29-gruppen på det kraftigste medlemsstaterne og institutionerne i EU til sammen med USA at diskutere en politisk, lovlig og teknisk løsning som muliggør overførsel af persondata til USA.[127]

[126] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 73
[127] Statement of the Article 29 Working Party af 16. oktober 2015 - http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf, sidst aktiveret den 12.07.2017

6. Efter Safe Harbor-dommen

6.1 Privacy Shield-ordningen (EU's og USA's værn om privatlivets fred)

Den 12. juli 2016 blev Privacy Shield-ordningen mellem EU og USA offentliggjort. Privacy Shield-ordningen afløser den ugyldige Safe Harbor-ordning og skal alt andet lige sikre et tilstrækkeligt beskyttelsesniveau, som ikke strider imod artikel 25 (6) i Databeskyttelsesdirektivet. I og med at Safe Harbor-ordningen blev erklæret ugyldig pga. manglende konstatering af et tilstrækkeligt beskyttelsesniveau, så vil gennemgangen af Privacy Shield-ordningen fokusere på, om det kan konstateres, at USA har et tilstrækkeligt beskyttelsesniveau.

6.1.1 Tilstrækkeligt beskyttelsesniveau

I henhold til Privacy Shield-ordningen, så skal amerikanske virksomheder for at tilslutte sig ordningen foretage selvcertificering om tilslutning til principperne over for det amerikanske handelsministerium.[128] Aftalen består af 7 principperne samt 16 supplerende principper.

De syv principper er; oplysningspligt, valgfrihed, ansvar for videreoverførsel, sikkerhed, dataintegritet og formålsbegrænsning, indsigt, klageadgang, håndhævelse og ansvar.[129]

Selvom principperne i Privacy Shield-ordningen er langt mere udførligt beskrevne end i Safe Harbor-ordningen, så er principperne sammenlignelige.[130] I bilag I til Kommissionens gennemførelsesafgørelse 2016/1250 (Privacy Shield), har USA i et brev til EU kommissær Vêra Jourová beskrevet, at USA i samarbejde med Kommissionen har udviklet værnet om privatlivets fred, så virksomheder i USA får mulighed for at opfylde kravene om et tilstrækkeligt beskyttelsesniveau jf. EU-retten. Kommissionen selv er af den overbevisning, at USA sikrer et tilstrækkeligt beskyttelsesniveau for de personoplysninger, som overføres fra EU til virksomheder i USA under EU's og USA's værn om privatlivets fred.[131]

6.1.1.1 Beskyttelse af privatlivets fred

De syv principper, som er anført ovenfor skal overholdes af de selvcertificerede amerikanske virksomheder.

[128] Kommissionens gennemførelsesafgørelse EU 2016/1250, bilag 2, bilag II side 1, afsnit 2
[129] Kommissionens gennemførelsesafgørelse EU 2016/1250, bilag 2, bilag II, side 2-5
[130] Voss, W. Gergory, The future of transatlantic data flows: Privacy Shield or Bust?, side 14
[131] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 136

Med hensyn til princippet om oplysningspligt, så har de amerikanske virksomheder, som har tilsluttet sig ordningen pligt til give oplysninger til den registrerede om behandling af hans personoplysninger.[132] – herunder at de personlige oplysninger alene opbevares i en form, som gør det muligt at identificere eller gøre en person identificerbar så længe det tjener det formål, som den oprindelige indsamling var baseret på.[133] Det er endvidere en pligt for de amerikanske virksomheder, som har tilsluttet sig ordningen, at personoplysninger skal begrænses til de oplysninger, som er relevante for formålet med behandlingen – det betyder, at en virksomhed ikke må behandle personoplysninger til andre formål end det formål, som de blev indsamlet med henblik på, medmindre dette efterfølgende er blevet godkendt af den registrerede.[134] Bliver formålet med indsamlingen af personoplysningerne væsentligt ændret, men som sådan stadig er foreneligt med det oprindelige, så skal den registrerede have ret til modsætte sig anvendelsen af oplysningerne.[135] Amerikanske virksomheder, som har tilsluttet sig ordningen og som anvender eller spreder personoplysninger, skal sikre sig, at oplysningerne er tilstrækkeligt sikret. Udliciteres behandling af oplysninger skal dette sikres ved en databehandleraftaler, hvor underkontrahenten forpligter sig til at sikre det samme beskyttelsesniveau, som i Privacy Shield-ordningen.[136] Den registrerede har jf. princippet om indsigt i Privacy Shield-ordningen ret til at få oplyst om en virksomhed behandler personoplysninger om ham og hvis det er tilfældet at få udleveret oplysninger om dette inden for rimelig tid.[137] Videreoverførsel af personoplysninger kan kun finde sted, hvis der er et begrænset og bestemt formål, hvis det sker på grundlag af en aftale – og udelukkende hvis denne aftale sikrer samme niveau af beskyttelse, som principperne. Denne pligt gælder uanset hvor tredjeparten befinder sig.[138]

6.1.1.2 Forvaltning og overvågning

Privacy Shield-ordningen vil blive forvaltet og overvåget af det amerikanske handelsministerium[139], det har den betydning, at det amerikanske handelsministerium offentliggør en liste over de virksomheder, som på baggrund af selvcertificering har tilsluttet sig Privacy Shield-ordningen.[140] Listen er offentliggjort på en webside, hvor der også forefindes link til klageadgang, og de rettigheder osv., som den enkelte registrerede EU-borger har. 2326 amerikanske virksomheder har på nuværende tidspunkt tilsluttet sig

[132] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 20
[133] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 23
[134] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 21
[135] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 22
[136] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 124
[137] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 25
[138] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 28 og 29
[139] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 18
[140] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 31

ordningen.[141] Det amerikanske handelsministerium vil ved en virksomheds certificering kontrollere, om virksomhedens privatlivspolitik er i overensstemmelse med principperne i ordningen. [142] Virksomhederne har pligt til årligt at foretage en re-certificering af deres anmeldelse og det amerikanske handelsministerium ajourfører den offentliggjorte liste på baggrund af denne re-certificering. Vælger en amerikansk virksomhed frivilligt at trække sig ud af ordningen eller bliver virksomheden udelukket af ordningen, det kan f.eks. være på baggrund af en virksomheds manglende re-certificering eller vedvarende overtrædelse af ordningens principper, så vil virksomheden fremgå af det amerikanske handelsministeriums liste over fjernede virksomheder – og i enkelte tilfælde angives årsagen til fjernelsen. Selv efter fjernelse fra den offentliggjorte liste over tilsluttede virksomheder, vil virksomheden blive overvåget af det amerikanske handelsministerium mht. behandling af de allerede modtagne oplysninger, for at sikre, at de allerede modtagne oplysninger enten bliver slettet, tilbagesendt eller beholdt – bliver de beholdt, så skal virksomheden, selvom den er fjernet fra den offentliggjorte liste, stadig anvende principperne i ordningen.[143]

