Persondataforordningens internationale virkning over for tredjelande

15. MAJ 2018

SUITTI JEPPESEN (51963)
MING XIA JØRGENSEN (8805)

Vejleder: Vishv Priya Kohli

Kandidatafhandling i Cand.merc.aud– Erhvervsret
Copenhagen Business School

Kontraktnummer: 11356
Antal anslag: 242.015 anslag
Antal sider: 113 sider

Indholdsfortegnelse

Abstract

This thesis is about the upcoming EU's General Data Protection Regulation (GDPR), which is going to be enforced on the 25th of May 2018, and has impact on the EU citizens, when they have given the personal information. The technological opportunity has changed radically since computer and internet came to the world, such as people exchanges information and personal data without thinking of the consequences. The purpose of the GDPR is to strengthen and harmonize data protection for individuals in the EU. GDPR applies to all organizations worldwide handling personal data about citizens of the EU. Not all third countries outside the EU provide a corresponding level of protection, which could lead to privacy violations and/or marketing abuse of the information. The thesis will examine whether the actual protection of EU citizens' information meets the theoretical protection provided by the Regulation for the transfer of personal data to subsidiaries operating in the EU, but transfers information to either subsidiaries in a third country outside EU cooperation or to parent companies in a third country outside EU cooperation. Similarly, the importance of the EU's principle of free movement of personal data has been taken into account and in comparison with the EU's international relations and trade, the principle has also been taken into account as the EU makes concrete assessments of the adequacy of all third countries' level of protection , so that there is no arbitrary decision on the matter. The results of our study show that the protection of personal data has been increased since 24 October 1995 when Directive 95/46 / EC was born and the improvement is supported by the adoption of the Regulation when harmonizing Union legislation in order to dilute the different interpretations of the Member States of what may apply to privacy, including the protection of personal data. The analysis by the Google Spain case from 2014 shows that web service providers' affiliates registered in the Union will also be covered by the Regulation's definition of "data controller" and can therefore be held responsible for processing personal data. Further in the analysis by the Schrems case from 2015 is illustrated the relationship between the Safe Harbor Agreement in 2000 and EU-US Privacy Shield Framework in 2016. Safe-Habor is invalidated in the judgment, which leads to the US and EU entering into EU-US Privacy Shield Framework to comply with the obligations deriving from the principles of Article 7 of the Charter on privacy and Article 8 on the protection of personal data.

1. Kapitel 1

1.1. Indledning

Den længe ventede Databeskyttelsesforordning[1] vil den 25. maj 2018 træde i kraft og dermed erstatte det nuværende Databeskyttelsesdirektiv[2]. Dette sker med ønsket om at modernisere de gældende regler, da vi står over for anvendelse af en masse nye teknologier, siden det gamle direktiv blev skrevet i 1995. Ved at skabe et fælles regelværk for medlemsstaterne, opnår man, altså lovgiverne, endvidere harmonisering af reglerne inden for EU. Hensigten er at værne om den basale menneskeret, nemlig at selv kunne bestemme hvem man deler sine oplysninger med og hvornår. Altså retten til at have et privatliv.

Fra gammel tid har husfredskrænkelser været betegnelsen for ulovlig indtrængen, altså at en person uberettiget har skaffet sig adgang til et ikke-offentligt sted. I den nyere tid hvor globalisering og internationalisering stadig er voksende, er der flere forhold, som kan krænke privatlivet, hvorfor retten til et privatliv tillægges stadig større betydning: På daglig basis registrerer vi borgere vores personlige data hos virksomheder, samt organisationer, sådan at persondata faktisk udgør en meget vigtig ressource, således at rammerne for hvornår et privatliv bliver krænket har rykket sig i takt med den teknologiske udvikling.

Privatlivets fred er evnen for den enkelte borger, grupper eller institutioner til selv at bestemme, hvornår og hvordan, samt i hvilket omfang oplysninger om dem formidles til andre. Dette forudsætter, at den enkelte kan kontrollere alle informationer om sig selv. Det er en løbende tilpasningsproces, hvor der balanceres mellem behovet for at værne om privatlivets fred med ønsket om videregivelse af oplysninger.

[1] Europa-Parlamentet og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)

[2] 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

De tekniske muligheder er i konstant udvikling, og i og med at handel inden for digital teknologi og –tjenester er blevet et centralt element i internationale økonomiske relationer, måtte det findes naturligt, at man inden for Den Europæiske Union må følge op på lovgivningen inden for dette komplekse område i forhold til behandling og lagring af persondata.[3]

Forordningen gælder for alle virksomheder der har etableret sig i EU eller retter tjenester mod folk i EU. Virksomheder uden for EU bliver således også omfattet, hvis de tilbyder varer eller tjenester til EU-borgere, så de også er forpligtiget til at overholde lovgivningen i forhold til registrering af persondata, herunder behandling af oplysningerne, samt overdragelsen af disse til tredjepart. Specielt vedrørende overførsel af persondata til lande uden for Den Europæiske Unions grænser, hvor der kan opstå komplikationer. Grænserne for og indholdet af, hvad der anses for *privatlivet fred* kan nemlig variere imellem kulturer og individer, til trods for at de deler et grundlæggende fælles tema. Ikke alle tredjelande uden for EU yder et tilsvarende beskyttelsesniveau, hvilket kan medføre til blandt andet integritetskrænkelser og/eller markedsføringsmæssig misbrug af oplysningerne, og i værste tilfælde kan det medføre til identitetstyveri[4]. Måden hvorpå vi, inden for EU's regi, definerer *tilstrækkeligt beskyttelsesniveau* giver særlig anledning til at undersøge hvilke forudsætninger der er, for at opretholde sikkerhedsforanstaltningerne, der kræves, at beskytte EU-borgernes persondata, hvis eller når de bliver overført til tredjelande. Ét er, hvad EU-lovgiverne indgår af aftaler ud fra vurderinger om tredjelandes beskyttelsesniveau, men andet er, hvis en EU-borger påberåber sig Databeskyttelsesdirektivet, eller den kommende Databeskyttelsesforordning - netop fordi *EU-borgeren* betvivler tredjelandets beskyttelsesniveau - er der så en reel beskyttelse i praksis?

EU-lovgiverne har således fået muligheden for at udvide virkeområdet for EU's lovgivning om personoplysninger ved i visse tilfælde at omfatte selskaber uden for EU,

[3] (EU) 2016/679: præambel 6 og 7, der udtrykker at teknologiens hastige udvikling, samt globaliseringen, og med særlig henblik på overførsel af personoplysninger til tredjelande, kræver det for EU-borgernes sikkerhed, at styrke en databeskyttelsesramme, som understøttes ad effektiv håndhævelse.

[4] Afhandlingen vil dog ikke undersøge forholdet om identitetstyveri, se afsnit 1.3. om afhandlingens afgrænsning.

som behandler data om borgere i EU. *Hvor* langt EU's virkeområde rent faktisk finder anvendelse er særligt interessant at undersøge, når lovgivningen ændres fra Databeskyttelsesdirektivet til Databeskyttelsesforordningen. Det er her særligt interessant at undersøge *hvilke* selskaber der omfattes, navnlig selskabernes nationalitet, og *hvorvidt* Databeskyttelsesforordningen vil have en reel beskyttende virkning på EU-borgernes personoplysninger ved overførsel af disse til tredjelande, som ikke er en del af Den Europæiske Union eller EØS-samarbejdet. Her er det interessant at undersøge hvorvidt den faktiske beskyttelse af EU-borgernes oplysninger lever op til den teoretiske beskyttelse som Forordningen vil yde, når det gælder overførsel af personlysninger til dattervirksomheder, der har fast drift i EU, men som sender oplysninger videre til moderselskaber i et tredjeland uden for EU-samarbejde. Problemstillingen vil da blive belyst ved at tage afsæt i gældende retsforhold, altså ud fra Databeskyttelsesdirektivet.

1.2. Problemformulering

Det er interessant at undersøge effekten af den kommende Databeskyttelsesforordning uden for EU's landegrænser, særligt i problemstillingen, der opstår ved overførsel af EU-borgers personoplysninger til *tredjelande*. Afhandlingen vil særligt belyse problemstillingen i forhold til overførsel til *usikre tredjelande*, ved at tage udgangspunkt i redegørelsen af forskellen mellem *sikre tredjelande* og *usikre tredjelande*.[5] I forlængelse hermed ønskes undersøgt hvorvidt EU-borgeren har tilstrækkelig adgang til at påberåbe sig forordningens lovgivning, når overførsel til et tredjeland har fundet sted.

Endvidere ønskes problemstillingen belyst ud fra to modsættende, men fundamentale EU-principper, navnlig princippet om beskyttelse af privatlivets fred og princippet om tjenesteydelsers frie bevægelighed. Princippet om privatlivets fred, herunder beskyttelse af personoplysninger finder hjemmel i Den Europæiske Unions Charter om Grundlæggende Rettigheder i artikel 7 og 8. Princippet om tjenesteydelsers frie bevægelighed vil blive redegjort på to niveauer: For det første vil afhandlingen redegøre for fri bevægelighed i henhold til Unionens definition, og dernæst blive redegjort i

[55] Jf. dir. 95/46/EF, art. 25, stk. 1, 2, 3, 4 og 6

henhold til Verdenshandelsorganisationens[6] definition. Denne toleddede redegørelse vækker diskussion i analysen med særligt henblik på forordningens præambel nr. 101, der udtrykker, at *strømmen af personoplysninger til og fra lande uden for Unionen og til og fra internationale organisationer er nødvendig af hensyn til udbygningen af den internationale samhandel og det internationale samarbejde*.

I betragtning af, at EU har opstillet nogle forbehold som forhindrer overførsel af personoplysninger til *usikre tredjelande*, er det interessante netop at undersøge de legitime hensyn der oppebærer forbeholdene, til trods for, at der i forordningens præambel 101 udtrykkes et ønske om at udbygge det internationale samhandel. Hvordan kan EU oppebære de to modsættende, men fundamentale principper, over for tredjelande i samme effekt som de har inden for EU's rammer, altså projiceringen af principperne til internationale forhold? Sagt på en anden måde, ønskes det undersøgt, *hvordan* de legitime hensyn anvendes i forhold til ønsket om, at følge princippet om *fri bevægelighed* over for *usikre tredjelande*. Det er netop i dette forhold, at belysningen af WTO-forholdet spiller ind.

Afhandlingen vil anvende Schrems-sagen, C-362/14, også bedre kendt som Facebook-sagen i medierne, analogt på indeholdende Alibaba-case. Hensigten er at undersøge om udfaldet i dommen har haft en særlig betydning for EU-borgere og deres sikkerhed i forhold til virksomhedernes behandling af deres personoplysninger, særligt ved overførsel af oplysningerne til de såkaldte *usikre tredjelande*.[7]

Det ønskes endvidere undersøgt, hvordan og hvorledes man inden for Unionen har taget problemstillingen i dommen til sig, og endvidere hvad udfaldet i dommen har medført i henhold til problemstillingen. Spørgsmålet er således, om man har skærpet forholdene omkring *overførsel af persondata* til tredjelande, og hvorfor man har fundet det nødvendigt. Hvis forholdene er skærpet, følger disse så det grundlæggende

[6] World Trade Organisation, WTO
[7] Begrebet uddybes i kapitel 5 og kapitel 12

proportionalitetsprincip? Endvidere ønskes det undersøgt *hvilken* indvirkning eller konsekvenser de forbehold eventuelt vil have på forholdet mellem EU og *tredjelande*?[8]

Ud fra problemformuleringen kan problemstillingen udledes, hvori det ønskes undersøgt om hvorvidt EU-borgerne kan føle sig sikre i forholdet om overførsel af personoplysninger fra EU-dattervirksomheder til deres moderselskaber henhørende *usikre tredjelande*[9], endvidere hvorledes den praktiske beskyttelse forefindes i henhold til den teoretiske beskyttelse i lovgivningen?

1.2.1. Problemstilling

Har den kommende Persondataforordning en reel beskyttende virkning på EU-borgernes personoplysninger ved overførsel af disse til tredjelande uden for EU?

1.3. Afgrænsning

Afhandlingen vil gennemgå Databeskyttelsesforordningens grundlæggende principper om *Kravet om samtykke for at lovlig behandling kan gøres gældende, Datas følsomhed, Oplysning, Retten til at blive glemt, Dataportabilitet, Retten til ikke at blive profileret, Den dataansvarliges pligter, Databehandlerens forpligtelser, Overførsel til tredjelande, One-stop-shop og sammenhængsmekanismen, Administrative bøder, og Harmonisering*. Principperne fra Databeskyttelsesdirektivet og forordningen vil redegøres kort i metode afsnittet, for at give en baggrundsforståelse for Dataforordningens virkeområder. De principper som har relevans for forståelsen af de problemstillinger, der opstår ved overførsler af persondata til tredjelande uden for EU og EØS-samarbejdet, således at de bidrager til forståelsen for problemformuleringen, vil da blive uddybet og anvendt i analysen.

[8] Afhandlingen vil anvende begrebet *tredjelande* som definition på lande, der ikke er EU-medlemsstater og som endvidere ikke er en del af EØS-samarbejdet. Bemærk, at *Tredjelande* vil blive defineret i afhandlingen i kapitel 5 og kapitel 12

[9] *Usikre tredjelande* er nærmere uddybet i kapitel 5 og kapitel 12

Afhandlingen afgrænser sig til problemstillingen ved overførsel af persondata fra EU til usikre tredjelande uden for EU- og EØS-samarbejdet. Problemstillingen omfatter som udgangspunkt hverken specifikke medlemsstater eller specifikke tredjelande, men forholder sig udelukkende til problemstillingen, der opstår i forholdet mellem EU over for et tredjeland uden for samarbejde. Det danske Datatilsyns vejledninger vil særligt blive anvendt til fortolkning af EU-lovgivningen, men den danske Persondatalov vil ikke blive nærmere anvendt, da der afgrænses fra nationale lovgivninger. Denne afgrænsning udleder særligt til at undersøge styrken i beskyttelse af EU-borgernes personoplysninger ved medlemsstaternes tilsynsmyndigheder ud fra direktivet og ud fra forordningen, jf. dir. 95/46, art. 28, henholdsvis, for. (EU) 2016/679, art. 51.

I forlængelse hermed vil forholdet om Verdenshandelsorganisationen blive redegjort og princippet om *fri bevægelighed* vil blive anvendt til diskussionen om EU's forbud mod overførsel af personoplysninger til *usikre tredjelande*. Afhandlingen vil således ikke gå i dybden med WTO-lovgivning, men udelukkende med henblik på, at skabe en nuanceret diskussion af problemstillingen.

Afhandlingens case om Alibaba anvendes til at belyse EU-borgerens sikkerhed i forhold til virksomheders overførsel af personoplysninger til tredjelande, og afgrænser sig fra andre virksomhedstyper end Alibaba Group.[10] Alibaba Group er en koncernvirksomhed, hvor moderselskabet har sæde i Kina, der har datterselskaber, kontorer, i Europa, og endvidere de amerikanske datterselskaber Alibaba.com, samt Alibaba Cloud, som begge har tiltrådt EU-U.S. – Privacy Shield ordningen, således at der kan overføres personoplysninger imellem de europæiske datterselskaber og de amerikanske datterselskaber. Afgrænsningen retter særligt fokus på anvendelsen ved Google Spain-sagen og Schrems-sagen, således at sagerne anvendes analogt på Alibaba Groups virksomhedstype. [11] I analysen vil Österreichischer-sagen [12] blive anvendt til at understøtte analyserne ved Google Spain-sagen og Schrems-sagen, med særligt henblik

[10] For. (EU) 2016/679, art. 4, litra 16b) om hovedvirksomhed, litra 17) om repræsentant, og litra 19) om koncern: Alibaba Group er det kinesiske moderselskab, Alibaba Group
[11] Altså koncernvirksomhed med moderselskab i et tredjeland uden for EU- og EØS-samarbejdet og datterselskaber inden for Unionen
[12] De forenede sager C-465/00, C-138/01 og C-139/01 (Österreichischer-sagen)

på at uddybe betydningen af princippet om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.