6.1.1.3 Klageadgang

Endvidere er Kommissionens vurdering af det tilstrækkelige beskyttelsesniveau begrundet med, at den registrerede EU-borger nu har mulighed for indgive klager om de selvcertificerede amerikanske virksomheders manglende overholdelse af principperne i ordningen til virksomheden selv, en uafhængig tvistbilæggelsesinstans, de nationale databeskyttelsesmyndigheder eller til FTC (Federal Trade Commision).[144] Det betyder, at en registreret EU-borger kan klage direkte over manglende overholdelse af principperne i ordningen til den selvcertificerede amerikanske virksomhed. Virksomheden har pligt til at indføre en effektiv klagemekanisme til håndering af klagerne, som skal fremme en løsning. Privatlivspolitikken, som ved indgivelse af anmeldelsen om tilslutning til ordningen, bliver kontrolleret af det amerikanske handelsministerium, skal indeholde oplysninger om, hvem der i eller uden for virksomheden skal kontaktes med henblik på behandling af klagerne. [145] En amerikansk virksomhed, som har modtaget en klage, skal fremsende et svar tilbage til den registrerede EU-borger inden for 45 dage.[146]

[141] https://www.privacyshield.gov/welcome, sidst aktiveret den 20.07.2017
[142] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 32
[143] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 31, 33 og 34
[144] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 41
[145] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 43
[146] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 44

Den registrerede har også den mulighed, at han kan indgive klage direkte til den uafhængige tvistbilæggelsesinstans, som er udpeget af virksomheden til at undersøge og afgøre individuelle klager. Den uafhængige tvistbilæggelsesinstans er forpligtet til hvert år, at offentlige en rapport med statistik over den samlede antal modtagne klager, typen af modtagne klager, klagebehandlingstid og resultatet af de modtagne klager.[147] Vælger en amerikansk virksomhed, som har tilsluttet sig ordningen ikke at følge den afgørelse, som enten et selvregulerende organ eller tvistbilæggelsesinstansen er kommet frem til, så indberettes den manglende overholdelse til det amerikanske handelsministerium, FTC eller en kompetent domstol. Den amerikanske virksomheden får derefter et varsel på 30 dage til at rette sig efter afgørelsen, imødekommer virksomheden ikke det, så bliver den fjernet fra den offentliggjorte liste.[148]

Derudover kan den fysiske person også indgive klage til de nationale databeskyttelsesmyndigheder. En amerikansk virksomhed, som har tilsluttet sig ordningen har pligt til at samarbejde med de nationale databeskyttelsesmyndigheder, såfremt denne databeskyttelsesmyndighed har modtaget en klage over den pågældende virksomhed og virksomheden frivilligt har underlagt sig databeskyttelsesmyndighedernes tilsyn. Virksomheden har pligt til at rette sig efter datamyndighedernes anbefalinger.[149] Anbefalingerne vil blive afgivet, når både den amerikanske virksomhed og den fysiske person har haft mulighed for at fremsætte bemærkninger og dokumentation. Senest 60 dage efter modtagelse af klagen, vil anbefalingerne blive afgivet. Virksomheden har 25 dage til at rette sig efter anbefalingen, sker dette ikke vil konsekvensen højst sandsynligt være en fjernelse fra den offentliggjorte liste.[150]

Det er også muligt for den fysiske person, at indgive klager til de nationale databeskyttelsesmyndigheder selvom den amerikanske virksomhed, der har tilsluttet sig ordningen, ikke har udpeget denne som tvistbilæggelsesinstans. Databeskyttelsesmyndigheden kan herefter henvise klagen til det amerikanske handelsministerium eller til FTC.[151] Databeskyttelsesmyndigheden skal ved henvisningen følge en af den amerikanske handelsministerium specifik procedure, som skal fremme behandling af klagen.[152]

En amerikansk virksomhed, som har tilsluttet sig ordningen er underlagt de undersøgelses- og håndhævelsesbeføjelser, som er tillagt de amerikanske myndigheder og især FTC (Federal Trade Commision).[153] Hvis en virksomhed ikke efterlever afgørelser på de klager, om manglende overholdelse

[147] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 45
[148] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 47
[149] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 48
[150] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 48 og 49
[151] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 51
[152] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 52
[153] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 54

af principperne i ordningen, så kan FTC henvise sagen til den kompetente domstol med henblik på at virksomheden bliver idømt civilretlige sanktioner. FTC har også mulighed for at anmode en føderal domstole om at udstede et foreløbigt eller endeligt påbud.[154]

Hvis en klage ikke er blevet håndteret tilfredsstillende via de tilgængelige klagemuligheder, så kan den registrerede EU-borger indbringe sagen for "panelet i værn om privatlivets fred" med henblik på en tvungen voldgift. Voldgiftspanelet vil bestå af en pulje af mindst 20 voldgiftsmænd udpeget af Kommissionen og det amerikanske handelsministerium. Den enkelte sag skal behandles af enten 1 eller 3 voldgiftsdommere sammensat af parterne.[155]

Der findes også den mulighed, at såfremt en databeskyttelsesmyndighed modtager en klage fra en registreret EU-borger og finder, at overførslen af personoplysningerne til en virksomhed i USA sker i strid med EU's databeskyttelsesregler, så kan databeskyttelsesmyndigheden udøve sine beføjelser i forbindelse med overførslen af personoplysningerne, altså i forhold til dataeksportøren og suspendere dataoverførslen.[156]

6.1.1.4 De amerikanske myndigheders adgang til og brug af personoplysninger til nationale sikkerhedsformål

Kommissionen har analyseret de amerikanske offentlige myndigheders begrænsede ret til adgang til og brug af overførte personoplysninger fra EU til USA.[157] Presidential Policy Directive 28 (PPD-28), som er udstedt den 17. januar 2014 fastslår, at signalefterretninger kun må indsamles til udenlandske efterretnings –eller kontraspionageformål. Endvidere er kravene i PPD-28, at indsamlingen skal være så målrettet som muligt, hvilket betyder, at de amerikanske efterretningstjenester først skal forsøge at finde og anvende andre tilgængelige oplysninger og alternativer, samt at der ikke bliver tale om en masseindsamling.[158] – dette afspejler principperne om nødvendighed og proportionalitet.[159] Indsamlende oplysninger må kun opbevares i højst fem år, medmindre der er en særlig bestemmelse i lovgivningen, som hjemler en længere opbevaring eller at en fortsat opbevaring er i den nationale sikkerheds interesse.[160] Kommissionen konkluderer, at USA har indført regler, som begrænser de