Ved analog anvendelse af EU-Domstolens afgørelser i Google Spain-sagen, [13] henholdsvis Schrems-sagen [14] på Alibaba-casen, kan afhandlingen således lave en uddybende analyse af EU-borgerens teoretiske beskyttelse i henhold til beskyttelsen i praksis. [15] Casen anvender det opstillede forhold, hvor datterselskaber under Alibaba Group er placeret rundt omkring i Europa[16], hvis moderselskab har hovedsæde i Kina. Kina er af Kommissionen ikke oplistet som værende et land, der sikrer et tilstrækkeligt beskyttelsesniveau.[17] Alibaba Group har dog et datterselskab i USA, Alibaba Cloud, som har indgået en gyldig aftale gennem EU-US Privacy Shield[18], hvorunder Alibaba.com-hjemmesiden også indgår i aftalen.

Afhandlingen vil således anvende casen til at konkretisere forholdet om overførsel af persondata ud fra datterselskaber i EU til sikre- og usikre tredjelande, herunder U.S.A.[19] og Kina, og afgrænser sig fra behandling af andre konkrete usikre tredjelande. Der afgrænses yderligere fra forholdet om overførsel af persondata imellem datterselskaberne inden for EU.

Schrems-sagen vil endvidere blive anvendt til at belyse forholdet om Safe-Harbor ordningen der ugyldiggøres i dommen, og som endvidere fører til, at USA og EU indleder en ny aftaleindgåelse, på lovligt grundlag, altså gennem Privacy Shield Framework. Afhandlingen vil ikke analysere på aftalernes indhold, men derimod anvende dem til at belyse EU's handlinger, når afgørelsen, udstedt af Kommissionen, betvivles og findes

[13] Sag C-131/12 (Google Spain-sagen)
[14] Sag C-362/14 (Schrems-sagen)
[15] Afhandlingen anvender begrebet "beskyttelse i praksis" i forhold til EU-borgerens klageadgang, og hvad klageadgangen indleder til, navnlig tilsynsmyndighedernes ansvarsområder
[16] Kontorerne ligger i henholdsvis Storbritannien., Italien, Frankrig, Tyskland og Holland: http://www.alibabagroup.com/en/contact/offices
[17] https://www.datatilsynet.dk/erhverv/tredjelande/sikre-tredjelande/ om tredjelande der generelt sikrer et tilstrækkeligt beskyttelsesniveau
[18] https://www.privacyshield.gov/list
[19] USA er defneret som værende sikkert tredjeland i henhold til EU-U.S. Privacy Shield aftalen, og nærmere i Kommissionens gennemførelsesafgørelse (EU) 2016/1250

ugyldig af EU-Domstolen, og at det endvidere leder til at lave en aftale på ny, der tilstræber at overholde forpligtelserne der udledes af principperne i chartrets artikel 7 om *privatlivets fred*, henholdsvis artikel 8 om *beskyttelse af personoplysninger*.

Endvidere er koncentrationen således rettet mod den private sektor, og ikke den offentlige sektor, herunder offentlige myndigheder.

Da fokus er rettet mod *overførsel af persondata til usikre tredjelande*, afgrænser afhandlingen ligeledes fra ISO 27001 og ISO 27002, der udleder problemstillinger i forhold til den tekniske sikkerhed, herunder virksomhedernes forvaltning af persondata, samt sikkerhedsbrud i form af hackerangreb og lignende.

Ydermere afgrænses afhandlingen fra at undersøge anvendelse- og opbevaring af persondata i forhold til kriminalitet, således at politidirektivet ikke vil blive undersøgt. Afhandlingen er dog opmærksom på de specifikke elementer i vurderingen af beskyttelsesniveauets tilstrækkelighed, som er fastsat i artikel 36, stk. 2, i politidirektivet, om *overførsler baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet*.[20]

I EU-landene hersker der forskellige opfattelser af grænsen for hvornår man anses for at være myndig. Derfor anskuer afhandlingen grænsen for myndige som værende 18-årige i henhold til dansk lovgivning, herunder Grundlovens[21] § 7 sammenholdt med Værgemålslovens[22] § 1, modsætningsvist. Problemstillingen udleder konkret forholdet

[20] Europa-Parlamentet og Rådets direktiv (EU) 2016/680 af 27. april 2016 *om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA*

[21] Danmarks Riges Grundlov (Grundloven): Vi Frederik den Niende, af Guds Nåde Konge til Danmark, de Venders og Goters, Hertug til Slesvig, Holsten, Stormarn, Ditmarsken, Lauenborg og Oldenborg, Gør vitterligt: I overensstemmelse med bestemmelserne i § 94 i Danmarks Riges Grundlov af 5. juni 1915 med ændringer af 10. september 1920 har rigsdagen 2 gange vedtaget, og folketingsvælgerne ved en den 28. maj 1953 afholdt folkeafstemning godkendt, hvorefter Vi nu ved Vort allerhøjeste samtykke stadfæster Danmarks Riges Grundlov

[22] Bekendtgørelse af værgemålsloven: Herved bekendtgøres værgemålsloven, lov nr. 388 af 14. juni 1995, med de ændringer, der følger af § 15 i lov nr. 542 af 24. juni 2005, § 8 i lov nr. 552 af 24. juni 2005 og § 26 i lov nr. 538 af 8. juni 2006. Den ændring, der følger af § 8 i lov nr. 434 af 8. maj 2006, er ikke indarbejdet i denne lovbekendtgørelse, da tidspunktet for ikrafttræden af

om persondata tilhørende myndige EU-borgere, og vil dermed afgrænse sig fra forholdet om børn, herunder definitionen om umyndige henhold til Værgemålsloven.[23]

1.4. Synsvinkel

Det skal som indledende bemærkes, at den formelle titel på den kommende *Databeskyttelsesforordning*, eller blot forordningen, anvendes igennem hele afhandlingen. Til trods for den tro anvendelse gennem afhandlingen, er den formelle titel dog ikke anvendt på titlen i afhandlingen, og dette er med god grund. Databeskyttelsesforordningen og dets indhold kan for den almene borger virke som et meget tungt og omfattende emne. Overordnet kan det virke som et abstrakt område, samtidig med, at det kan virke uigennemskuelig med forordningens omfattende indhold. *Persondataforordningen* er derimod anvendt i titlen på afhandlingen, med et symbolsk formål, der leder direkte til afhandlingens synsvinkel, navnlig den almene EU-borger.

Afhandlingens synsvinkel udspringer fra EU-borgerens over for udenlandske virksomheder med hovedsæde i *tredjelande*. Heri menes, at i det øjeblik en EU-borger afgiver sine personoplysninger[24] til en internetside tilhørende en virksomhed[25] med fast driftssted i EU, er en gyldig aftale indgået, med samtykke fra den registrerede[26], imellem EU-borgeren og EU-virksomheden, når reglerne i henhold til direktivet[27] er overholdt, alt andet lige. Retsforholdet, der som udgangspunkt er lovligt, kan dog ændre sig i det øjeblik, at EU-virksomheden sender personoplysningerne videre til sit moderselskab i et tredjeland uden for EU- og EØS-samarbejdet, således at retsforholdets lovlighed kan betvivles, og dermed bør undersøges. Årsagen til denne usikkerhed skal ses i lyset af, at

ændringen fastsættes af ministeren for familie- og forbrugeranliggender, jf. § 15, stk. 3, i lov nr. 434 af 8. maj 2006.

[23] Bekendtgørelse af værgemålsloven, LBK nr. 1015 af 20/08/2007

[24] Jf. dir. 95/46/EF, art. 2, litra a) om personoplysninger, i forlængelse hertil litra b) om personoplysninger der gør til genstand for behandling

[25] Jf. dir. 95/46/EF, art. 2, litra d) om den registeransvarlige

[26] Jf. dir. 95/46/EF, art. 2, litra h) om den registreredes samtykke

[27] Jf. dir. 95/46/EF, art. 6, stk. 1 og 2 om principper vedrørende oplysningernes pålidelighed

tredjelande kan defineres som værende sikre[28] eller som værende usikre[29]. Afhandlingen anvender den internationale koncernvirksomhed[30] Alibaba Group som case til netop at belyse de opstillede problemstillinger, der opstår med synspunkt fra EU-borgerens retsstilling.

1.5. Metode

1.5.1. Retskilder og retskildelæren

Projektets problemstilling vil blive besvaret ud fra juridisk analyse ved anvendelse af gældende retskilder i EU.

At være medlemsstat i EU medfører, at staterne i nogle tilfælde afgiver suverænitet, eksempelvis ved tiltrædelse af traktater. Herved har EU hjemmel til at regulere på det pågældende område i forhold til de tiltrædende medlemslande.[31] EU's beføjelser rækker dog ikke længere, end hvad der er givet dem hjemmel til af medlemslandene, jf. legalitetsprincippet. Ligeledes forventes det efter subsidiaritetsprincippet, at EU regulerer, hvor det findes nødvendigt og hvor det antages ikke at være tilstrækkelig effektivt, såfremt medlemslandene selv skulle regulere på området.[32] EU forpligter sig endvidere ved samarbejdet til, at betragte proportionalitetsprincippet, jf. TEU art. 5, som pålægger dem at regulere så reglerne er egnede til at sikre virkeliggørelsen af det formål, som de forfølger, og at de ikke må være mere indgribende end hvad der er nødvendigt.[33]

EU har ikke et veldefineret retskildehierarki som Danmark, hvor retskildelæren og den retsdogmatiske metode har en lang historie. EU har et forholdsvis nyt retssystem, EU-retten er kun 50 år gammel, hvilket er ungt for et retssystem[34], og dækker over mange

[28] Jf. dir. 95/46/EF, art. 25, stk. 6, hvor Kommissionen kan fastslå, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, jf. endvidere stk. 2
[29] Jf. dir. 95/46/EF, art. 25, stk. 3, om at et tredjeland ikke sikrer et tilstrækkeligt beskyttelsesniveau, jf. endvidere stk. 2
[30] Forordningens definition på koncernvirksomhed i artikel 4, litra 19)
[31] Rasmus Baastrup; http://www.eu-oplysningen.dk/dkeu/grundlov/hvornaar/ (2010, s. 1-2)
[32] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 136)
[33] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 182)
[34] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 53)

lande, hvorfor formålet med retssystemet bliver tillagt meget vægt, når forståelsen af retskilderne skal udledes. Retskildelæren definerer fire former for retskilder: *Regulering*, hvor der forekommer rangorden grundet lex superior-princippet [35] , *Retspraksis*, *Retssædvane* og *Forholdets natur*. I retskilderne er der hjemmel og retskilderne anvendes til retsvidenskabeligt at tage stilling til et retligt problem.[36] Endvidere er der ikke noget hierarki imellem retskilder, ifølge retskildelæren. I EU-ret klassificeres retskilderne efter Lissabon-traktatens[37] ikrafttræden således: *Primærretten*, som er EU's traktatgrundlag og grundlæggende rettigheder og retsprincipper, *Afledt ret*, altså bindende sekundærregulering, f.eks. forordninger, direktiver og beslutninger mv., samt *Subsidiære retskilder*, altså ikke bindende regulering, der består i EU-domme og soft law.[38]

Ved fortolkning af EU-retskilderne, kan retskildernes formål anskues, da disse er formålsbestemmelser. Dette har særligt betydning, da formålet findes i retsaktens tekst, særligt i den indledende artikel, men også i dennes præambel, samt i EU's overordnede formål.[39] Ved *teleologisk fortolkning*, altså objektiv formålsfortolkning, fortolkes der ud fra lovtekst og retlige principper.[40] Fortolkningen af EU-retskilderne kan styrkes ved fortolkning i flere sprog, men på grund af tidsbegrænsning er EU-rettens retskilder læst ud fra det danske sprog, som inden for EU er et autentisk sprog.[41]

Afhandlingens juridiske analyse vil i den redegørende del tage afsæt i den retsdogmatiske metode, for at følge en vis systematik, idet at EU endnu er et ungt retssystem, og derfor endnu ikke har en udviklet metode eller teori. Retsdogmatik er systematikken mellem *Retsfaktum* og *Retsfølge*.[42]
En retsregel består af to led, altså for det første af *retsfaktum*, som forudser de operative fakta med hensyn til kompetence, kilde, adressater, situation og indhold, mv., og for det

[35] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 34)
[36] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 30, 35)
[37] Traktat om den Europæiske Union
[38] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 119, 135)
[39] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 34)
[40] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 225)
[41] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 76)
[42] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 36)

andet af *retsfølge*, der foreskriver de retlige konsekvenser af de operative fakta, herunder muligheder for at anvende tvang til at håndhæve reglen.[43]

I den retsdogmatiske analyse anvendes retskilderne, men ud fra en antagelse af, at der er et hierarki imellem dem, hvor førstnævnte har størst retskildeværdi: *Primær ret*, herunder traktaterne og de generelle principper, endvidere chartret om grundlæggende rettigheder, nævnes som Chartret, samt folkeretlige aftaler, der er indgået af Den Europæiske Union, og *Sekundær ret*, som dog kun har gyldighed, hvis den overholder de retsakter og aftaler, som har forrang for den.[44] Sidst består de *subsidiære retskilder* i EU-domme, samt Soft law. En dom fra EU-domstolen er bindende i alle enkeltheder. Når den angiver, hvem den er rettet til, er den kun bindende for disse. Soft law er ikke bindende, men har derimod betydning for fortolkning af retskilderne. Soft law udvikles ved forholdets natur og retspraksis – men ender ofte som nedskrevne retskilder, som primær traktatregulering eller sekundær/afledt regulering, jf. eksempelvis Chartret.[45]

Afhandlingens analyse vil følge den retsdogmatiske systematik med det formål at få afdækket alle områder, før der kan konkluderes på emnet. Helt konkret betyder dette, at der først vil blive redegjort for nogle grundlæggende ting som har relevans for at forstå omstændighederne i problemstillingen, såsom forholdet imellem EU og tredjelande uden for EU- og EØS-samarbejdet, forholdet mellem Databeskyttelsesdirektivet og Databeskyttelsesforordningen, samt det generelle princip om *retten til privatlivets fred*, og princippet om *fri bevægelighed*. I afhandlingen vil princippet om *fri bevægelighed* blive redegjort i henhold til EU-regi og i henhold til Verdenshandelsorganisationen. Dette er med henblik på at få belyst forskellen mellem *fri bevægelighed* inden for EU og uden for EU, altså på internationalt plan.

Herefter vil det retsfaktuelle blive betragtet, hvilket i dette tilfælde er det faktum, at nogle tredjelande er oplistet hos EU-Kommissionen som værende lande, der sikrer et beskyttelsesniveau i forhold til retten til privatlivets fred, herunder personoplysningers

[43] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 62)
[44] Jævnfør Europa-Parlamentets hjemmeside om EU-retten – Kilder og rækkevidde: http://www.europarl.europa.eu/atyourservice/da/displayFtu.html?ftuId=FTU_1.2.1.html
[45] Chartret om grundlæggende rettigheder

sikkerhed, der lever op til EU's krav om sikkerhedsniveau, men ikke alle *tredjelande* er på denne liste. Udgangspunktet i analysen er, at alle tredjelande er ens, alt andet lige, hvoraf forskelle i tredjelande vil blive udledt, og at der dermed opstilles *sikre tredjelande* henholdsvis *usikre tredjelande*. Grunden til dette er, at Kommissionen har udstedt vejledning, samt liste over sikre tredjelande, hvortil virksomheder inden for EU kan videresende personoplysninger til, ved opfyldning af kriterier, som afhandlingen vil redegøre for i kapitel 5 og 11. Analysen vil nærmere undersøge forholdet om overførsel til *usikre tredjelande* i henhold til Alibaba-casen, hvor Kina bliver anskuet som *usikkert tredjeland*.

Herefter vil der i analysen anlægges en formålsfortolkning af relevante EU-lovregler, samt retspraksis fra EU-Domstolen, for at besvare på det juridiske problem.

Til at iagttage problemstillingen anvendes Databeskyttelsesdirektivet til at redegøre for, samt analysere gældende ret. Databeskyttelsesforordningen vil hertil anvendes til at sammenligne over for direktivet, således at der analyseres på forordningens styrke i forhold til direktivet, når forordningen træder i kraft.

Forordningen er med hjemmel i Traktaten om Den Europæiske Unions Funktionsmåde artikel 16 udstedt af Europa-Parlamentet og Rådet med det formål, at beskytte *fysiske personer i forbindelse med behandling af personoplysninger og regler om fri udveksling af personoplysninger*, jf. forordningens artikel 1, stk. 1, uanset om behandlingen foretages helt eller delvis ved hjælp af automatisk databehandling, eller ikke-automatisk behandling, jf. art. 2, stk. 1.

Forordninger er i henhold til TEUF art. 288, stk. 2 almengyldige, og er dermed direkte anvendelige således, at de er bidende i alle enkeltheder og gælder umiddelbart i hver Medlemsstat.[46] Dette betyder konkret, at forordninger ikke må inkorporeres i national ret, da de skal anvendes i deres EU-retlige form og endvidere betyder dette, at forordninger er klart direkte forpligtende både for det offentlige og for private.[47] Dette skal forstås

[46] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 223)
[47] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 223)

sådan, at forordninger finder anvendelse for alle i objektivt bestemte situationer.[48] Således er formålet, at udlede i hvilket omfang der er reguleret mod overførsel til tredjelande i fællesskabsretten, og dermed hvorvidt princippet om *tjenesteydelsers* fri bevægelighed finder anvendelse i forholdet mellem EU og tredjelande.

Det følger af subsidiaritetsprincippet, at EU's handling skal udformes så enkelt som muligt, således, at direktiver alt andet lige bør foretrækkes frem for forordninger, men som det fremgår af Hvidbogen[49] om nye styreformer, så anfører Kommissionen, at forordninger bør overvejes, *når der er behov for ensartet anvendelse og retssikkerhed i hele EU. Det kan være særligt vigtigt for fuldendelsen af det indre marked og har den fordel, at man undgår forsinkelser i forbindelse med gennemførelsen af direktiver i national lovgivning.*

Der vil således foretages en objektiv formålsfortolkning ved anvendelse af Databeskyttelsesforordningen, hvorunder enkeltbestemmelser, jf. CILFIT-dommen,[50] vil blive fortolket med hensyn til det samlede systems målsætning. Dommens præmis 20 lyder således:

20. Endelig skal de enkelte EF-regler vurderes i deres rette sammenhæng og fortolkes i lyset af EF-rettens bestemmelser som helhed, den bagved liggende målsætning og EF-rettens udviklingstrin på tidspunktet for de pågældende bestemmelsers anvendelse.

Dette har særlig betydning i forhold til analysen af direktivets kapitel IV om overførsel til tredjelande, navnlig kapitlets artikel 25 og forordningens kapitel V om overførsel til tredjelande, navnlig kapitlets artikel 44, hvor afhandlingen, jf. CILFIT-dommens præmis 20, vil betragte de nævnte artikler ud fra en helhedsfortolkning af direktivets- og forordningens overordnede formål.

Efterfølgende vil Google Spain-sagen og Schrems-sagen blive anvendt analogt som en del af analysen til en samlet besvarelse af problemformuleringen, og hvor

[48] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 129)
[49] KOM(2001) 428, *Nye styreformer i EU – En Hvidbog*, s. 17
[50] Sag 283/81 (pr. 20)

Österreichischer-sagen vil blive anvendt til at understøtte analysen i henhold til det grundlæggende princip om privatlivets fred. Domme afsagt ved EU-Domstolen er bindende sekundærregulering, og er således retligt bindende i alle enkeltheder. Når den er henvendt til en bestemt adressat, er den kun bindende for denne, jf. TEUF art. 288, 5. og 6. pkt., og således har High Court of Ireland (Irland) indgivet anmodning om præjudiciel afgørelse i henhold til nævnte artikel på vegne af Maximillian Schrems mod Data Protection Commissioner.

En national domstol har pligt til at forelægge EU-Domstolen et præjudicielt spørgsmål, såfremt der skulle opstå tvivl om fortolkning af EU-retten, ved en afgørelse som ikke kan appelleres, jf. TEUF art. 267, stk. 2. Dette betyder konkret i henhold til TEUF art. 267, at betingelserne om, for det første, at et spørgsmål rejses i forbindelse med en verserende sag, og for det andet at afgørelsen af spørgsmålet, skal være nødvendig for at en dom kan afsiges, skal være opfyldt. Hvis betingelserne er opfyldt, har EU-domstolen som udgangspunkt pligt til at besvare spørgsmålene EU-Domstolen har altså i henhold til TEUF art. 267, stk. 1, kompetence til at afgøre præjudicielle spørgsmål om fortolkning af traktaterne, samt gyldighed og fortolkning af EU-retsakter, og dermed præcisere over for den nationale domstol, hvordan de pågældende regler skal fortolkes.[51] Grundet sin bindende karakter for adressaterne, som er den nationale domstol ved præjudicielle spørgsmål, er denne forpligtiget til, at følge den foreskrevne fortolkning fra EU-Domstolen. Der skabes derfor retsvirkning for henholdsvis den nationale domstol og EU-Domstolen ved besvarelsen af det præjudicielle spørgsmål. Afgørelsen kan dermed anvendes analogt af andre nationale domstole, på spørgsmål af samme karakter.

Google Spain-sagen analyserer forholdet om behandling af personoplysninger på internettet og en internetudbyders anvendelse af personoplysninger til indeksering, hvor forskellen imellem søgemaskineudbyder og websideudbyder behandles nærmere. Sagen handler om Google Spain som søgemaskineudbyder, men vil blive anvendt analogt på Alibaba-casen, med særligt henblik på forholdet om websideudbyder og indeksering, samt profilering.

[51] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 74)

Schrems-sagen omhandler overførsel af personoplysninger til USA gennem daværende Safe Harbor-ordning, hvorfor den anvendes analogt i Alibaba-casen til at undersøge hvorvidt overførsel af personoplysninger til tredjelande generelt kan anerkendes. Problemstillingen i Safe Harbor-ordningen vil blive anskuet med henblik på at være blevet ugyldiggjort i Schrems-dommen og har ført til at EU-U.S. Privacy Shield er blevet vedtaget, som er grundlaget for lovlig overførsel af personoplysninger til virksomheder i USA. Endvidere leder analysen fra Schrems-sagen til diskussion om forskellen imellem overførsel til USA som et *sikkert tredjeland* og overførsel til Kina som et *usikkert land*, hvor betragtningerne i Politidirektivets artikel 36, stk. 2, vil blive anskuet i forholdet hertil.

Præjudikatværdien vil hertil blive anskuet til at vurdere begge dommes retskraft og i hvilket omfang de har dannet præcedens. Dissens, altså meningsforskelle og/eller uenigheder imellem dommerne ved en dommers mindretalsudtalelse, der strider mod den opfattelse, som rettens andre dommere giver udtryk for, anvendes ikke i EU-domme, som i danske domme.[52] Altså fremstår dommere som enige udadtil. Ved anvendelse af Generaladvokaternes forslag til dommene, kan det diskuteres, hvorvidt der kan have været uenighed, hvis altså Generaladvokaterne når frem til et andet resultat end dommens. En uenighed fra Generaladvokatens forslag kan dog ikke anvendes til at konstatere, hvorvidt der har været uenighed i og med, at dommerne fremstår som enige i domskonklusionen.[53]

Endvidere vil det blive fortolket hvordan EU-Domstolen anvender proportionalitetsprincippet i den forbindelse, for at forbuddet mod overførsel af personoplysninger i henhold til overholdelsen af dette kan opretholdes. Dele af afgørelsen vil således blive anvendt analogt på problemstillingen omkring forbud mod overførsel af personoplysninger til *tredjelande*.

Hertil vil Österreichischer-sagen blive anvendt som den analoge anvendelse af både Google Spain-sagen og Schrems-sagen. Sagen behandler særligt forholdet om beskyttelse

[52] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 178)
[53] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 178)

af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, hvor særligt EMRK artikel 8, endvidere chartrets artikel 7 og 8, bliver belyst i dette aspekt. Afhandlingen vil anvende relevante præmisser til at understøtte analysen i Alibaba-case, men vil dog ikke gå nærmere i dybden og analysere på Österreichischer-dommen.

Det skal bemærkes, at der inden for EU-retten anvendes en objektiv formålsfortolkning, som betyder, at fortolkningen tager udgangspunkt i lovteksten, samt en eventuel præambel til overordnet forståelse af konteksten i forordningen og/eller direktivet. Således skal formålet udelukkende udledes af lovens tekst og ordlyd. Dette adskiller sig fra den danske praksis på området, da man i Danmark særligt anvender en subjektiv fortolkning, hvortil man tillægger forarbejder stor værdi med det formål at anvende loven i overensstemmelse med lovgivers ønske. Man nærmer sig, i den danske metode, i højere grad den objektive formålsfortolkning, da EU-retten får stadig større betydning nationalt.[54] Retskilder i denne afhandling vil således blive fortolket efter den objektive formålsfortolkning i henhold til EU-regi.

1.5.2. Persondataforordningens formål

Afhandlingens problemstilling udleder til at undersøge forholdet i overgangen fra Databeskyttelsesdirektivet til Databeskyttelsesforordningen. Da Forordningens lovgivning udspringer fra Direktivet, finder afhandlingen det centralt at sammenligne betydningen i ændringen fra Direktiv til Forordning. Således vil analysen gå nærmere i dybden med Direktivets kapitel IV om *Videregivelse af personoplysninger til tredjelande* blive sammenlignet med Forordningens kapitel V om *Overførsler af personoplysninger til tredjelande eller internationale organisationer*, og hvis der forefindes forskelle, vil afhandlingen ligeledes gå nærmere i dybden med disse.

Til at iagttage problemstillingen anvendes Databeskyttelsesforordningen, udstedt af Europa-Parlamentet og Rådet, som har sin hjemmel i Den Europæiske Unions Charter

[54] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 55)

om grundlæggende rettigheder[55], også kaldet Chartret, artikel 8 om *at sikre respekt for privat- og familielivets fred*, hvori udgangspunktet for beskyttelsen af personoplysninger forefindes.

Databeskyttelsesforordningen fastslår, at databeskyttelse er en grundlæggende rettighed efter EU's Charter om grundlæggende rettigheder og traktaten om Den Europæiske Unions funktionsmåde. Som det nævnes i forordningens 6. præambel, har den hastige teknologiske udvikling og globaliseringen skabt nye udfordringer, hvad angår beskyttelse af personoplysninger. Denne udvikling kræver en stærk og mere sammenhængende databeskyttelsesramme i EU, om understøttes af effektiv håndhævelse, for at skabe den tillid, der gør det muligt, at den digitale økonomi kan udvikle sig på det indre marked. Endvidere beskriver forordningens 101. præambel, at strømmen af personoplysninger til og fra lande uden for EU er nødvendig af hensyn til udbygningen af den internationale samhandel og det internationale samarbejde.

Chartret om grundlæggende rettigheder har oprindeligt været soft law, men har fået traktatstatus ved Lissabon-traktatens vedtagelse i 2009, jf. TEU art. 6. Chartrets grundlæggende værdier består i menneskets værdighed, frihed, lighed og solidaritet. Chartret svarer langt hen ad vejen til Den Europæiske Menneskerettighedskonvention, EMRK – menneskerettighederne, som også er en del af EU-ret og dansk ret. Det svarer også til den hidtidige retspraksis fra EU-Domstolen, men går videre end både EMRK og retspraksis. Ved en kodificering af Chartret, har det formentlig også større juridisk gennemslagskraft.

Forordningen forener konflikten imellem to modsættende, men grundlæggende principper inden for EU; for det første er princippet om beskyttelse af personlige data, og for det andet den frie bevægelighed af sådanne personlige data inden for *det indre marked*. I stedet fastslår forordningen klart en balance mellem disse rettigheder og fastslår endvidere, at fri bevægelighed for personoplysninger inden for EU ikke må begrænses mere end hvad der er fastsat deri.

[55] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 306) om Den Europæiske Unions Charter om Grundlæggende Rettigheder (2010/C 83/02)

I en bilateral eller multilateral sammenhæng bør EU anvende lovgiverens begrundelse for, dvs. den forholdsmæssige balance mellem den grundlæggende ret til beskyttelse af personoplysninger og fri bevægelighed for sådanne oplysninger inden for det indre marked. Den samme ligevægt skal sandsynligvis også omsættes til en bilateral eller multinational aftale, hvilket betyder, at når de forhandler om databeskyttelseskrav i en aftale, bør de kombineres med bestemmelser, der muliggør fri bevægelighed for data (herunder personoplysninger) mellem landene.

Der gælder nogle fundamentale principper i forbindelse med behandling af personoplysninger, uanset om det er i henhold til Direktivet eller i henhold til Forordningen, hvorfor det findes nødvendigt at redegøre for disse principper i det følgende.

1.5.3. Principper

Kravet om samtykke for at lovlig behandling kan gøres gældende

Der er ikke noget nyt i, at der skal indhentes samtykke fra de registrerede ved behandling af almindelige personoplysninger i en række sammenhænge, for at behandlingen kan være lovlig. Dog er der alligevel noget nyt, da samtykket ikke længere blot kræves at være frit, specifikt og informeret, men dertil kræves det, at samtykket også skal være utvetydigt ved behandling af personfølsomme oplysninger. Dét er det, når de registrerede foretager en bekræftende handling, som tilkendegiver, at de accepterer en konkret behandling af personoplysningerne til et konkrete formål. Dette betyder også at et samtykke ikke kan udgøre et lovligt behandlingsgrundlag, hvis der er klar ubalance mellem datasubjektet og den dataansvarlige. Den dataansvarlige bliver hertil forpligtiget til at kunne dokumentere, at samtykket er tilkendegivet, og endvidere skal samtykket være eksplicit hvis der behandles følsomme personoplysninger. Dét er det lige så snart den registrerede eksempelvis har *godkendt* den dataansvarliges registreringer, eksempelvis i en boks der dukker op med valgmulighederne imellem ”Godkend” og ”Annuller”.

Datas følsomhed

I Databeskyttelsesforordningen vil der alene være tale om almindelige og følsomme personoplysninger.

Dette betyder, at oplysninger som navn, adresse, og e-mail vil bibeholde kategorien som almindelige personoplysninger. Yderligere vil oplysninger om strafbare forhold, sociale problemer og andre rent private forhold end følsomme oplysninger kategoriseres som almindelige persondata.

Oplysninger om race, etnisk oprindelse, politisk-, religiøs- eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetiske data, biometriske data, helbredsoplysninger, samt oplysninger om seksuelle forhold- eller orientering, kategoriseres som følsomme personoplysninger.

Ret til hjælp fra dataansvarlig

Den registrerede har ret til at få hjælp til at udfolde sine rettigheder fra den dataansvarlige.

Oplysning

Når Forordningen træder i kraft, skal virksomhederne give langt flere oplysninger om behandlingen, hvad de har været vant til. Oplysningerne der skal gives, indeholder blandt andet den dataansvarliges kontaktinformation, formålet med behandlingen, lovligheden af behandlingen, eventuel overførsel til tredjeparter, perioden for behandlingen (inklusiv lagring), retten til at gøre indsigelse og begrænse behandlingen, muligheden for at trække samtykke tilbage, muligheden for at klage til datatilsynet, samt angivelse af om behandlingen indgår i en profilering.