[154] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 55
[155] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 56 og 57
[156] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 60
[157] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 66
[158] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 71
[159] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 76
[160] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 86

eventuelle indgreb af hensyn til den nationale sikkerhed, som kan foretages til det **strengt nødvendige**.[161]

6.1.1.5 Effektiv retsbeskyttelse og individuel klageadgang

Den amerikanske efterretningstjeneste er underlagt kontrol- og tilsynsordninger fra den udøvende magt. [162] Tilsynsfunktionerne er understøttet af krav til rapportering af manglende overholdelse. Sker manglende overholdelse, som involverer personoplysninger uanset nationalitet, så skal dette indberettes Intelligence Oversight Board, som fører tilsyn med de amerikanske efterretningsmyndigheders overholdelse af forfatningen.[163]

En registreret EU-borger har en række klagemuligheder, hvis han er usikker på, om hans personoplysninger er blevet behandlet af den amerikanske efterretningstjeneste.[164] – for at udvide denne mulighed, så har den amerikanske regering oprettet en "ombudsmandsfunktion", som skal værne om privatlivets fred.[165] Denne funktion skal sikre, at individuelle klager bliver undersøgt ordentligt, at den amerikanske lovgivning er blevet overholdt og at den eventuelle manglende overholdelse bliver afhjulpet.[166] Fordelen ved denne mekanisme er; at ombudsmanden vil modtage og besvare individuelle klager; ombudsmanden vil samarbejde med nationale efterretningsmyndigheder og uafhængige tilsynsorganer. Ombudsmanden er desuden uafhængig og kan derfor ikke påvirkes af den amerikanske efterretningstjeneste.[167]

Kommissionen finder på baggrund af dette, at ombudsmandsfunktionen sikrer, at individuelle klager bliver grundigt undersøgt og behandlet og ombudsmandens uafhængighed godtgør, at der er tale om tilstrækkeligt og effektive garantier mod misbrug.[168]

6.1.2 Vurdering af om Privacy Shield-ordningen garanterer et tilstrækkeligt beskyttelsesniveau

Kommissionen gør afsluttende klart i præmis 136- 141 til Kommissionens gennemførelsesafgørelse EU 2016/1250, at den konkluderer, at USA sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, som overføres fra EU til virksomheder i USA under Privacy Shield-ordningen. Kommissionen finder

[161] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 88
[162] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 92 og 93
[163] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 99 og 101
[164] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 111
[165] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 116
[166] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 117
[167] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 120 og 121
[168] Kommissionens gennemførelsesafgørelse EU 2016/1250, betragtning 122

endvidere, at principperne i Privacy Shield-ordningen sikrer et niveau, som i det væsentlige svarer til det niveau, som er garanteret i Databeskyttelsesdirektivet.

Det tilstrækkelige beskyttelsesniveau skal vurderes på baggrund af de krav, som Domstolen tilkendegav både i Safe Harbor-dommen (C-364/14) og i Digital Rights Ireland m.fl-dommen (C-293/12 og C-594/12), at begrænsninger af personoplysningers beskyttelse skal holdes inde for det strengt nødvendige (proportionalitetsprincippet), ordningen skal bero på klare og præcise regler, som regulerer rækkevidden og anvendelsen af denne, samt at de registrerede skal have ret til effektiv domstolsbeskyttelse. Det blev i Safe Harbor-dommen konkluderet, at ordningen ikke respekterede beskyttelsen i Chartrets artikel 7 og 8 om ret til respekt for privatlivet og beskyttelse af personoplysninger.

Endvidere opstiller Artikel 29-gruppen 4 garantier på baggrund af praksis fra EU-Domstolen og Den Europæiske Menneskerets Domstol, som er en forudsætning for, at der kan ske overførsel af personoplysninger til tredjelande.

> ***1. Myndigheders adgang til personoplysninger skal ske på grundlag af klare, præcise og tilgængelige regler.***
> ***2. Myndighedernes adgang til og brug af personoplysninger skal være nødvendig og proportional (der skal være balance mellem formålet (national sikkerhed) og indgrebet i de registreredes ret til beskyttelse af deres privatliv).***
> ***3. Der skal være en uafhængig og effektiv tilsynsmyndighed.***
> ***4. Der skal være tilgængelige og effektive retsmidler for de registrerede.***[169]

6.1.2.1 Begrænsninger af personoplysninger skal holdes inde for det strengt nødvendige (proportionalitet)

Uanset, at USA har introduceret PPD-28, som begrænser de amerikanske myndigheders mulighed for indsamle persondata om de registrerede EU-borgere, så er det uvist om der i USA fortsat sker masseindsamling af data. Dog pointerer Artikel 29-gruppen, at der er tegn på, at der stadig sker masseindsamlinger i USA begrundet i, at der netop i PPD-28 er opremset specifikke begrænsninger i mulighed for at indsamle persondata.[170] PPD-28 indeholder dog bestemmelser om, at indsamling af

[169] Betænkning nr. 1565 om Databeskyttelsesforordningen, side 636
[170] Artikel 29-gruppen: Opinion 01/2016 on the EU-U:S. Privacy Shield draft adequacy decision, side 40 og Kommissionens gennemførelsesafgørelse EU 2016/1250, bilag 6, side 3, afsnit 4

signalefterretninger skal målrettes, således det ikke er nødvendigt at foretage masseindsamling.[171] I den forbindelse skal det bemærkes, at en masseindsamling godt kan være målrettet.[172]

6.1.2.2 Privacy Shield-ordningen skal bero på klare og præcise regler

Safe Harbor-ordningen blev bl.a. erklæret ugyldig på grund af, at Kommissionen ikke behørigt konstaterede, at USA's lovgivning sikrede et beskyttelsesniveau, som i det væsentligste svarede til det, som er sikret i EU.[173] I Privacy Shield-ordningen er relevant lovgivning angivet og en del også gengivet. Derudover, er lovgivningsmateriale på overvågningsområdet tilgængeligt online og de amerikanske myndigheder har derved højnet gennemsigtigheden. – men der er stadig en del dokumenter, som omhandler rettigheder for individer uden for USA, som er hemmeligstemplede. – og de, som er blevet tilgængelig for offentligheden giver kun en begrænset indsigt i overvågningsaktiviteterne. Selvom PPD-28, som begrænser de amerikanske myndigheders mulighed for overvågning, er blev offentliggjort, så er det stadig svært at vurdere, om den amerikanske lovgivning er tilstrækkelig klar og præcis.