Retten til at blive glemt

Til trods for at der har været meget mediemæssig bevågenhed i forhold til retten at blive glemt, så bliver reglerne ikke væsentligt anderledes end i dag. Den registrerede har i en række tilfælde ret til at få slettet sine oplysninger, således hvis den dataansvarlige pålægges at slette disse personoplysninger, skal den ansvarlige tage rimelige skridt til at

andre dataansvarlige, som også behandler disse oplysninger, får slettet personoplysningerne eller links hertil.

Dataportabilitet

Der introduceres en ny rettighed som indebærer, at de registrerede kan kræve at få udleveret deres personoplysninger i et struktureret, almindeligt anvendt og maskinlæsbart format således, at de registrerede kan sende disse personoplysninger til en anden dataansvarlig. Formålet er at gøre det let for den registrerede dels at få overblik over alle sine data og dels at kunne portere sine data til en anden konkurrerende serviceudbyder.

Retten til ikke at blive profileret

Der introduceres yderligere en ny rettighed til de registrerede, som skal sikre, at de ikke kan profileres. Profilering er afgørelser, der alene er baseret på automatiserede behandlinger, som har retsvirkning eller betydelige konsekvenser, hvorfor profilering således ikke må bruges til f.eks. kreditvurdering eller e-rekruttering. Der kan dog samtykkes til profilering til markedsføringsformål, ligesom der også er enkelte andre retlige grundlag for profilering.

Generelt er hensigten med profilering at forudsige en persons fremtidige adfærd, som for eksempel på personens tidligere handlinger. Profilering defineres i Forordningen som enhver automatisk behandling af data, der udføres med henblik på at evaluere personlige aspekter, når dette har retlige virkninger i forhold til den pågældende person.

Forholdet om profilering har særlig betydning i forhold til Alibaba-casen, da Alibaba.com netop anvender sine kunders oplysninger til at profilere, og endvidere, ved at indsamle sine kunders søgehistorik, indekserer Alibaba.com, og finder de relevante varer, samt reklamer til den pågældende bruger.[56]

[56] Uddybes nærmere i kapitel 5

Evalueringen kan altså dreje sig om den pågældende persons arbejdsmæssige præstationer, økonomiske situation, personlige præferencer og interesser eller fremtidige adfærd.

Den dataansvarliges pligter

Den dataansvarlige vil fortsat have ansvaret for, at behandlingen af personoplysninger er i overensstemmelse med forordningen. Hertil bliver der introduceret en række nye forpligtelser for den dataansvarlige, der redegøres kort for.

Data protection by design and default er definition på, at beskyttelsen af personoplysninger skal under en række forudsætninger designes ind i en løsning og slås til som standard (data protection by design and default). I forordningens bilag 3, om privatlivsfremmende teknologier, gennemgås nogle tekniske bud på data protection by design, herunder pseudonymisering og kryptering, som fremstår som centralt tiltag i forordningen.

Dokumentation er meget centralt i forordningen, og betyder, at der skal udarbejdes dokumentation for den behandling, der foretages.

De *Fornødne sikkerhedsforanstaltninger* skal af den dataansvarlige fortsat, som i henhold til direktivet, tilvejebringe de fornødne sikkerhedsforanstaltninger, for at sikre at data ikke er til fare for misbrug.

Hvad angår *Meddelelse til Datatilsynet*, så skal der foretages meddelelse til datatilsynet i medlemsstaten, hvis der er sket en sikkerhedshændelse, som har kompromitteret personoplysninger. Under visse omstændigheder skal de registrerede ligeledes underrettes.

Ved *Risikovurdering* skal der under visse omstændigheder foretages en risikovurdering set fra de registreredes synspunkt ved at oplysningerne behandles. En såkaldt konsekvensanalyse.

Der skal i visse tilfælde udpeges en *Databeskyttelsesrådgiver*, som skal inddrages i alle spørgsmål vedrørende beskyttelse af personoplysninger. Inddragelsen bør således ske på øverste ledelsesmæssige niveau, som f.eks. ved deltagelse på direktions- og ledelsesmøder.

Den obligatoriske *Anmeldelse til Datatilsynet* i medlemsstaten, af behandling af personoplysninger bortfalder generelt. Hvis der behandles personoplysninger, som kan udsætte de registrerede for særlige risici, skal der under en række forudsætninger alligevel foretages anmeldelse.

Databehandlerens forpligtelser

I forhold til Direktivet får databehandleren som noget nyt sine egne forpligtelser. Databehandlerens forpligtelser har hidtil alene været reguleret i databehandleraftalen indgået mellem den dataansvarlige og databehandleren. Nu introduceres de særlige forpligtelser i forordningen. Der kan idømmes bøde, hvis databehandleren ikke efterlever disse. Væsentligst er det, at databehandleren er forpligtiget til at hjælpe den dataansvarlige med at efterleve en række af sine forpligtelser, således at databehandlerens forpligtigelse bliver at oplyse den dataansvarlige hvis det vurderes, at en instruktion er ulovlig.

Overførsel til tredjelande

Der kan overføres personoplysninger til tredjelande, hvis Kommissionen har truffet afgørelse om, at et tredjeland eller en organisation i pågældende land er sikkert, og uden at der først skal søges om godkendelse fra en kompetent tilsynsmyndighed eller lignende. Dette er dog under forudsætning af, at forordningens øvrige regler overholdes. Princippet om overførsel til tredjelande vil da uddybes nærmere i analysen.

One-stop-shop og sammenhængsmekanismen

Den dataansvarlige skal fremover som hovedregel alene interagere med datatilsynet i medlemsstaten, hvor virksomheden foretager beslutninger vedrørende behandlingen. Således vil hver virksomhed som hovedregel få ét datatilsyn som myndighed i stedet for 28 (for hver medlemsstat). Dette er i overensstemmelse med, at Unionen med

databeskyttelsesforordningen opnår ét enkelt paneuropæisk regelsæt, i stedet for de nuværende 28 nationale lovgivninger. Hvis et eventuelt tvist har sit udspring i en anden medlemsstat, end der hvor virksomheden interagerer med sit datatilsyn, skal datatilsynene i samarbejde via sammenhængsmekanismen, så der træffes afgørelser, som begge datatilsynene er tilfredse med. Hvis datatilsynene ikke kan blive enige om en afgørelse, vil afgørelsen eskaleres til samarbejdet mellem alle de europæiske datatilsyn, som træffer afgørelsen i fællesskab. Formålet er således at sikre en harmoniseret fortolkningspraksis på tværs af medlemsstaterne.

Administrative bøder

Virksomhederne kan pålægges bøder for ikke at overholde forordningen. For manglende efterlevelse af den dataansvarlige eller databehandlerens pligter, kan virksomhederne straffes med bøder på 2% af moderselskabets omsætning eller 10 mio. EUR, alt efter hvad der er højest. For manglende efterlevelse af principperne, de registreredes rettigheder, overførsel til lande uden for EU uden retligt grundlag eller manglende efterlevelse af ordrer fra datatilsyn, kan virksomheden straffes med bøder på 4% af moderselskabets omsætning eller 20 mio. EUR. Det største beløb vil således altid blive lagt til grund for en eventuel strafudmåling overfor den pågældende virksomhed.

Harmonisering

Da forordningen blev lavet, var det et essentielt hensyn, at der skulle ske en harmonisering af reglerne inden for EU. Dette kunne således sikres ved gennemførelse af en forordning, som er gældende i medlemsstaterne som den er, i modsætning til et direktiv, som skal tilpasses national ret, men også ved harmonisering af fortolkningspraksis gennem sammenhængsmekanismen, kan der således opnås en vis grad af harmonisering med de nye regler.

Man har i det politiske kompromis lavet ganske mange muligheder for at fastsætte national lovgivning, dels for at fastsætte mere bestemte regler for anvendelsen af forordningen, og dels ved i national lov at fastsætte retligt grundlag på særlige områder. National lovgivning og nærmere fastsatte regler vil derfor underminere harmonisering på en række områder, hvorfor virksomhederne er nødt til at være opmærksomme på,

hvorvidt der er fastsat national lovgivning i de EU-medlemsstater de opererer i, og dermed ikke alene fokusere på at efterleve forordningen.

1.5.4. EU's internationale relationer gennem Verdenshandelsorganisationen

Hvis EU afstår fra at indgå i bilaterale eller multilaterale forhandlinger og i stedet fortsat anvender Databeskyttelsesforordningen ensidigt, kan der være en højere risiko for, at et WTO-medlem kunne udfordre Forordningen under Verdenshandelsorganisationens regler.

På grund af den hurtige tekniske udvikling i de seneste år er flertallet af grænseoverskridende dataoverførsler helt uafhængige af enhver bevægelse af fysiske varer. I dag er det mere sandsynligt, at sådanne overførsler vil være knyttet til grænseoverskridende tjenester. Derfor ville en WTO-udfordring til Forordningen sandsynligvis blive fremsat under henvisning til GATS.

1.6. Projektets struktur

Afhandlingen lægger ud med sit kapitel 1, som indeholder indledningen, der beskriver behandling af personoplysninger som et internationalt emne, og leder videre til problemformuleringen, hvor forskellige delproblemstillinger udledes, og endvidere fører til den overordnede problemstilling. Efterfølgende beskriver afsnittet om afgrænsning hvad afhandlingen nærmere behandler, og herunder hvad afhandlingen ikke vil behandle nærmere. I metodeafsnittet beskrives selve den retsdogmatiske metode som anvendes i afhandlingen i forhold til den juridiske problemformulering- og stilling. I kapitel 2 behandles EU-institutioner nærmere, dette er med henblik på at klargøre EU-institutionernes roller i forhold til Databeskyttelsesforordningen, også Direktivet. Kapitel 3 behandler EU's princip om tjenesteydelsers fri bevægelighed med henblik på at projicere princippet i forhold til EU's internationale forhold, altså ledes videre til kapitel 4, navnlig forholdet til andre medlemsstater inden for Verdenshandelsorganisationen, og hvordan EU kan opretholde sin forpligtelser hertil, samt oppebære Chartrets bestemmelser om de grundlæggende rettigheder som vægtes ved fortolkningen af Databeskyttelsesdirektivet- og Forordningen.

I kapitel 5 behandles betydningen i ændringen fra bestemmelser om databeskyttelse i form af direktiv til i form af forordning. Dette er med henblik på, at undersøge hvorvidt EU-borgeres rettigheder bestyrkes og forbedres.
I det 6. kapitel behandles EU-borgernes rettigheder i forhold til Databeskyttelsesforordningen, særligt rettighederne i forhold til virksomheder, der som dataansvarlige behandler EU-borgeres oplysninger, og derefter i forhold til EU-borgernes klageadgang, altså i forhold til ansvarlige tilsynsmyndighederne.
I kapitel 7 udledes Alibaba-casens forhold til det Europæiske Marked og leder således videre til kapitel 8, hvor anvendelsen af Google Spain-dommen og Schrems-dommen belyses.
I kapitel 9 redegøres for Österreichischer-dommen med særligt henblik på at udrede EU-Domstolens fastsættelse af betydningen af EMRK's artikel 8, herunder Chartrets artikel 8, om EU-borgeres grundlæggende rettighed i forhold til beskyttelse af personoplysninger.
I kapitel 10 analyseres Alibaba-casen ud fra Google Spain-dommen og endvidere i kapitel 11 analyseres Alibaba-casen ud fra Schrems-dommen.
Afhandlingens konklusion findes i kapitel 12 og endvidere perspektiveringen i kapitel 13 bliver belyst.
I kapitel 14 er litteraturlisten oplistet med bibliografi, anvendte retskilder, EU-domme- og afgørelser, samt anvendelsen af Europæiske Datatilsyn, og til sidst anvendte hjemmesider til inspiration af afhandlingen, endvidere brug af Justitsministeriet, samt Datatilsynet til at understøtte fortolkning af EU-retskilder.

2. Den Europæiske Union

I dette afsnit vil der redegøres for Den Europæiske Union, herunder EU's institutioner, navnlig EU-Domstolen, og lovgivningsprocessen. Hertil vil EU's kompetence i forhold til national ret blive redegjort, og endvidere vil der redegøres for retskilderne, herunder EU-rettens forrang. Dette er med henblik på at forstå forholdene imellem de gældende retskilder og afgørelser i forholdet om personoplysninger og behandling af disse, herunder overførsel til tredjelande.

2.1. Medlemsstaternes og EU's indbyrdes forhold

Ved Medlemsstaternes tilslutning til den Europæiske Union afgives enten delvis eller fuld suverænitet, således at Medlemsstaterne lader sig tilslutte fællesskabsretten hvor EU dermed har hjemme til at regulere.
Eksempelvis lod Danmark sig tilslutte til EU (daværende EF, det Europæiske Fællesskab) i 1973 og lod sig afgive delvis suverænitet. Dermed lod Danmark sig tilslutte fællesskabsretten hvor EU har hjemmel til at regulere.

Til trods for at EU-retten ikke har udviklet en juridisk metode, eksisterer der nogle fortolkningsprincipper, som medlemsstaterne skal iagttage. Det drejer sig som EU-rettens forrang og EU-konform fortolkning. EU-rettens forrang er ikke et traktatfæstet princip, men blev derimod fastslået i sagen 6/64, Costa mod ENEL.[57] Ifølge EU-Domstolen har bindende EU-regulering med direkte virkning forrang for national ret.[58]

EU-konform fortolkning er, som princippet om EU-rettens forrang, heller ikke traktatfæstet. EU-Domstolen har dog udledt fortolkningsprincippet af loyalitetsprincippet i TEU art. 4, nr. 3, der blandt andet tilsiger, at *"Medlemsstaterne træffer alle almindelige eller særlige foranstaltninger for at sikre opfyldelsen af de forpligtelser, der følger af traktaterne eller af retsakter vedtaget af EU-institutionerne"*. Princippet pålægger altså Medlemsstaterne, så vidt muligt, at skabe overensstemmelse mellem EU-retten og den nationale ret.[59] Pligten til at fortolke national ret EU-konformt, er ligeledes en pligt for de nationale domstole til fuldt ud at anvende det eksisterende nationale fortolkningsskøn, hvormed man vil kunne opnå en EU-konform løsning.[60]

2.2. EU's institutioner

[57] Ulla Neergaard & Ruth Nielsen; EU ret (2016, s. 45)
[58] Ulla Neergaard & Ruth Nielsen; EU ret (2016, s. 244)
[59] Ulla Neergaard & Ruth Nielsen; EU ret (2016, s. 45)
[60] Ulla Neergaard & Ruth Nielsen; EU ret (2016, s. 239)

EU's institutioner består af Kommissionen, Europa Parlamentet, Ministerrådet, EU-Domstolen, Den Europæiske Revisionsret og Den Europæiske Centralbank.[61]
Europa-Kommissionen har som hovedregel eneretten til at fremlægge lovforslag i EU. Rådet, gerne i samarbejde med Europa-Parlamentet, vedtager efterfølgende lovene, men Kommissionen kan dog i nærmere afgrænsede tilfælde selv vedtage regler. [62]
Europa-Parlamentet er medlovgiver sammen med Rådet. Den almindelige lovgivningsprocedure indebærer, at Rådet og Europa-Parlamentet skal være enige om et lovforslag, før en retsakt kan blive vedtaget.[63]
Rådet for Den Europæiske Union kaldes ofte for "Ministerrådet" eller blot "Rådet", og er sammen med Europa-Parlamentet de lovgivende institutioner i EU.[64]
EU-domstolens rolle er til, for at sikre at EU-lovgivningen fortolkes og anvendes på samme måde i alle Medlemsstater, samt at landene og EU-institutioner overholder reglerne.[65] Den er oprettet i 1952 i Luxembourg, og er sammensat af 47 dommere fra EU-lande, samt 11 generaladvokater.