6.1.2.3 Effektiv domstolsbeskyttelse

Som tidligere anført, så har en registreret EU-borger forskellige muligheder for at klage såfremt en virksomhed ikke overholder Privacy Shield-principperne. De mange forskellige klagemuligheder er af bekymring for Artikel 29-gruppen, som udtrykker, at kvaliteten af oprejsningsmuligheder skal overvinde mængden af oprejsningsmuligheder, så den registreredes rettigheder ikke bliver underminerede.[174]

6.1.2.4 Uafhængig og effektiv tilsynsmyndighed.

Med ombudsmandsmekanismen garanterer USA et uafhængigt tilsyn og en individuel klageadgang for de EU-borgere, hvis oplysninger er blevet overført til selvcertificerede virksomheder i USA. Ombudsmanden skal være uafhængig, så han ikke kan presses rent politisk til at påtage sig en holdning, som andre har bestemt.[175]

[171] Kommissionens gennemførelsesafgørelse EU 2016/1250, bilag 6, side 2
[172] Artikel 29-gruppen: Opinion 01/2016 on the EU-U:S. Privacy Shield draft adequacy decision, side 40
[173] Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor), præmis 96
[174] Artikel 29-gruppen: Opinion 01/2016 on the EU-U:S. Privacy Shield draft adequacy decision, side 26
[175] Artikel 29-gruppen: Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data, side 10

6.1.2.4 Sammenfatning på vurdering af, om Privacy Shield-ordningen garanterer et tilstrækkeligt beskyttelsesniveau

Kommissionen vedtog ret hurtigt efter Safe Harbor-ordningen blev erklæret ugyldig Privacy Shield-ordningen. Den nye ordning er opbygget på samme måde som Safe Harbor-ordningen med et selvcertificeringssystem, som amerikanske virksomheder kan anvende, såfremt de ønsker at tilslutte sig Privacy Shield-principperne. Uanset om Privacy Shield-ordningen er mere deltaljeret beskrevet og den omfatter langt mere dokumentation, så har den modtaget massiv kritik, især fra Artikel 29-gruppen. Det er ikke tilstrækkeligt godtgjort i Privacy Shield-ordningen, at USA garanterer et tilstrækkeligt beskyttelsesniveau af personoplysninger. I og med at tidligere præsident Barack Obama udstedte PPD-28, blev amerikanske myndigheders indsamling af ikke amerikanske statsborgeres personoplysninger begrænset, men ikke videre end at masseindsamling af disse personoplysninger stadig kan foregå, såfremt der er tale om en målrettet søgning. "Målrettet" er ikke videre defineret og da der er tale om et udefineret begreb, så kan alt andet lige mange forskellige formål falde herindunder, så længe at det kan argumenteres for, at det er målrettet.

Den amerikanske lovgivning, som Privacy Shield-ordningen er bundet op på er gengivet udførligt i ordningen. Dog er der stadig hemmeligstemplede dokumenter, som angiver rettigheder for de registrede EU-borgeres personoplysninger, som der ikke er adgang til. Det modarbejder klart kravet om klar og præcis lovgivning og i og med denne usikkerhed består, så konstateres det, at den amerikanske lovgivning ikke lever op til dette krav.

Det er endvidere uklart, om de amerikanske myndigheders adgang til overførte personoplysninger er i strid med de garantier, som der jf. Artikel 29-gruppens WP 237 skal stilles af tredjelandet, før det kan bliver anerkendt som et sikkert tredjeland. Men det tyder på, at Privacy Shield-ordningen bør underkendes på sammen måde som Safe Harbor-ordning på grund af den grad af usikkerhed, som statueres.

Endvidere kan det undre, at Privacy-Shield-ordningen kun er baseret på indholdet i Databeskyttelsesdirektivet, når en ny persondataforordning blev vedtaget den 27. april 2016, altså før beslutningen Privacy Shield-ordningen blev gennemført. Privacy Shield-ordningen må derfor antages at leve på lånt tid, da der er nye regler i den nye Databeskyttelsesforordningen, som skal iagttages:

> ***Artikel 45***
>
> ***Overførsler baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet***

1. Overførsel af personoplysninger til et tredjeland eller en international organisation kan finde sted, hvis Kommissionen har fastslået, at tredjelandet, et område eller en eller flere specifikke sektorer i dette tredjeland, eller den pågældende internationale organisation har et tilstrækkeligt beskyttelsesniveau. En sådan overførsel kræver ikke specifik godkendelse.

2. Ved vurdering af beskyttelsesniveauets tilstrækkelighed tager Kommissionen navnlig følgende elementer i betragtning:

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

b) tilstedeværelse af en eller flere velfungerende uafhængige tilsynsmyndigheder i tredjelandet, eller som den internationale organisation er underlagt, med ansvar for at sikre og håndhæve, at databeskyttelsesreglerne overholdes, herunder tilstrækkelige håndhævelsesbeføjelser, for at bistå og rådgive de registrerede, når de udøver deres rettigheder, og for samarbejde med tilsynsmyndighederne i medlemsstaterne, og

c) de internationale forpligtelser, som tredjelandet eller den internationale organisation har påtaget sig, eller andre forpligtelser, der følger af retligt bindende konventioner eller instrumenter og af landets eller organisationens deltagelse i multilaterale eller regionale systemer, navnlig vedrørende beskyttelse af personoplysninger.

3. Kommissionen kan efter vurdering af beskyttelsesniveauets tilstrækkelighed ved hjælp af en gennemførelsesretsakt fastslå, at et tredjeland, et område eller en eller flere specifikke sektorer i et tredjeland, eller en international organisation sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med denne artikels stk. 2. I den pågældende gennemførelsesretsakt fastsættes en mekanisme for regelmæssig revision, som foretages mindst hvert fjerde år, og som inddrager enhver relevant udvikling i tredjelandet eller den internationale organisation. I gennemførelsesretsakten angives dennes territoriale og sektorbestemte anvendelsesområde og i påkommende tilfælde den eller de tilsynsmyndigheder, der er omhandlet i denne artikels stk. 2, litra b). Gennemførelsesretsakten vedtages efter undersøgelsesproceduren i artikel 93, stk. 2.

4. Kommissionen overvåger løbende udvikling i tredjelande og internationale organisationer, der kan påvirke virkningen af afgørelser, der er vedtaget i henhold til denne artikels stk. 3, og afgørelser og beslutninger, der er vedtaget på grundlag af artikel 25, stk. 6, i direktiv 95/46/EF.

5. Kommissionen ophæver, ændrer eller suspenderer i det omfang, det er nødvendigt, uden tilbagevirkende kraft afgørelsen omhandlet i denne artikels stk. 3 ved hjælp af gennemførelsesretsakter, hvis tilgængelige oplysninger, navnlig efter den i denne artikels stk. 3 omhandlede revision, viser, at et tredjeland, et område eller en eller flere specifikke sektorer i et tredjeland, eller en international organisation ikke længere sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med denne artikels stk. 2. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 93, stk. 2.

I behørigt begrundede særligt hastende tilfælde vedtager Kommissionen efter proceduren i artikel 93, stk. 3, gennemførelsesretsakter, der finder anvendelse straks.

6. Kommissionen fører konsultationer med tredjelandet eller den internationale organisation med henblik på at afhjælpe den situation, der har givet anledning til en afgørelse vedtaget i henhold til stk. 5.

7. En afgørelse som angivet i denne artikels stk. 5 berører ikke overførsel af personoplysninger til det pågældende tredjeland, et område eller en eller flere specifikke sektorer i dette tredjeland, eller den pågældende internationale organisation i medfør af artikel 46-49.

8. Kommissionen offentliggør i Den Europæiske Unions Tidende og på sit websted en liste over tredjelande, områder og specifikke sektorer i tredjelande samt internationale organisationer, som den har fastslået sikrer eller ikke længere sikrer et tilstrækkeligt beskyttelsesniveau. 4.5.2016 DA Den Europæiske Unions Tidende L 119/61

9. Afgørelser og beslutninger, der er vedtaget af Kommissionen på grundlag af artikel 25, stk. 6, i direktiv 95/46/EF, gælder fortsat, indtil de ændres, erstattes eller ophæves ved en kommissionsafgørelse, der vedtages i henhold til nærværende artikels stk. 3 eller 5.

Endvidere er Privacy Shield-ordningen allerede blevet anfægtet i Digital Rights Ireland mod Kommissionen, hvor det skøn, som Kommissionen har foretaget mht. om USA sikrer et tilstrækkeligt beskyttelsesniveau, påstås afgivet på et åbenbart urigtigt grundlag.[176] Der er endnu ikke faldt afgørelse i sagen.

[176] T-670/16 (Digital Rights Ireland)

6.2 Andre muligheder for at overføre personoplysninger til tredjelande

Europæiske multinationale virksomheder har også andre muligheder for at overføre personoplysninger til tredjelande. I nedenstående gennemgås mulighederne. Det betyder at såfremt Privacy Shield-ordningen bliver underkendt, så vil virksomhederne stadig have mulighed for at overføre personoplysninger til USA. – det skal blot gøres på en anden måde og det praktiske arbejde vil alt andet lige i en højere grad ligge hos dataeksportøren.

6.2.1 Binding Corporate Rules

En dansk koncern med datterselskaber i lande uden for EU kan og vil højst sandsynligt have brug for at udveksle personoplysninger med datterselskabet. Dette kan gøres på baggrund af Corporate Binding Rules (BCR), som er hjemlet i Databeskyttelsesforordningens artikel 47. BCR er et internt regelsæt i koncernen, som sikrer, at datterselskaber som ligger i lande, hvor et tilstrækkeligt beskyttelsesniveau ikke er garanteret, godt må modtage og behandle personoplysninger, da det pågældende datterselskab, skal følge det interne regelsæt, som koncernen har fastsat. BCR regelsættet i koncernen skal specifikt indeholde regler om: principper for beskyttelse af personlige oplysninger, effektivitetsværktøjer (revision, træning, klagehåndtering osv.) og bevis på at reglerne er bindende.[177] BCR skaber derved et fælles grundlag for overførsel for store multinationale virksomheder i EU til deres koncernforbundne selskaber uden for EU.

En dansk virksomhed, som ønsker at få en BCR-godkendelse, skal sende ansøgning herom til Datatilsynet.

Godkendelsen af BCR-ansøgningen kan opsummeres i 5 trin:

1, Virksomheden skal vælge, hvilken DPA (databeskyttelsesmyndighed), der skal lede virksomhedens ansøgning om godkendelse af BCR, dette er normalt i det land, hvor virksomhedens europæiske hovedkvarter ligger.[178]

2, Virksomheden udarbejder et udkast til det interne BCR-regelsæt i henhold til de anvisninger, som er angivet i Artikel 29-gruppens arbejdsdokumenter. Udkastet sendes, hvis der er tale om en virksomhed med dansk hovedsæde, til Datatilsynet, som gennemgår udkastet for at sikre, at det overholder alle kravene i artikel 29-gruppens dokumenter.

[177] http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm, sidst aktiveret den 25. juli 2017
[178] https://www.datatilsynet.dk/erhverv/tredjelande/binding-corporate-rules-bcr/

3, Datatilsynet begynder samarbejdet med de andre relevante databeskyttelsesmyndigheder i EU, såfremt virksomheden har koncernforbundne selskaber i andre EU lande disse koncernforbundne selskaber også skal overføre persondata ud af EU.

4, EU-samarbejdet afsluttes, når databeskyttelsesmyndighederne i de relevante EU-lande har anerkendt modtagelse af BCR-ansøgningen. I praksis har flere datamyndighederne i EU aftalt, at når DPA'en har godkendt et BCR-regelsæt, så accepterer de andre databeskyttelsesmyndigheder denne beslutning. Dette for at fremme behandlingstiden. Danmark er dog ikke med i denne ordning.

5, Når BCR-regelsættet er godkendt af alle databeskyttelsesmyndighederne i EU, så skal virksomheden anmode om godkendelse af overførsel af personoplysninger til tredjelande på baggrund af denne.[179]

På nuværende tidspunkt, er der kun 2 danske virksomheder; Novo Nordisk A/S og Mærsk Group, som fremgår af listen over de virksomheden, som har fået godkendt deres BCR-procedure.[180] Fordelen ved BCR, er at den også dækker de selskaber, som er uden for EU. Det er en grænseoverskridende aftale, som er bundet op på Koncernen og ikke på EU-grænserne. En virksomhed med datterselskaber i usikre tredjelande kan med fordele anvende BCR og derved sikre en ensartet politik for behandling af personoplysninger i hele Koncernen.