2.3. Nærmere om EU-Domstolen

EU-domstolens primære rolle er at sikre at fortolkning, samt at afgøre retstvister mellem national regering og EU's institutioner. Den kan i visse tilfælde anvendes af enkeltpersoner, virksomheder eller organisationer til at påberåbe sig overfor en EU-institution, hvis de mener at den har tilsidesat deres rettigheder.

EU-Domstolen er den dømmende magt på EU-regulerede områder, og har således kompetence til at afsige dom i typiske følgende sager: præjudicielle afgørelse, overtrædelsesprocedurer, annullationssøgsmål, passivitetsspørgsmål samt erstatningsspørgsmål og forelæggelser. Forskellen i disse vil nu kort blive redegjort.

[61] Ulla Neergaard & Ruth Nielsen; EU ret (2016, s. 42)
[62] Ulla Neergaard & Ruth Nielsen; EU ret (2016, s. 105)
[63] Ulla Neergaard & Ruth Nielsen; EU ret (2016, s. 103)
[64] Ulla Neergaard & Ruth Nielsen; EU ret (2016, s. 104)
[65] Ulla Neergaard & Ruth Nielsen; EU ret (2016, s. 106)

Nationale domstole kan kun stille spørgsmål under en aktuel tvist og i forbindelse med dennes afgørelse. EU-domstolen laver ikke responsa. Domstolen kan kun udtale sig om EU-regler, ikke om nationale regler. Den går dog ofte langt med hensyn til udtalelsen om nationale reglers overensstemmelse med EU-retten.

Fortolkning af love, altså *præjudicielle afgørelser,* hvor de nationale domstole som udgangspunkt skal sikre, at EU-lovene anvendes og fortolkes korrekt, altså EU-konformt, men nogle gange kan de nationale domstole i EU-landene fortolke EU-lovene forskelligt. Hvis en national domstol er i tvivl om fortolkningen eller gyldigheden, kan denne spørge EU-Domstolen til råds. På samme måde kan EU-Domstolen afgøre om national ret eller retspraksis er forenelig med EU-retten.

Præjudicielle forelæggelser, er spørgsmål, der ofte forelægges for en generaladvokat, hvorefter denne skal oplyse om sagen og komme med et begrundet forslag til et svar. Søgsmålene indledes med sagens nummer og stikord om sagen, og derefter følger et resumé af sagen, med de væsentlige konklusioner. Derefter præsenteres sagen af parterne, en national domstol og EU-domstolen, samt kendelsen, der fører til fremlæggelsen af det præjudicielle spørgsmål. Endvidere oplyses hvilke bestemmelser i EU-retten det drejer sig om, og derefter de nationale bestemmelser, efterfulgt af de præjudicielle spørgsmål, og hvorefter spørgsmålene besvares ét efter ét. Sidst opsummeres svarene og sagsomkostningerne, i sagens udfald.

2.4. Grunde, der taler for og imod at tillægge præjudikater retskildeværdi

En række omstændigheder taler for at benytte præjudikater som retskilde. Det er en procesbesparende, herunder appelbesparende og derigennem arbejds- og omkostningsbesparende anvendelse.

Det kan således lette dommernes arbejde, hvis de kan skrive af efter et fortilfælde frem for selv at skulle udtænke en løsning. Det styrker måske indtrykket af rettens autoritet, hvis resultatet af forskellige retssager bliver det samme, og det sikrer den formelle

retfærdighed, dvs. princippet om, at det lige skal behandles lige eller sagt på en anden måde, at enhver konkret afgørelse skal begrundes i en almindelig regel.

Hvis en dom har dannet grundlag for udvikling af en administrativ praksis, vil dette tale for, at dommen følges op i senere retspraksis.

På den anden side kan der også være stærke grunde til at bryde med ældre praksis. Det vil navnlig gælde, hvis der er sket en betydelig samfundsudvikling på et område. Det vil da være utilfredsstillende at lade sig styre af fortiden. Herved ville den materiale, altså det indholdsmæssige, retfærdighed blive tilsidesat til fordel for den formelle retfærdighed.

Domstolens hovedfunktion antages normalt at være at løse de konflikter, parterne forelægger for dem. En vidtdreven præjudikatdyrkelse forskyder vægten fra den konkrete konfliktløsning over mod den generelle regeldannelse og giver i nogen grad domstolene lovgivende funktioner, hvilket strider mod magtfordelingslæren.[66]

2.5. EU-ret

Principper i traktater om for eksempel *fri bevægelighed* mm. er som udgangspunkt direkte anvendelige. Ligeledes er forordninger direkte anvendelige, jf. art. 288, hvorfor de ikke skal inkorporeres i national ret, men anvendes i deres EU-retlige form, således at de er anvendelige både for offentlige og private.
Ved direktiver er der tale om en vertikal direkte virkning, at de har direkte virkning overfor myndigheder, men ikke overfor private. Direktiver har altså ikke direkte horisontal virkning, da de skal implementeres, før de gælder overfor borgere og virksomheder. En borger eller en virksomhed kan dog påberåbe sig et direktiv overfor en offentlig myndighed.

[66] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 32)

EU-retsprincipper uden for traktater skal i national ret respekteres, hvorfor de har derfor direkte virkning, på områder for EU, som eksempelvis Chartret, der ved Lissabon traktaten fik traktatrang, jf. TEU art. 6. Chartret har særlig betydning i forhold til problemstillingen og Alibaba-casen, fordi direktivet og forordningens indhold skal læses i henhold til Chartrets artikel 8 om beskyttelse af personoplysninger.

Princippet om EU-rettens forrang er flittigt blevet omdiskuteret. Direkte anvendelig EU-ret, herunder traktatbestemmelser, forordningsbestemmelser og præcise direktivbestemmelser har forrang for national ret, i hvert fald ifølge EU-domstolen, jf. sag 6/64, Flaminio Costa mod ENEL. Sammenstød mellem disse og national ret medfører derfor, at national ret må vige. De nationale domstole skal således undgå at anvende regler der strider med EU-retten.[67]

Rækkevidden af dette princip er omdiskuteret, og er alene fastslået via retspraksis. Princippet om forrang er derfor ikke så entydigt, hvis spørgsmålet om dets rækkevidde besvares af medlemsstaterne.[68]

EU har et fortolkningsprincip, der kan udfylde de huller i EU-rettens gennemslagskraft, der måtte være tilbage efter principperne om direkte virkning og forrang. National ret skal således fortolkes i overensstemmelse med EU-retten.

Ved fortolkning af EU-retskilderne, kan restkildernes formål anskues, da disse er formålsbestemmelser. Dette har særligt betydning, da formålet findes i retsaktens tekst, særligt i den indledende artikel, men også i dennes præambel, samt i EU's overordnede formål.[69] Ved *teleologisk fortolkning*, altså objektiv formålsfortolkning, fortolkes der ud fra lovtekst og retlige principper.[70] Fortolkningen af EU-retskilderne kan styrkes ved fortolkning i flere sprog, men på grund af tidsbegrænsning er EU-rettens retskilder læst ud fra det danske sprog, som inden for EU er autentisk sprog.[71]

[67] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 121)
[68] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 122)
[69] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 34)
[70] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 225)
[71] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 76)

2.6. EU's kompetence i forhold til national ret

2.6.1. Legalitetsprincip og hjemmel

EU har kun kompetence til at vedtage regler af et indhold, der falder inden for, hvad der er tillagt dem ved EU- og EF- traktaterne. Der er derfor enkelte nationale forhold, der falder uden for EU-rettens kompetence til at lovgive, f.eks. visse forhold omkring grundloven. En stor del af den nationale kompetence falder dog indenfor. EU-retskilder skal således have hjemmel, dvs. de skal holde sig indenfor de områder, de har fået kompetence til at lovgive indenfor, ellers er lovgivningen ugyldig.[72] Med ugyldighed menes nærmere, at retsakten ikke har nogen betydning i national ret. Modsat er dansk lovgiver ikke på samme måde begrænset af et hjemmelskrav, de kan stort set lovgive om alt.[73]

EU's kompetence styres af principperne om *subsidiaritet* og *proportionalitet*.[74] Princippet om *subsidiaritet*, lader EU lovgive på de områder, hvor det ikke vil være tilstrækkeligt effektivt, at medlemsstaterne lovgiver individuelt. EU skal således kun lovgive, hvor det er nødvendigt, også kaldet nærhedsprincippet. Princippet skaber et dynamisk retssystem, hvor EU kan udvide og indskrænke lovgivningen efter behov, blot det er inden for EU's beføjelser. Princippet om *proportionalitet* har den betydning, at lovgivningen skal forfølge et lovligt mål og ikke må gå udover hvad der er nødvendigt, for at opnå det tiltænkte mål. Der anvendes en treleddet test, herunder om der er et lovligt mål, at midlerne til at nå det er egnet, og at de ikke må være mere indgribende end nødvendigt.

I henhold til Traktaten om EU's Funktionsmåde artikel 294, om EU's lovgivningsprocedure, kan der kun vedtages regler inden for de emner, som EU har kompetence til at vedtage regler indenfor. EU- regler skal således have regler, ellers er de

[72] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 37-39)
[73] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 109)
[74] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 135-136)

ugyldige. Det vil sige, EU kan ikke få fikse ideer og lovgive om noget medlemslandene ikke har givet dem kompetence til.

Europa-Parlamentet og Rådet har sammen vedtaget Direktiv 95/46/EF, Databeskyttelsesdirektivet, i oktober 1995. Dette er således i overensstemmelse med art. 14 TEU, hvor Europa-Parlamentet sammen med Rådet udøver den lovgivende magt.[75] Direktivet er endvidere udstedt overensstemmende med EMRK artikel 8 om beskyttelse af menneskerettigheder og frihedsrettigheder, jf. direktivets præambel 10.

Ligeledes har Europa-Parlamentet sammen med Rådet udstedt og vedtaget Forordning (EU) 2016/679, Databeskyttelsesforordningen, i april 2016. Forordningens bestemmelser er vedtaget i overensstemmelse med Chartrets artikel 8, stk. 1 om grundlæggende rettigheder og endvidere i overensstemmelse med TEUF artikel 16 og enhvers ret til beskyttelse af personoplysninger. Af forordningens præambel 170 fremgår det endvidere, at forordningen er vedtaget i overensstemmelse med proportionalitetsprincippet i henhold til TEU art. 5, at forordningen ikke går videre end hvad der er nødvendigt for at nå forordningens formål, nemlig at sikre et ensartet niveau for beskyttelse af fysiske personer og fri udveksling af oplysninger i Unionen, jf. 170. præambel.

3. Princippet om fri bevægelighed for tjenesteydelser

Grænseoverskridende handel af varer og tjenesteydelser har en større og større betydning ved hjælp af især Internet. Dette er uanset om det er inde for EU eller med tredjelande uden for EU. Udveksling af persondata er i forbindelse hermed på højeste niveau af aktuelle emner på international plan.

Almindelige principper og grundlæggende rettigheder skal for det første respekteres internt i EU-retten. Alle EU-institutioner skal respektere dem, når de vedtager regler og træffer beslutninger.

[75] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 35)

Grundlæggende rettigheder skal derudover for det andet respekteres i national ret på EU-regulerede områder, men ikke på områder, der ikke er EU-regulerede. Det betyder, at de skal respekteres, når Medlemsstaterne implementerer EU-regler, og når de indfører restriktioner for den fri bevægelighed.[76]

I ERT-sagen og Familiapress-sagen fastslog EU-Domstolen i sager om fri bevægelighed at når en Medlemsstat påberåber sig bestemmelser, som kan begrænse den fri udveksling af tjenesteydelser (ERT) eller varer (familiapress), skal begrundelsen herfor fortolkes i lyset af de almindelige retsgrundsætninger, navnlig grundrettighederne. De nationale bestemmelser kan derfor kun begrunde indskrænkninger i reglerne om fribevægelighed, hvis de er i overensstemmelse med de grundlæggende rettigheder, som EU-domstolen beskytter.

3.1. EU's princip om Fri bevægelighed

Grundlaget for det indre marked er de fire friheder, som er fastlagt i EU-Traktaten: fri bevægelighed for varer, for personer, for tjenesteydelser og for kapital.[77] Afsnittet vil kort redegøre for de fire friheder, dog vil fri bevægelighed for tjenesteydelser blive uddybet nærmere. Dette er med henblik på at kunne begrebsliggøre persondata, da disse i henhold til Databeskyttelsesdirektivet og i henhold til Databeskyttelsesforordningen som udgangspunkt skal kunne videreføres frit inden for Unionen. Dette leder hen til at undersøge hvorvidt den frie bevægelighed kan overføres i det internationale forhold i henhold til Verdenshandelsorganisationen, og fri bevægelighed herunder.

3.1.1. Fri bevægelighed for varer

I de fleste tilfælde er det ikke et problem at afgøre om noget er en vare. EU-Domstolen har i relation til toldunionen, navnlig i relation til artikel 23 EF (nu artikel 28 TEUF), defineret varer bredt som produkter, *hvis værdi kan måles i penge, og som i sig selv kan*

[76] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 212)
[77] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 267)

være genstand for omsætning, jf. eksempelvis Sag C-115/02, pr. 77.[78] Hertil understreges ofte det fysiske element samt til tider et krav om varens grænsepassage.[79]

De frie varebevægelser blev oprindelig fastlagt inden for rammerne af toldunionen med ophævelse af told, kvantitative restriktioner og tilsvarende bestemmelser i samhandelen mellem medlemslandene, samt indførelse af en fælles toldtarif over for tredjelande. De frie varebevægelser er først for alvor blevet en realitet med gennemførelsen af det indre marked den 1.1.1993. Grundlaget blev skabt i Den Europæiske Fælles Akt, som trådte i kraft i 1987.[80] Heri blev det indre marked defineret som et område uden indre grænser, inden for hvilket den frie cirkulation af varer, personer, tjenesteydelser og kapital skulle sikres gennem traktatens bestemmelser. Således blev fysiske hindringer fjernet, det vil sige kontrol ved grænserne, tekniske hindringer blev fjernet gennem indførelse af eksempelvis fælles standarder, regulering af regler om offentlige indkøb og endvidere blev hindringer på afgiftsområdet fjernet i et vist omfang ved at gennemføre harmonisering af medlemslandenes moms og punktafgifter.[81]

Arbejdet med at fjerne begrænsninger i de frie varebevægelser er gennemført ved en omfattende fælles lovgivning, som for størstedelens vedkommende er vedtaget med kvalificeret flertal [82] i Ministerrådet og med EU-Parlamentets aktive medvirken. [83] Gennemførelsen af det indre marked har været afgørende for Fællesskabets udvikling og har ydet et væsentligt bidrag til den europæiske industris internationale konkurrenceevne.

Det må hertil udledes, at persondata ikke kan defineres som varer i henhold til at persondatas værdi ikke kan måles i penge, og som i sig selv kan være genstand for

[78] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 331 og 335) og Sag C-115/02, Administration des douanes et droits indirects mod Riogalss SA og Transremar SL, Saml. 2003 I-12705, præmis 17
[79] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 331)
[80] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 271)
[81] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 272-274)
[82] Et kvalificeret flertal kræver, at 55 pct. af medlemslandene, der repræsenterer mindst 65 pct. Af EU's befolkning, stemmer for forslaget: Hjemmesiden for Det Europæiske Råd, Rådet for Den Europæiske Union, om stemmeregler: http://www.consilium.europa.eu/da/council-eu/voting-system/qualified-majority/
[83] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 271-272)

omsætning, sammenholdt med at persondata ikke er et fysisk element, og endvidere sammenholdt med argumentet om, at persondata i sig selv ikke er fysisk element, der kan transporteres over en grænsepassage. Princippet om vareres fri bevægelighed finder således ikke anvendelse på persondata, som følge heraf.

3.1.2. Fri bevægelighed for personer og tjenesteydelser

Romtraktaten fra 1957 garanterede borgerne i medlemslandene fri passage over de indbyrdes grænser uden kontrol og formaliteter, samt adgang til erhvervsudøvelse i andre medlemslande på lige fod med deres egne borgere. Oprindeligt tog traktatbestemmelserne især sigte på fri bevægelighed for personer i *erhvervsøjemed*, dels arbejdstagere og personer, som etablerer sig som selvstændige erhvervsdrivende, og dels personer, som præsterer tjenesteydelser. Grundprincippet var afskaffelse af forskelsbehandling af egne statsborgere og borgere fra andre medlemslande.[84]

For arbejdstagere fastslog EF-Domstolen i 1974, at enhver statsborger i et medlemsland fra 1.1.1970 med sin familie skulle have ret til frit at bevæge sig inden for medlemslandenes område, for at søge beskæftigelse og arbejde på samme vilkår som indenlandske arbejdstagere. Medlemsstaterne kunne dog begrænse den frie bevægelighed, når det blev begrundet i hensyn til den offentlige orden, sikkerhed og sundhed.

For at fremme den frie bevægelighed for personer, hvad enten der er tale om arbejdstagere, om etablering eller om præstation af tjenesteydelser, er der gennemført vidtgående regler

[84] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 272)

angående gensidig anerkendelse[85] af uddannelser og kvalifikationer.[86] I første omgang var disse regler baseret på en vis harmonisering af uddannelseskravene, især inden for en række liberale erhverv.

Den frie bevægelighed for personer fik særlig betydning i forhandlingerne om unionsborgerskab i Maastrichttraktaten. Bestræbelser på at skabe et "borgernes Europa" omfattede især retten til fri bevægelighed og fri opholdsret i ethvert medlemsland. Ved Maastrichttraktaten blev disse rettigheder traktatfæstet for også ikke-erhvervsaktive i EF-Traktaten, idet det såkaldte unionsborgerskab blev indført, og det blev fastslået, at enhver unionsborger har ret til at færdes og opholde sig frit på medlemsstaternes område med de begrænsninger og på de betingelser, der er fastsat i EF-Traktaten og i gennemførelsesbestemmelserne hertil. Etableringsretten og retten til at præstere tjenesteydelser omfatter også juridiske personer. Særligt den frie bevægelighed for tjenesteydelser inden for finanssektoren, på forsikringsområdet og på transportområdet har krævet omfattende lovgivning på fællesskabsniveau.[87]

Persondata kan ikke defineres i forhold til fri bevægelighed for personer og herunder tjenesteydelser i henhold hertil, hvorfor fri bevægelighed i henhold hertil ikke finder anvendelse.

[85] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 187, 188 og 308): Det ikke-traktatfæstede princip om gensidig anerkendelse indebærer, at lovligt producerede varer i én medlemsstat, skal anerkendes i de andre medlemsstater, også selvom måden hvorpå varen er produceret, ikke er i overensstemmelse med de tekniske eller kvalitative krav, som der bliver stillet i det pågældende land, jf. Cassis de Dijon. Derudover sørger princippet også for, at der er en vis form for ligestilling for medlemsstaterne.
TEUF's artikel 34, som regulerer et forbud mod kvantitative indførselsrestriktioner, og dermed en hæmning af den fri bevægelighed for varer, er en del af den forpligtelse som alle EU-lande har, når de skal forfølge princippet om gensidig anerkendelse.

[86] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 424)

[87] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 423)

3.1.3. Den frie bevægelighed for kapital

Der er ikke nogen nærmere angivelse af, hvad der menes med kapitalbevægelser i EUF-Traktaten, men gælder ifølge Leo Flynn, at *capital movements cover, in essence, those resources used for, or capable of, investment intended to generate revenue. This term covers cash, bonds and other debt instruments, shares and so on.*[88]

I Romtraktaten var den frie bevægelighed for kapital begrænset til, hvad der skønnedes nødvendigt for "fællesmarkedets funktion". Den frie bevægelighed gjaldt kun for kapitalbevægelser mellem medlemslandene. For kapitalbevægelser til og fra tredjelande var målet "den størst mulige" liberalisering.[89]
Først ved beslutningen i 1988, med ikrafttrædelse 1.7.1990, om det indre marked opnåedes der enighed om at indføre helt frie kapitalbevægelser. Herved kom også de kortfristede bevægelser med i liberaliseringen, eksempelvis indskud i banker, samt finanskreditter. Direktivet fastslog desuden princippet om ligelig behandling af kapitalbevægelser internt i det indre marked, samt mellem medlemslande og tredjelande. Disse principper blev traktatfæstet i EF-Traktatens afsnit III om den frie bevægelighed for personer, tjenesteydelser og kapital som en afgørende forudsætning for gennemførelsen af Den Økonomiske og Monetære Union.[90] Mens der eksisterer et absolut forbud mod restriktioner for de indre bevægelser, kan visse eksisterende begrænsninger opretholdes i forhold til tredjelande.[91]

Det må hertil udledes, at persondata ikke kan defineres som kapital i henhold til at persondata hverken kan defineres som kontanter, obligationer, eller andre gældsinstrumenter, aktiver og lignende, hvorfor persondatas fri bevægelighed ikke kan henledes til kapitalbevægelser.

---

[88] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 559): Flynn, Leo: Coming of Age: The Free Movement of Capital Case Law 1993-2002, Common Market Law Review 2002 s. 776
[89] Europa-Parlamentets Faktablade om Den Europæiske Union, nærmere om Frie kapitalbevægelser: http://www.europarl.europa.eu/atyourservice/da/displayFtu.html?ftuId=FTU_2.1.3.html
[90] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 559-560)
[91] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 559-560)

3.2. Nærmere om etableringsfrihed og fri udveksling af tjenesteydelser

Definitionen om *tjenesteyder* beskriver enhver fysisk person eller enhver juridisk person i en Medlemsstat, jf. TEUF art. 54, der udbyder eller udfører en tjenesteydelse for en *tjenestemodtager* der beskrives som værende enhver fysisk person eller enhver juridisk person i en Medlemsstat, jf. TEUF art. 54 i erhvervsøjemed eller andet øjemed ønsker at anvende en tjenesteydelse.[92]

3.2.1. Tjenesteydelsesdirektivet — hen imod færdiggørelsen af det indre marked

I 2006 blev Tjenesteydelsesdirektivet[93], som styrker friheden til at levere tjenesteydelser inden for EU, vedtaget med gennemførelsesfrist den 28. december 2009. Direktivet er afgørende for færdiggørelsen af det indre marked, idet det indeholder muligheder for at skabe fordele for forbrugerne og SMV'er[94]. Formålet er således at skabe et åbent indre marked for tjenesteydelser i EU og samtidig sikre kvaliteten af de tjenesteydelser, der leveres til forbrugerne i Unionen.[95]

I henhold til service-direktivets[96] artikel 4, stk. 1, nr. 1 forstås "tjenesteydelse", som "*enhver selvstændig erhvervsvirksomhed, der normalt udføres mod betaling, jf. traktatens artikel 50*". Det er en forudsætning for at TEUF art. 56, kan anvendes, at der er tale om grænseoverskridende udveksling af tjenesteydelser. Det betyder at rent interne forhold ikke kan nyde beskyttelse af fri bevægelighedsreglerne. Det skal være et grænseoverskridende element og medlemsstatsbegrebet fortolkes bredt. Dette betyder konkret, at alle offentlige myndigheder på alle niveauer omfattes af begrebet.

Som tjenesteydelser i TEUF art. 57 betragtes ydelser som normalt udføres mod betaling og i det omfang de ikke omfattes af bestemmelserne vedrørende den frie bevægelighed for varer, kapital, samt personer.

---

[92] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 486)
[93] Direktiv 2006/123/EF
[94] Direktivets definition af SMV, Direktiv 2006/123/EF
[95] Direktiv 2006/123/EF, pr. 1.
[96] Direktiv 2006.123.EF af 12. december 2006 om tjenesteydelser i det indre marked

I henhold til traktatens artikel 14, stk. 2, *indebærer det indre marked et område uden indre grænser med fri bevægelighed for tjenesteydelser.* Dette betyder, at en EU-borger som forbruger i medlemsstaterne kan frit vælge service ligegyldigt hvilken medlemsstat ydelsen kommer fra.

Jf. direktivets artikel 2 stk. 2 er der oplistet en negativ liste under anvendelsesområde, der fastslår, hvad der ikke kan betragtes som tjenesteydelser i henhold til direktivet. "Overførsel af persondata" er ikke med i listen, hvorfor det må udledes at "overførsel af persondata" som værende tjenesteydelse, jf. direktivets art. 2, stk. 2, modsætningsvist. Sammenholdt med ovenstående nærmere definition af tjenesteydelse, kan persondata henledes til høre ind under begrebet om tjenesteydelser, hvorfor endvidere, tjenesteydelsers fri bevægelighed har relevans i forhold hertil.

Som fastsat i traktaten om Den Europæiske Unions Funktionsmåde, samt understøttet af EU-Domstolens retspraksis, sikrer etableringsfriheden og den frie udveksling af tjenesteydelser fri bevægelighed for virksomheder og erhvervsdrivende i EU. Med henblik på den videre gennemførelse af disse to friheder er der høje forventninger til tjenesteydelsesdirektivet fra 2006[97], eftersom dette direktiv har afgørende betydning for færdiggørelsen af det indre marked.

Retsgrundlaget for etableringsfrihed og fri udveksling af tjenesteydelser forefindes i traktaten om Den Europæiske Unions Funktionsmåde artikel 26, om det indre marked, artikel 49-55, om etableringsretten og artikel 56-62 om tjenesteydelser.

Målet er således, at selvstændige, erhvervsdrivende eller juridiske personer, som omhandlet i TEUF artikel 54, som driver lovlig virksomhed i én medlemsstat, kan drive økonomisk virksomhed på stabil og kontinuerlig vis i en anden medlemsstat[98], eller tilbyde deres tjenester i en anden medlemsstat, samtidig med at de forbliver i deres

[97] Europa-Parlamentets og Rådets direktiv 2006/123/EF, af 12. december 2006, om *tjenesteydelser i det indre marked*
[98] Etableringsfriheden i TEUF artikel 49

oprindelsesland[99]. Dette indebærer eliminering af forskelsbehandling på grund af nationalitet og, hvis disse friheder skal anvendes effektivt, vedtagelse af foranstaltninger med henblik på at gøre det lettere at udøve dem, herunder harmonisering af nationale adgangsregler eller gensidig anerkendelse.[100]

Etableringsretten indebærer adgang til at optage og udøve selvstændig erhvervsvirksomhed, samt retten til at oprette og lede virksomheder med en permanent aktivitet af stabil og kontinuerlig art på de vilkår, som i etableringslandets lovgivning er fastsat for landets egne borgere.[101]

Det kan således udledes, at fri udveksling af tjenesteydelser gælder for alle de ydelser, herunder persondata, der normalt udføres mod betaling, for så vidt de ikke er omfattet af bestemmelserne vedrørende den frie bevægelighed for varer, kapital og personer. Med henblik på at yde en sådan tjenesteydelse, kan en tjenesteyder midlertidigt udøve sin virksomhed i den medlemsstat, hvor ydelsen præsteres, på samme vilkår, som den pågældende medlemsstat har fastsat for sine egne statsborgere, jf. TEUF art. 54.[102]

4. EU's internationale forhold – Verdenshandelsorganisationen

Beskyttelse af personoplysninger er et behov der ikke blot søges dækket på EU's områder, men er ligeledes et behov der søges dækket på global plan.[103] Forbrugere i hele verden sætter i stigende grad pris på deres privatliv, hvorfor lande og regionale organisationer vidt omkring i verden ligeledes vedtager nye eller ajourførte eksisterende databeskyttelsesregler. Dette er med særligt henblik på, at udnytte de muligheder, der knytter sig til den globale digitale økonomi, og dermed imødegår den voksende

[99] Fri udveksling af tjenesteydelser i TEUF artikel 56
[100] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 499)
[101] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 499-505)
[102] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 509)
[103] COM(2017) 7 final (s. 2)

efterspørgsel efter en stærkere beskyttelse af data og privatlivets fred.[104] Dette er uanset om det er i kommercielt øjemed eller med henblik på samarbejde mellem offentlige myndigheder.[105] Til trods for, at der er forskelle mellem landene med hensyn til deres tilgang og lovgivningsmæssige udvikling, så er der, som Kommissionen meddeler til Europa-Parlamentet og Rådet i COM(2017) 7 final, *"tegn på større konvergens i retning af vigtige databeskyttelsesprincipper"*[106], og udtaler endvidere, at EU dermed bør gribe muligheden for at fremme sine databeskyttelsesværdier, for at fremme datastrømme ved at tilskynde til konvergens mellem retssystemer.

I henhold til EU-retten kan personoplysninger blandt andet overføres til andre lande på grundlag af Kommissionens afgørelse om *tilstrækkeligheden af beskyttelsesniveauet*. Ved en sådan afgørelse kan Kommissionen således fastslå, at et tredjeland sikrer et databeskyttelsesniveau, *som i det væsentlige svarer*[107] til det, der sikres i EU.

Reformen fra Direktivet til Forordningen formaliserer og øger mulighederne for at anvende eksisterende instrumenter, såsom standardkontraktbestemmelser[108] og bindende virksomhedsregler[109].[110] Standardkontraktbestemmelserne kan inkluderes i en kontrakt mellem EU-baserede databehandlere og databehandlere i et tredjeland, jf. forordningens artikel 46, stk. 2, litra c) og d), sammenholdt med 168. præambel i forordningen, men dette forhold vil dog ikke uddybes yderligere.

[104] COM(2017) 7 final (s. 2)
[105] COM(2017) 7 final (s. 2)
[106] Jf. UNCTAD: "Data protection regulations and international data flows: Implications for trade and development"
[107] Domstolens dom af 6. oktober 2015 i sag C-362/14, Schrems-sagen, præmis 73, 74 og 96 sammenholdt med forordningens 104. præambel
[108] I standardkontraktbestemmelserne fastlægges EU-eksportørens og det importerende tredjelands databeskyttelsesforpligtelser
[109] Bindende virksomhedsregler er interne regler vedtaget af en multinational concern vedrørende videregivelse af oplysninger inden for samme koncern til enheder beliggende i lande, som ikke sikrer et tilstrækkeligt beskyttelsesniveau. Direktivet indeholder allerede bestemmelser om bindende virksomhedsregler, men disse kodificeres og deres rolle som et redskab til videregivelse af oplysninger formaliseres i Forordningen
[110] COM(2017) 7 final (s. 5)

I henhold til forordningens ikrafttrædelse indføres nye instrumenter vedrørende internationale overførsler, jf. forordningens artikel 46, stk. 2, litra e) og f), navnlig godkendte adfærdskodeks, henholdsvis godkendte certificeringsmekanismer. Dataansvarlige og databehandlere får således mulighed for at anvende godkendte certificeringsmekanismer eller adfærdskodekser, som for eksempel privatlivsmærkninger eller -mærker, på visse betingelser for at sikre "fornødne garantier". [111] Ingen dataansvarlige uden for EU vil kunne overholde en EU-adfærdskodeks eller certificeringsmekanisme ved gennem kontrakter eller andre retligt bindende instrumenter, at afgive bindende tilsagn, som kan håndhæves, om at anvende databeskyttelsesgarantierne i disse instrumenter, jf. forordningens artikel 42, stk. 2.[112] Altså burde dette gøre det muligt, at udvikle skræddersyede løsninger vedrørende internationale overførsler, ved at de afspejler en specifik sektors eller industris, eller specifikke datastrømmes særlige karakter. Det gør det ligeledes muligt at sikre de "fornødne garantier" for overførsel af oplysninger mellem offentlige myndigheder eller organer på grundlag af internationale aftaler eller administrative ordninger, jf. forordningens artikel 46, stk. 2, litra a) og artikel 46, stk. 3, litra b).