6.2.2 Standard Contractual Clauses (Standardkontrakter)

En virksomhed i EU, som overfører personoplysninger til et koncernforbundet selskab i et tredjeland har også den mulighed, at den kan benytte sig at de såkaldte Standardkontrakter, hjemlet i Databeskyttelsesforordningens artikel 46 (2) litra c. En Standardkontrakt sikrer passende beskyttelsesforanstaltninger med hensyn til overførsel af personoplysninger. Kommissionen har med hjemmel i artikel 26 (4) i Databeskyttelsesdirektivet fået kompetence til at beslutte, at visse Standardkontrakter sikrer disse passende beskyttelsesforanstaltninger. Indtil videre har Kommissionen udstedt to Standardkontrakter, en for overførsel af personoplysninger fra en databehandler i EU til en databehandler uden for EU og en for overførsel af personoplysninger til en dataansvarlig uden for EU.[181] Såfremt en dansk virksomhed anvender en kontrakt, som er fuld overensstemmelse med bestemmelserne i Kommissionens Standardkontrakt, så skal der ikke ansøges om tilladelse fra Datatilsynet jf. persondataloven § 27, stk. 5, - ændrer en virksomhed derimod indholdet af en

[179] http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/procedure/index_en.htm, sidst aktiveret 25.07.2017
[180] http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm, sidst aktiveret den 25.07.2017
[181] http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm, sidst aktiveret den 25.07.2017

Standardkontrakt, så skal der søges om tilladelse fra Datatilsynet jf. persondatalovens § 27, stk. 4 – og Datatilsynet vil herefter konkret vurdere, om beskyttelsesniveauet og de garantier, der er givet til beskyttelse af de registreredes rettigheder er tilstrækkelige.[182] Udfordringen er her, at der ikke er tale om en over de europæiske grænser aftale. Har en virksomhed i EU datterselskaber i andre EU medlemsstater, så skal jf. denne medlemsstats regler søges om godkendelse hos den nationale databeskyttelsesmyndighed – så der ikke tale om en "samlet" løsning, som ved BCR.

6.2.3 Samtykke

Den mindst omfattende mulighed af dem alle, er at indhente den registreredes samtykke. I henhold til § 3, stk. 1, nr. 8, så skal samtykke forstås således:

> ***Den registreredes samtykke:***
>
> ***Enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling.***

Har en virksomhed tusindvis af ansatte, er dette selvfølgelig ikke en særdeles god løsning, medmindre virksomheden har sikret sig i ansættelsesbeviset/kontrakten, at alle medarbejdere har skrevet under på, at den ansatte giver sit udtrykkelige samtykke til behandling af personoplysninger uanset følsomhed og at disse personoplysninger må overføres til tredjeland. Det er nok utopi at tænke, at mange virksomheder har været så fremsynede. I samtykkebegrebet ligger en viljeserklæring, og den tillægges stor betydning, fordi den hjemler behandlingen af personoplysningerne. Viljeerklæringen skal som udgangspunkt meddeles af den registrerede selv, men kan også meddeles af den person, som den registrerede har tildelt fuldmagt. I en situation, hvor den registrerede pga. sygdom eller rejseaktivet ikke selv kan give samtykke, så kan fuldmagtshaveren give det på den registreredes vegne. Forældre har mulighed for at give samtykke på deres børns vegne.[183] Her kan tænkes i den situation, hvor barnets idrætsklub ønsker at offentliggøre fotografier af barnet på idrætsklubbens hjemmeside, hvor der er adgang for alle.

Et samtykke kan gives både mundtligt og skriftligt, men det er databehandleren, der skal bevise, at foreligger et samtykke, så derfor anbefales det altid at samtykke indhentes skriftligt. Et samtykke skal endvidere være afgivet frivilligt, hvilket betyder, at det på ingen måder må være afgivet under tvang.[184] Samtykket skal gives til et konkret formål, hvor det tydeligt fremgår, hvad samtykket skal anvendes til.

[182] https://www.datatilsynet.dk/erhverv/tredjelande/kommissionens-standardkontrakter/ - sidst aktiveret den 03.08.2017
[183] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 168
[184] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 170 og 171

Det skal fremgå, hvem der meddeles samtykke til, hvilke oplysninger der må behandles og hvad formålet med behandlingen af personoplysningerne er.[185] Den samtykkende skal være klar over, hvad det er han meddeler samtykke til – samtykket skal afgives på et informeret grundlag.[186] Samtykket skal som udgangspunkt afgives til den dataansvarlige, som skal bruge samtykket til behandling af oplysningerne. Dog er der ikke noget til hinder for, at databehandleren "blot" formidler samtykket.[187]

I henhold til persondatalovens § 27, stk. 3, nr. 1, så kan personoplysninger overføres til tredjelande såfremt den registrerede giver samtykke hertil. Dog er det en hel klar forudsætning for en sådan overførsel, at denne ikke strider imod § 5 i persondataloven, som omhandler god databehandlerskik. I Datatilsynets afgørelse: journalnummer 2003-233-0028, som omhandlede danske revisorers samtykke til behandling af personoplysninger i USA, samt offentliggørelse på PCAOB (**Public Company Accounting Oversight Board**)'s hjemmeside. Kravet om at revisorerne skulle registreres på hjemmesiden PCAOB var etableret i forbindelse med Sarbanes Oxley Act, som foreskriver at for en revisor kunne forestå revision af amerikanske virksomheder, så skal han være opført på denne hjemmeside. De personoplysninger, der skulle fremgå af PCAOB er; Oplysning om ansatte revisorers involvering i verserende straffesager, civile sager, disciplinærsager, uoverensstemmelser med klienter og voldgiftssager inden for de sidste fem år. På grund af at revisorerne ved at give samtykke til at disse oplysninger bliver behandlet vil kompromittere deres tavshedspligt lagde Datatilsynet til grund, at dette var en overtrædelse af god databehandlerskik og dermed § 5 i persondataloven.

6.2.4 Sammenfattende om andre mulighed for at overføre personoplysninger til tredjelande

En virksomhed har forskellige muligheder for at overføre personoplysninger til tredjelande – og alt efter størrelse og ambitionsniveau, så kan virksomheden selv beslutte, hvilken én, som den vil anvende. Er der tale om en stor koncern med 50 datterselskaber uden for EU, så vil det blive særdeles byrdefuldt at skulle holde styr på alle standardkontrakter og det taler derfor for, at den virksomhed vælger at bruge anvende BCR, især også fordi det blot skal meddeles til Datatilsynet én gang om året, om der er sket udskiftninger i de selskaber, som er omfattet af ordningen. Når først en BCR er godkendt, så udløber den ikke og i og med at BCR er en integreret del af Databeskyttelsesforordningen, så må den anses til at have en lang levetid. Er der tale om en mindre virksomhed med få datterselskaber uden for EU og som har behov for at oveføre personoplysninger om mange registrerede (det kunne være medarbejdere), så vil

[185] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 173
[186] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 174
[187] Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, 2015, side 176

det give mest mening at anvende Standardkontrakter. Er der tale om en dansk virksomhed med få ansatte og med få datterselskaber uden for EU og denne virksomhed ”kun” har behov for at overføre personoplysninger om medarbejderne, så ville den mest optimale løsning være at bede om medarbejdernes udtrykkeligt samtykke til overførslen.