I forordningens artikel 49 præciseres anvendelsen af de såkaldte *undtagelser*, altså et samtykke, opfyldelse af en kontrakt eller vigtige samfundsinteresser, som enheder i specifikke situationer kan basere deres dataoverførsler på, hvis der ikke er vedtaget en afgørelse om tilstrækkeligheden af beskyttelsesniveauet.[113] Dette er uanset om et af ovennævnte instrumenter er anvendt. Ligeledes indeholder forordningens artikel 49, stk. 1, andet afsnit en ny, om end begrænset undtagelse om overførsler, der kan foretages i forbindelse med en virksomheds forfølgelse af legitime interesser.[114]
Endelig er det anerkendt, at et tættere samarbejde mellem myndighederne på international plan både kan sikre en mere effektiv beskyttelse af den enkeltes rettigheder og større retssikkerhed for virksomheder, hvor forordningens artikel 50, om *internationalt samarbejde om beskyttelse af personoplysninger*, tillægger Kommissionen beføjelser til

[111] COM(2017) 7 final (s. 5)
[112] COM(2017) 7 final (s. 5)
[113] COM(2017) 7 final (s. 5)
[114] COM(2017) 7 final (s. 5)

at udvikle mekanismer for internationalt samarbejde for at lette håndhævelsen af databeskyttelsesreglerne, herunder ordninger for gensidig bistand.[115]

Kommissionen har statueret i sin meddelelse[116] til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg, og Regionsudvalget, at til trods for, at privatlivets fred ikke er en handelsvare, så gøres det til genstand i den forstand, at beskyttelse af privatlivets fred er en forudsætning for stabile, sikre og konkurrencedygtige globale handelsstrømme, i og med, at internettet og digitaliseringen af varer og tjenesteydelser har ændret den globale økonomi, samt grænseoverskridende overførsel af oplysninger, herunder personoplysninger.[117] Dette skal ses i lyset af, at samhandel i stigende grad afhænger af udveksling af personoplysninger, hvorfor de gøres til genstand som et led i de europæiske virksomheders daglige drift, og endvidere har gjort, at beskyttelsen af privatlivets fred og datasikkerheden er blevet en central faktor i forbrugertilliden.[118]

I et samfund der er så digitaliseret og globaliseret[119], må målet om at fremme høje databeskyttelsesstandarder nødvendigvis følges ad med målet om at fremme international handel, og til trods for, at beskyttelsen af personoplysninger ikke er til forhandling i handelsaftaler, så er EU-systemet for international videregivelse af oplysninger, jf. ovenfor, beskrevet som en bred og varieret værktøjskasse, der gør det muligt, at videregive oplysninger i forskellige situationer, i overensstemmelse med at der tilsigtes at sikre et højt beskyttelsesniveau.[120]

4.1. EU og Verdenshandelsorganisationen

4.1.1. Forskellen mellem EU og Verdenshandelsorganisationen

[115] COM(2017) 7 final (s. 6)
[116] Meddelelse fra Kommissionen om *Handel for alle – En mere ansvarlig handels- og investeringspolitik*, COM(2015) 497 final af 14.10.2015 (s. 7)
[117] COM(2017) 7 final (s. 6)
[118] COM(2017) 7 final (s. 6)
[119] Forordningens 6. præambel
[120] COM(2017) 7 final (s. 6)

Ifølge Verdenshandelsorganisationens egen forståelse, så har organisationen opnået succes ved at skabe et fællesskab af nationaliteter med en fælles vision om at opnå international liberalisering inden for handel.[121] Fællesskabet bygger kun på aftaler som nationerne tiltræder og de derefter er forpligtet af. EU er derimod opbygget således, at det efterhånden er blevet ét overnationalt politisk system, som styrer liberaliseringen af handel inden for *det indre marked*. EU er således opbygget for det første af medlemsstaterne der i flere sammenhænge har afgivet suverænitet, og for det andet af institutioner med hver deres kompetence, der er lovfæstet i TEUF (institutionelt struktureret).

Forholdet imellem EU, medlemsstaterne i EU og WTO består i, at EU i sig selv er én nation der er medlem af WTO, og hver EU-medlemsstat hver især uafhængige nationer, der deltager i fællesskabet inden for WTO gennem EU. Dette skal forstås sådan, at medlemsstaterne i EU, opretholder hver deres autonomi og suveræne kontrol over essentielle elementer inden for økonomisk, finans- og socialpolitik inden for WTO.

4.1.2. Harmonisering

Begrebet *harmonisering* er en vigtig del af forståelsen for hvordan forholdet imellem to store systemer som WTO og EU er opbygget. Inden for EU anvendes *harmonisering* i forhold til lovgivning, hvor medlemsstaterne har pligt til at harmonisere initiativer igennem direktiver og forordninger. Direktiver tilstræber at bringe medlemsstaternes lovgivning i indbyrdes overensstemmelse, til forskel fra forordninger som har direkte virkning i samtlige EU-medlemsstater.

Harmonisering skal i forhold til Verdenshandelsorganisationen forstås mere bredt, og værdien af *harmonisering* kan enten være eksplicit eller implicit. Implicit harmonisering dækker de retlige områder, hvor der ikke er nogen udtrykkelig forpligtelse for en harmonisering, men hvor harmoniseringen alligevel kan give mening af andre grunde.[122] Ved eksplicit harmonisering, kræver organisationen, at nationernes lovgivning er i

[121] Sanford E. Gaines m.fl.; Liberalising trade in the EU and the WTO; edition 2014 (s. 9)
[122] Sanford E. Gaines m.fl.; Liberalising Trade in the EU and the WTO; edition 2014 (s. 11)

overensstemmelse med WTO-aftaler og fortolkningen af tvistbilæggelsesorganet.[123] WTO's autoritet til at binde EU juridisk gælder fx i områder for lovgivning inden for anti-dumping, sikkerhedsforanstaltninger, told og m.v. EU har således pligt til at overholde aftalerne i WTO. Hvis der opstår tvivl om fortolkning af ordlyden i retskilderne, f.eks. at der i en konkret situation bliver lagt sag an imellem WTO-medlemsnationer, så fortolker tvistbilæggelsesorganet ordlyden i den konkrete situation. Tvistbilæggelsesorganets kendelser vægtes derfor tungt i forståelsen af en retsstilling inden for WTO, og medlemsnationerne har pligt til at følge "their interpretation by the Dispute Settlement Body".[124]

For at forstå hvorfor EU er forpligtet til at udarbejde sin lovgivning i med hensyn til WTO-aftaler, redegøres der i dette afsnit for forholdet mellem WTO og EU.

4.1.3. EU's forpligtelser over for andre WTO-medlemmer - herunder overholdelse af GATS-aftale

I 1995 tiltrådte EU Verdenshandelsorganisationen, WTO, ved at underskrive en række WTO-aftaler, såsom aftalen om *General Agreement on Tariffs and Trade GATT*, samt *General Agreement on Trade in Services, GATS*. Visionen var at tage del i at fremme liberaliseringen i international handel, hvor Kommissionen er den eneste forhandler og talsmand for EU i organisationen.[125]

I Uruguay-runden, januar 1995, blev GATT transformeret og institutionaliseret som *World Trade Organisation*, WTO, da udviklingen af den internationale handel havde bevæget sig ud over materielle goder og ind i udveksling af ydelser. Verdenshandelsorganisationen integrerede GATT med de tidligere handelsaftaler om

[123] Sanford E. Gaines m.fl.; Liberalising Trade in the EU and the WTO; edition 2014 (s. 11)
[124] Citat fra Sanford E. Gaines m.fl.; Liberalising Trade in the EU and the WTO; edition 2014 (s. 11)
[125] I 1947 blev den internationale handelsaftale GATT, underskrevet af 23 lande med ikrafttrædelse 1. januar 1948. Sammen med Den internationale Valutafond og Verdensbanken, blev GATT oprettet i efterkrigstiden for at hjælpe med at regulere den internationale økonomi. Dette skulle gøres ved liberalisering af international handel med varer, for at forebygge *protektionistiske politikker*, hvormed der forhandledes reduktion af toldbarrierer imellem medlemsnationerne.

bl.a. landbrug, tekstiler etc., og der blev yderligere etableret GATS om handel med serviceydelser.

Det er bemærkelsesværdigt, at GATS blev integreret i WTO's handelstraktater i 1995 samme år som EU's Databeskyttelsesdirektiv blev vedtaget. Dette udtrykker særligt at, i takt med globaliseringen, den teknologiske udvikling og handel med tjenesteydelser på globalt plan havde nået en højere status inden for lovgivning, i og med, at der ikke længere kun var lovgivning i forhold til handel med fysiske varer, men at handel med tjenesteydelser og rettigheder i forbindelse hertil, såsom privatlivets fred og behandling af persondata mv., fik yderligere essentiel betydning.

GATS blev inspireret af i det væsentlige de samme mål som sin modpart inden for handel med varer, den almindelige overenskomst om told og udenrigshandel, GATT: At skabe et troværdigt og pålideligt system for internationale handelsregler sikre fair og retfærdig behandling af alle deltagere (princippet om forbud mod forskelsbehandling) stimulere økonomisk aktivitet gennem garanterede politiske bindinger og fremme handel og udvikling gennem progressiv liberalisering. GATS anerkender udtrykkeligt medlemmernes ret til at regulere udbuddet af tjenesteydelser i overensstemmelse med deres egne politiske målsætninger og søger ikke at påvirke disse mål. Aftalen etablerer snarere en ramme for regler for at sikre, at tjenesteforordninger administreres på en rimelig, objektiv og upartisk måde og ikke udgør unødige handelshindringer.

I henhold til Databeskyttelsesforordningens præambel 101 lægges der vægt på, at udbygningen af den internationale samhandel og det internationale samarbejde findes nødvendigt, men at udvidelsen af datastrømme af personoplysninger skaber nye udfordringer, da *behandling af personoplysninger bør have til formål at tjene menneskeheden*, jf. for. pr. 4, hvor EU-borgerens grundlæggende rettigheder i henhold til Chartret, som udledt i forordningens 1. præambel, vægtes lige så højt. Målet er som udledt i forordningens 4. præambel, at finde en balance i henhold til proportionalitetsprincippet.

WTO spiller en vigtig rolle som en platform for verdens handelsnationer og der forhandles aftaler imellem medlemsstaterne om at opnå fælles regulering. WTO-

aftalernes regulering er skrevet meget bredt for at efterleve de mange medlemsnationer krav. Der lægges særlig vægt på de store medlemsnationer, som EU, U.S.A og Kina, der har størst indflydelse på hvordan aftalerne formes.

Databeskyttelsesforordningen udleder i sit femte kapitel, at EU's medlemsstater og virksomheder herunder mv., kun må overføre persondata til tredjelande med tilstrækkeligt beskyttelsesniveau, jf. for. art. 44. Begrebet *tilstrækkeligt beskyttelsesniveau* udledes i Politidirektivets artikel 36, der i sit stk. 2, der endvidere er fastsat i forordningens artikel 45, stk. 2, udleder betragtninger, som Kommissionen skal overholde ved afgørelse om et tredjelands beskyttelsesniveau. Ved vurderingen skal Kommissionen for det første betragte elementet om tredjelandets retsstatsprincip, i overensstemmelse med art. 6 EU som affattet ved Maastricht-traktaten bestemte, at Unionen bygger på principperne respekt for menneskerettighederne og de grundlæggende frihedsrettigheder, relevant lovgivning om personoplysninger og databeskyttelsesregler, de faglige regler om sikkerhedsforanstaltninger mv., der gælder i det konkrete tredjeland, samt dets retspraksis og de effektive rettigheder for registrerede, som kan håndhæves med effektiv administrativ- og retslig prøvelse for de registrerede, hvis personoplysninger overføres. For det andet skal Kommissionen betragte elementet om tilstedeværelsen af velfungerende uafhængige tilsynsmyndigheder i tredjelandet, samt tilgængeligheden for samarbejde mellem EU og tredjelandet. For det tredje skal Kommissionen betragte elementet om de internationale forpligtelser som tredjelandet har påtaget sig i forhold til beskyttelse af personoplysninger.

EU og USA har således indgået en aftale, EU-U.S. Privacy Shield, der således binder de to nationer i forhold til aftale om overførsel af persondata, sådan at forordningens artikel 45, stk. 2 i overensstemmelse med Politidirektivets artikel 36, stk. 2 overholdes jf. endvidere direktivets artikel 25, stk. 6 i Kommissionens gennemførelsesafgørelse (EU) 2016/1250.

I henhold til Alibaba-casen er det interessant at undersøge forholdet om, Alibaba Group, der har sæde i Kina. Persondata bliver da overført til datterselskabet i USA, således at lovligheden af overførsel opretholdes. Det er dog særligt interessant at få belyst forholdet

til moderselskabet som tilhørende til et *usikkert tredjeland*, Kina, jf. manglende oplistning over *sikre tredjelande* som udført af Kommissionen.[126]
EU har dog vurderet at Kinas beskyttelsesniveau ikke kan leve op til EU's niveau i henhold til Databeskyttelsesforordningen, jf. den manglende oplistning af Kina udført af Kommissionen.[127]

I henhold til artikel II i GATS er medlemmerne forpligtet til straks og betingelsesløst, at udvide tjenesteydelsesleverandører fra alle andre medlemmer - "*treatment no less favourable than that accorded to like services and services suppliers of any other country*". Dette indebærer principielt forbud mod præferenceordninger mellem grupper af medlemmer i individuelle sektorer eller gensidighedsbestemmelser, der begrænser adgangsfordele til handelspartnere, der yder tilsvarende behandling.
GATS art. 2.1 indeholder *mestbegunstigelsesprincippet*, som er et grundlæggende princip inden for WTO, der principielt minder om EU's princip om varers/tjenesteydelsers frie bevægelighed, hvorfor WTO-medlemsnationerne er forpligtiget behandle hinandens ens. Det indebærer, at WTO-medlemsnationer ikke må behandle tjenesteydelser fra andre medlemsnationer mere eller mindre gunstigt end tilsvarende tjenesteydelser med oprindelse i en anden medlemsnation.

Det udledes af Databeskyttelsesforordningens system at EU ensidigt beslutter om tilladte overførsler til bestemte lande. Her menes at EU ikke inddrager tredjelandet selv når beskyttelsesniveauet i henhold til forordningens artikel 45, stk. 2 bliver vurderet og gensidigt bestemmer den manglende tilstrækkelighed i landets beskyttelsesniveau. Som udgangspunkt leder dette således til, at Kommissionens beslutning på vegne af EU som WTO-medlemsstat, kan risikere at blive betragtet som en overtrædelse af mestbegunstigelsesprincippet under GATS art. 2, stk. 1, da andre WTO-medlemslande ikke automatisk får samme rettigheder til dataoverførsler som de lande, der er omfattet af Kommissionens beslutninger om tilstrækkelighed. Endvidere risikerer den måde, hvorpå forordningen anvendes på, at overtræde GATS art. 6, der bestemmer, at de nationale

[126] Det danske Datatilsynet har lagt Kommissionens liste ud på den danske hjemmeside, som der henføres til i afhandlingen: https://www.datatilsynet.dk/erhverv/tredjelande/sikre-tredjelande/
[127] https://www.datatilsynet.dk/erhverv/tredjelande/sikre-tredjelande/

regler finder anvendelse på en rimelig og objektiv måde for ikke at hindre handel med tjenesteydelser. Bevisbyrden vil så ligge på EU for at retfærdiggøre brugen af dette system under en af GATS-undtagelserne, generel under GATS art. 14, om national sikkerhed eller GATS art. 5 for regional integration. I afsnittet nedenfor vil vi fokusere på GATS art. 14.