7. Danske virksomheders øgede fokus på behandling af oplysninger

Som tidligere nævnt, er der ingen tvivl om, at mange danske virksomheder har fået travlt med at revurdere de eksisterende eller måske ikke-eksisterende interne procedurer, de har for behandlingen af personoplysninger i forbindelse med vedtagelsen af Databeskyttelsesforordningen.

For en virksomhed, som ikke har været særlig opmærksom på reglerne i persondataloven lægger der en relativt stor opgave i at blive compliant med bestemmelserne i forordningen.

For en dansk virksomhed med datterselskaber flere steder rundt om i verden er én af de første opgaver, der skal kigges på en kortlægning af de datastrømme, der flyder mellem virksomheden og diverse databehandlere. For at kunne kortlægge disse data vil der skulle foretages interviews med nøglepersoner i virksomheden som fx HR-ansvarlige, indkøbsansvarlige, IT-ansvarlige osv. Hvis virksomheden er en offentlig virksomhed eller den primært beskæftiger sig med omfattende behandling af personoplysninger, så er det et krav, at virksomheden udpeger en Data Protection Officer (DPO) jf. artikel 37 i Databeskyttelsesforordningen. Herudover kan andre virksomheder eller organisationer vælge at udpege en DPO, hvis de ønsker det. Ud fra kortlægning af de datastrømme som løber mellem datterselskaberne og moderselskabet er det muligt at analysere sig frem til, hvilket behov der er for sikre det korrekte juridiske grundlag gennem aftaler såsom Standardkontrakter, BCR, Privacy Shield eller samtykke, desuden skal der ske anmeldelse til Datatilsynet, hvis virksomheden behandler følsomme personoplysninger. Der skal selvfølgelig kigges på de aftaler, der er indgået med leverandører, som leverer en ydelse, hvor leverandøren behandler personoplysninger – her kan f.eks. være tale om en leverandør, som behandler medarbejdernes lønoplysninger eller et rekrutteringsbureau, som virksomheden anvender i forbindelse med rekruttering og sikre at databehandleraftaler bliver underskrevet. Når det er kortlagt, hvor virksomheden skal indgå aftaler/indsende anmeldelser til, så skal de interne procedurer rettes til, så medarbejderen i virksomheden opnår forståelse for, hvordan personoplysninger skal behandles, især hvad virksomheden må og ikke må. Derfor er et stort element i det at blive compliant at undervise medarbejderne i de regler og især, hvis virksomheden ikke har arbejdet aktivt med beskyttelse af personoplysninger før). Når passende interne procedurer er implementeret i virksomheden og virksomheden er compliant med reglerne, så skal der i virksomheden selvfølgelig foretages løbende kontroller af om efterlevelse af de interne procedurer sker – eventuelt indføres der årlige audits. Desuden skal virksomhedens medarbejdere selvfølgelig informeres om, hvordan virksomheden arbejder med personoplysninger.

8. Konklusion

Ønsker en dansk virksomhed at overføre personoplysninger til et datterselskab, som er beliggende i et andet EU-land, så gælder der ingen specielle krav til overførslen så længe overførslen overholder bestemmelserne i persondataloven. Sker overførslen efter den 25. maj 2018, så er det reglerne i Databeskyttelsesforordningen, der skal overholdes. Der er i Danmark lagt op til at reglerne i Databeskyttelsesforordningen skal danne baggrund for en ny persondatalov, som inkorporerer de nye bestemmelser i Databeskyttelsesforordningen og der blev derfor afgivet betænkning nr. 1565 i maj 2017, så Regeringen har mulighed for at fremsætte forslag til lovgivning tidsnok til, at forslag kan nå at blive behandlet i folketinget (tre behandlinger) og vedtaget inden den 25. maj 2018.

Ønsker en virksomhed derimod at overføre personoplysninger til et datterselskab, som er beliggende uden for EU, så ser det straks anderledes ud. Det land, hvor datterselskabet er beliggende skal garantere et tilstrækkeligt beskyttelsesniveau af personoplysningerne.

En personoplysning er enhver information, som enten identificerer den registrerede direkte eller en information, som kan identificere den registrerede. Der er bl.a. tale om oplysninger om navn, adresse, lønoplysninger, biometriske oplysninger, dna-oplysninger mm. Selvom f.eks. en adresse erstattes af en kode, så vil der også være tale om behandling af personoplysninger, såfremt det er muligt at foretage en afkodning på et senere tidspunkt.

Et tilstrækkeligt beskyttelsesniveau af de oplysninger, som bliver overdraget til en virksomhed i et tredjeland, er straks lidt vanskeligere at definere. Men på baggrund af Safe Harbor-dommen kan det konkluderes, at et tilstrækkeligt beskyttelsesniveau skal forstås således:

> Et tredjeland skal på baggrund af sin egen lovgivning sikre et tilstrækkeligt beskyttelsesniveau og dette skal i det væsentligste svare til det niveau, som er sikret i Unionen.

Og følgende elementer skal anvendes, når det skal vurderes, om et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau:

> ***1. Myndigheders adgang til personoplysninger skal ske på grundlag af klare, præcise og tilgængelige regler.***
> ***2. Myndighedernes adgang til og brug af personoplysninger skal være nødvendig og proportional (der skal være balance mellem formålet (national sikkerhed) og indgrebet i de registreredes ret til beskyttelse af deres privatliv).***

3. Der skal være en uafhængig og effektiv tilsynsmyndighed.

4. Der skal være tilgængelige og effektive retsmidler for de registrerede.[188]

Det betyder generelt, at der skal foretages en helhedsvurdering af gældende ret og praksis i det pågældende tredjeland. Selvom Domstolen ikke fastslår, at tredjelandet skal garantere et identisk beskyttelsesniveau af personoplysninger, som det, der er gældende i EU – så er der ikke den store forskel på væsentlig og identisk – og Domstolen "presser" derved tredjelande, der ønsker at blive et sikkert tredjeland Unionens høje ambitionsniveau på området ned over dem. Det er for så vidt ikke en dårlig udvikling, men i stedet for at bruge ordet væsentlig, så ville ordet sammenlignelig passe bedre i forhold til den forståelse af reglerne, som Domstolen har fastlagt. Ved at anvende sammenlignelig, så vil det ikke længere være tvivl om, hvad der ligger i begrebet væsentlig. På den måde, som Domstolen er det jo klart, at beskyttelse af personoplysninger er et vigtigt område og at Unionsborgernes rettigheder skal beskyttes bedst muligt, selvom oplysninger bliver flyttet ud af Europa.

Relativt kort tid efter, at Safe Harbor-dommen blev afsagt, blev Privacy Shield-ordningen vedtaget af Kommissionen. Den indeholder en detaljeret gennemgang af den amerikanske lovgivning på området, men anses ikke som værende optimal grundet manglede iagttagelse af de kommende nye regler i Databeskyttelsesforordningen. Ordningen skal revurderes på en årlig basis og siden ordningen blev vedtaget den 16. juli 2016 er en revurdering lige om hjørnet. Om vurderingen i 2017 får en reel betydning, når det skal se med de nye regler for vurdering af tilstrækkeligt beskyttelsesniveau i Databeskyttelsesforordningen in mente er uvist – men det er tvivlsomt om Privacy Shield-ordningen kan blive ved med at bestå –især med den gyldighedssag, der allerede er igangsat (T-670/16) ved Domstolen.

En dansk virksomhed, som ønsker at overføre personoplysninger til et datterselskab i USA, har også andre muligheder end at benytte sig af Safe Harbor-ordningen, hvor det vil være det amerikanske datterselskab, der skal sørge for at overholde principperne i Safe Harbor-ordningen. Den danske virksomhed af en vis størrelse kan i stedet benytte sig at Binding Corporate Rules (BCR), som er et internt regelsæt, som anvendes for en hel koncern, men som anmeldes fra hovedkvarteret – i dette tilfælde til Datatilsynet i Danmark. En virksomhed af en mindre størrelse kan med fordel anvende sig af Standardkontrakter, hvor der udarbejdes kontrakter internt i Koncernen mellem alle enhederne. Slutteligt er det også en mulighed simpelthen af bede om den registreredes samtykke til overførslen.

[188] Betænkning nr. 1565 om Databeskyttelsesforordningen, side 636

9. Litteraturliste

Artikler

Voss, W. Gregory, The future of transatlantic data flows: Privacy Shield or Bust?, udgivet i Journal of Internet Law, volume 19, nummer 11, Maj 2016

Bøger

Blume, P., Persondataretlige grundfigurer, Jurist- og Økonomforbundet forlag (2017)

Blume, P., Persondataretten - i en brydningstid, Jurist- og Økonomforbundet forlag (2014)

Blume, P., Personoplysningsloven, Greens Jura (2000)

Blume, P., Retlig regulering af internationale persondataoverførsler, Jurist – og Økonomforbundets forlag (2006)

Høilund, D., Persondataloven, en indføring, Hans Reitzels Forlag, 3. udgave (2015)

Waaben, H. og *Nielsen*, K., Lov om behandling af personoplysninger med kommentarer, Jurist og Økonomforbundet Forlag, 3. udgave (2015)

EU-retsakter

Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger

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

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

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

Artikel 29-gruppens dokumenter

Opinion 01/2016 on the EU-U:S. Privacy Shield draft adequacy decision

Artikel 29-gruppens udtalelse nr. 4/2007 om begrebet personoplysninger (WP 136)

Artikel 29 gruppens arbejdsdokument af den 24. juli 1998 (WP12)

Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (WP 237)

Retspraksis

Domstolens dom af 6. oktober 2015 i sag C-362/14 (Safe Harbor)

Domstolens dom af 8. april 2014 i sag C-293/12 og C-594/12 (Digital Rights Ireland m.fl.)

Domstolens dom af 20. maj 2018 i sag C-465/00, C-138/01 og C-139/01 – (Österreichischer Rundfunk)

Domstolens dom af 17.oktober 2013 i sag C-291/12 (Michael Schwarz)

Domstolens dom af 6. november 2003 i sag C-101/01 (Lindquist)

Forslag til afgørelse fra generaladvokat Y. Bot fremsat den 23. september 2015 i sag C-362/14 (Safe Harbor)

Sag anlagt den 16. september 2016 – Digital Rights Ireland mod Kommissionen (Sag T-670/16) – ikke afgjort

Dansk Lovgivning

Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger

Betænkninger

Betænkning nr. 1345/1997 om behandling af personoplysninger

Betænkning nr. 1565 om Databeskyttelsesforordningen

Folketingstidende

Folketingstidende 1997-1998, 2. samling, tillæg A

Folketingstidende 1998-1999, tillæg A

Folketingstidende 1999-2000, tillæg A

Datatilsynets afgørelser

Datatilsynets afgørelse: Journalnummer 2002-321-0155 – Datatilsynets årsberetning 2002, side 42-43

Datatilsynets afgørelse: Journalnummer 2003-212-0143 – Datatilsynets årsberetning 2003, side 85-86

Datatilsynets afgørelse: Journalnummer 2007-321-0039

Datatilsynets afgørelse: Journalnummer 2007-219-0043

Datatilsynets afgørelse: Journalnummer 2007-632-0006

Datatilsynets afgørelse: Journalnummer 2009-631-0099

Datatilsynets afgørelse: Journalnummer 2008-313-0113

Datatilsynets afgørelse: Journalnummer 2003-233-0028

Elektroniske Kilder

http://www.juraplexus.dk/juridisk-leksikon/id.retsdogmatik/i.html - sidst aktiveret den 03.06.2017

http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf - sidst aktiveret den 12.07.2017

https://www.privacyshield.gov/welcome - sidst aktiveret den 20.07.2017

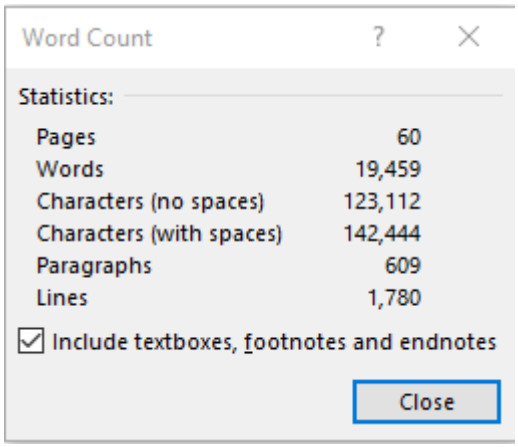
http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm - sidst aktiveret den 25.07.2017

http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm, sidst aktiveret den 25.07.2017

https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/offentliggoerelse-af-oplysninger-om-modstandsfolk-paa-internettet-ii/ - sidst aktiveret den 27.07.2017

https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/spoergsmaal-om-behandling-af-personoplysninger-i-forbindelse-med-whistleblowing/ - sidst aktiveret den 30.07.2017
https://www.datatilsynet.dk/erhverv/tredjelande/sikre-tredjelande/, sidst aktiveret den 02.08.2017

https://www.datatilsynet.dk/erhverv/tredjelande/kommissionens-standardkontrakter/ - sidst aktiveret den 03.08.2017



Opgjort den 9. august 2017