GATS art. 14 giver et WTO-medlem mulighed for at anvende foranstaltninger i strid med mestbegunstigelsesprincippet, når de blandt andet er "nødvendige" for at opretholde offentlig orden (artikel 14, litra a)) eller "nødvendigt" for at sikre overholdelse af love eller forordninger, der ikke er WTO-inkonsekvente der vedrører beskyttelse af privatlivets fred for enkeltpersoner i forbindelse med behandling og formidling af personoplysninger (artikel 14, litra b), nr. ii)). Uanset om det er berettiget i henhold til disse bestemmelser, må foranstaltningerne ikke anvendes på en måde, der er "vilkårlig eller uberettiget" mellem lande, hvor "ligesom vilkår hersker", hvilket er en forudsætning for at begrunde en undtagelse i henhold til artikel 14.

Således kan det konstateres at ved at alle tredjelande uden for EU- og EØS-samarbejdet i henhold til forordningens art. 45 skal vurderes i henhold til dennes stk. 2, så forskelsbehandler EU ikke tredjelande, da Kommissionen har pligt til at vurdere beskyttelsesniveauets tilstrækkelighed hos de enkelte tredjelande uden for EU- og EØS-samarbejdet. Kommissionens vurdering ved det enkelte tredjeland stemmer endvidere overens med undtagelsesreglen i GATS art. 14, der således giver EU hjemmel til at anvende foranstaltninger, der kan have konsekvens i en forskelsbehandling imellem *tredjelandene*, da de begrundes lovligt i henhold til offentlig orden, navnlig beskyttelsen af EU-borgeres grundlæggende rettigheder, herunder beskyttelsen af personoplysninger.

Ved at Alibaba Groups datterselskab Alibaba.com og Alibaba Cloud har tiltrådt aftalen i henhold til EU-U.S. Privacy Shield, jf. endvidere Kommissionens (EU) 2016/1250, kan Alibaba således opretholde lovligheden i overførsel af persondata fra EU til USA.[128] Så

[128] På Privacy Shield websiden er Alibaba.com og Alibaba Cloud oplistet som værende tiltrådt EU-USA aftalen, således at overførsler landene imellem er på lovligt grundlag: https://www.privacyshield.gov/participant_search

længe de europæiske datterselskaber i henhold til Kinas manglende oplistning som værende et *sikkert tredjeland*, findes det ulovligt for disse datterselskaber, at overføre EU-borgeres personoplysninger til Alibaba Group i Kina. Lovligheden opretholdes dog ved overførsel til afdelingen i USA gennem EU-U.S. Privacy Shield.

5. Databeskyttelsesforordningens ikrafttrædelse

Beskyttelsen af personoplysninger indgår i Unionens fælles konstitutionelle opbygning og er forankret i chartrets artikel 8. Beskyttelsen har således været et centralt aspekt i EU-retten i over 20 år lige fra Databeskyttelsesdirektivet i 1995 til vedtagelsen af Databeskyttelsesforordningen i 2016.
Databeskyttelsesforordningens anvendelsesområde, som følge af forordningens artikel 2 om det materielle anvendelsesområde og artikel 3 om det territoriale anvendelsesområde, svarer i vidt omfang til direktivets anvendelsesområde i direktivets artikel 3.

5.1. Forordningens generelle principper

De generelle principper der er udledt af direktivets artikel 2 er begreberne *personoplysninger, behandling af personoplysninger, register med personoplysninger, den registeransvarlige, registerfører, tredjemand, modtager* og *den registreredes samtykke.*

Begrebet *personoplysninger* er i henhold til direktivet enhver form for information der identificerer en fysisk person eller om en identificerbar fysisk person, altså en registrerede. Identificerbar person skal endvidere forstås som en person, der direkte eller indirekte kan identificeres, enten ved identifikationsnummer eller et eller flere elementer der er særlige for en given persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet, jf. art. 2, litra a).

Da begrebet *personoplysninger* kan forstås bredt, anvendes det danske Datatilsynet til at uddybe begrebets omfang. Det vejledes således på Datatilsynets hjemmeside, at oplysninger der endvidere er omfattet af begrebet personoplysninger som kan henføres til en fysisk person, uanset om dette forudsætter kendskab til personnummer,

registreringsnummer eller lignende særlige identifikationer, som for eksempel løbenummer.[129] Ligeledes vil oplysninger i form af billede, persons stemme, fingeraftryk eller genetiske kendetegn være omfattet af begrebet. Oplysninger der endvidere er omfattet af begrebet personoplysninger, er eksempelvis løbenumre, medlemsnummer eller journalnummer der er etableret i forbindelse med en behandling. Således er det uden betydning om identifikationsoplysningen er alment kendt eller umiddelbart tilgængelig, også i de tilfælde hvor det kun for den indviede vil være muligt at forstå, hvem en oplysning vedrører. Hvis et navn eller adresse er erstattet af en kode, der kan føres tilbage til den oprindelige individuelle personoplysning, eller er der tale om krypterede oplysninger, vil både koden og de krypterede oplysninger også være omfattet af definitionen. Hvis oplysningerne derimod er anonymiserede sådan, at den registrerede ikke længere kan identificeres, vil de ikke længere være omfattet af definitionen.[130]

For at afgøre om en person er identificerbar, skal samtlige hjælpemidler der med rimelighed kan tænkes at være anvendt til at nå frem til identifikationen, enten af den dataansvarlige eller af enhver tredjemand, tages i betragtning.[131]
Ud af begrebet *behandling af personoplysninger* skal *behandling* forstås bredt. Det omfatter ”*enhver operation eller en række af operationer med eller uden brug af elektroniske databehandling, som oplysninger gøres til genstand for”*, jf. art. 2, litra b. Enhver form for håndtering af oplysninger er således omfattet. Som eksempel kan nævnes registrering, opbevaring, samt enhver form videregivelse af oplysninger, og enhver form for indsamling.[132]

Et register med personoplysninger er i henhold til direktivets artikel 2, litra c, enhver struktureret samling af personoplysninger, der er tilgængelige efter bestemte kriterier, hvad enten denne samling er placeret centralt, decentralt eller er fordelt på et funktionsbestemt eller geografisk grundlag. Således vejleder Datatilsynet, at enhver form for manuelle registre, som for eksempel fortegnelser, journalkortsystemer, men derimod vil manuelle akter som indgår i den dataansvarliges konkrete

[129] Datatilsynet: Ordbog: Personoplysninger: https://www.datatilsynet.dk/ordbog/
[130] Datatilsynet: Ordbog: Personoplysninger: https://www.datatilsynet.dk/ordbog/
[131] Datatilsynet: Ordbog: Personoplysninger: https://www.datatilsynet.dk/ordbog/
[132] Datatilsynet: Ordbog: Behandling: https://www.datatilsynet.dk/ordbog/

Når man som virksomhed beskæftiger sig med behandling af personoplysninger, eksempelvis ved indsamling, registrering og videregivelse, er det vigtigt for virksomheden, at afklare, om man er *dataansvarlig*, altså registeransvarlig, jf. dir. art. 2, litra d), eller *databehandler*, altså registerfører, jf. dir. art. 2, litra e), i forbindelse med behandlingen. Det er som udgangspunkt den dataansvarlige, der er ansvarlig for overholdelsen af de nationale love i henhold til Databeskyttelsesdirektivet, og den dataansvarlige har endvidere pligt til at anmelde visse behandlinger af personoplysninger til de nationale datatilsyn, og endvidere er det den dataansvarlige, over for hvem en registreret kan udøve sine rettigheder efter de nationale love, eksempelvis den danske Persondatalov, herunder sin indsigelsesret, og retten til at få berigtiget urigtige oplysninger, mv.

Af definitionen af *den registeransvarlige* følger det, at der godt kan være flere dataansvarlige i forbindelse med en behandling af personoplysninger, således at der opstår *delt ansvar*.[133] Det danske datatilsyn har således i enkelte meget konkret begrundede sager accepteret et delt dataansvar, men der vil som udgangspunkt normalt kun være én dataansvarlig i forbindelse med en given behandling af personoplysninger.

Hvis man som dataansvarlig benytter sig af en databehandler, følger det som eksempelvis af dansk national lovgivning, at man skal indgå en skriftlig aftale herom med databehandleren, altså en såkaldt databehandleraftale.[134]

En databehandler, altså registerfører i henhold til direktivets artikel 2, litra e), kendetegnes ved kun at behandle personoplysninger på vegne af, efter instruks fra, en dataansvarlig. Databehandleren behandler altså ikke personoplysninger til egne formål,

[133] Datatilsynet: Vejledning: Hvornår er man henholdsvis dataansvarlig og databehandler?: https://www.datatilsynet.dk/erhverv/dataansvarlig-databehandler/hvornaar-er-man-henholdsvis-dataansvarlig-og-databehandler/
[134] Datatilsynet: Vejledning: Hvornår er man henholdsvis dataansvarlig og databehandler?: https://www.datatilsynet.dk/erhverv/dataansvarlig-databehandler/hvornaar-er-man-henholdsvis-dataansvarlig-og-databehandler/

hvorfor denne ikke må bruge de overladte oplysninger til andet end udførelsen af opgaven for den dataansvarlige.

I praksis kan en databehandler eksempelvis være en virksomhed, som varetager en anden virksomhed eller en myndigheds IT-systemer.[135]

I henhold til Datatilsynets vejledning, skal et tredjeland forstås som et land, der ikke indgår i Den Europæiske Union. Dog bliver en stat ikke betragtet som et tredjeland, hvis den pågældende stat har gennemført en aftale med Den Europæiske Union, og som indeholder love og regler svarende til persondatadirektivet (dir. 95/46/EF).[136]

Den registreredes samtykke kan i henhold til direktivet forstås bredt, hvorfor dette område analyseres yderligere i henhold til den danske Persondatalov[137] med vejledning fra det danske Datatilsyn.[138]

Behandling af almindelige personoplysninger må ske, hvis den registrerede har givet sit udtrykkelige samtykke. Kravet om udtrykkelighed betyder, at et stiltiende eller indirekte samtykke ikke er tilstrækkeligt.

Hvis behandlingen er nødvendig for at kunne opfylde en aftale som den registrerede er part i, kan behandling af almindelige personoplysninger finde sted. Det kan eksempelvis være nødvendigt at registrere og behandle oplysninger, der fremgår af ordrer, fakturaer og lignende i tilknytning til aftaler, hvor den registrerede er aftalepart.

Hvis behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige. En retlig forpligtelse kan eksempelvis være en forpligtelse, der er fastsat i en lov eller en bekendtgørelse

---

[135] Datatilsynet: Vejledning: Hvornår er man henholdsvis dataansvarlig og databehandler?: https://www.datatilsynet.dk/erhverv/dataansvarlig-databehandler/hvornaar-er-man-henholdsvis-dataansvarlig-og-databehandler/

[136] Datatilsynet: Ordbog: Tredjeland: https://www.datatilsynet.dk/ordbog/

[137] Lov nr. 429 af 31/05/2000 Gældende

[138] Datatilsynet: Persondataloven – Hvilke oplysninger må registreres? Hvad må oplysningerne bruges til? Hvordan kontrollerer du oplysningerne?

I henhold til direktivets artikel 3, stk. 1, anvendes direktivets bestemmelser på behandling af personoplysninger, der helt eller delvist foretages ved hjælp af edb, samt på ikke-elektronisk behandling af personoplysninger, der er, eller vil blive indeholdt i et register.

Begreberne personoplysning, behandling og register defineres i direktivets artikel 2, litra a), litra b) og litra c).

I henhold til direktivets artikel 3, stk. 2, 2. pind udledes det, at direktivet ikke gælder for behandling af personoplysninger, som foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter. Disse er nærmere uddybet i direktivets 12. præambel, hvori det anføres, at dette for eksempel er føring af adressefortegnelser, og hvorfor artiklen således ikke finder anvendelse i forhold til afhandlingens problemstilling.

5.2. Forpligtelser ved behandling - behandlingsprincipperne

Når Alibaba.com behandler personoplysninger er der en række forpligtelser som virksomheden skal iagttage, uanset om oplysningerne behandles inden for EU's rammer og endvidere overføres til USA.

Begrebet *behandling* omfatter enhver form for håndtering af personoplysninger, navnlig elektronisk behandling af oplysninger, der er omfattet af reglerne. Behandling kan således være indsamling, registrering, systematisering, opbevaring, søgning, brug og videregivelse, eller sletning af oplysninger.

Forordningen indeholder en række principper i sit kapitel II, som skal følges, hvis en virksomhed, altså den dataansvarlige i henhold til forordningens definition i artikel 4, litra 7) om *dataansvarlig*, ønsker at *behandle personoplysninger* i henhold til forordningens definition i artikel 4, litra 1) og 2). De generelle principper inkluderer blandt andet, at personoplysningerne skal behandles lovligt, for eksempel med samtykke, fair, transparent, og at oplysningerne kun må behandles til et specifikt, eksplicit og legitimt

formål. Ydermere må der ikke behandles flere oplysninger end nødvendigt, og ligeledes skal oplysningerne være korrekte og opdaterede. Oplysningerne må ikke lagres længere end nødvendigt og oplysninger skal desuden beskyttes gennem sikkerhedsforanstaltninger, der iværksættes efter en risikovurdering.

Når Alibaba koncernen overfører EU-borgeres personoplysninger til USA, skal koncernen således være opmærksom på, at det i så fald ikke er nok at overholde behandlingsreglerne i forordningens kapitel II, da de særlige regler om overførsel af personoplysninger til tredjelande udledes i forordningens kapitel V, ligeledes skal iagttages. Forholdet om overførsel til tredjelande vil da blive nærmere behandlet i afhandlingens kapitel 7.

I henhold til principperne bør Alibaba Group, navnlig datterselskabet Alibaba.com, som virksomhedskoncern være opmærksom på hvilke behandlinger denne ønsker at foretage, da det som udgangspunkt er virksomheden som er den *dataansvarlige*, jf. for. art. 4, litra 7). Alibaba behandler personoplysninger, som i overensstemmelse med forordningens artikel 2, stk. 1, nærmere om behandling af personoplysninger, der foretages ved hjælp af automatisk behandling.

Endvidere bør Alibaba undersøge, hvorvidt den opfylder principperne for behandling af oplysningerne, da det kan have konsekvenser for virksomheden ved manglende opmærksomhed. Endvidere må Alibaba undersøge, hvorvidt behandlingen af personoplysningerne er nødvendig, altså er der proportionalitet? I forlængelse hermed opstår spørgsmålet om hvorvidt virksomheden kan behandle oplysningerne på en mindre indgribende måde og stadig opnå formålet?

Alibaba.com overholder sin iagttagelse af proportionaliteten i og med, at virksomheden blot indsamler navn, telefon, e-mail, adresse og adresse i henhold til forordningens definition af personoplysninger i artikel 4, litra a), når en EU-borger opretter profilbruger på websiden Alibaba.com. EU-borgeren skal ikke informere oplysninger, der i henhold til forordningens artikel 9 kan kategoriseres som behandling af særlige kategorier af

personoplysninger, herunder oplysninger om EU-borgerens race eller etniske oprindelse, politiske- eller religiøse holdninger, filosofiske overbevisning eller seksuelle forhold mv.

Alibaba har i henhold til principperne om lovlighed, rimelighed og gennemsigtighed pligt til at give den registrerede lettilgængelig information om behandlingen af oplysningerne, jf. for. art. 5, stk. 1, litra a). Dette indebærer blandt andet, at den registrerede som udgangspunkt skal have oplyst, *hvem* der er ansvarlig for behandlingen af oplysningerne, og hvad der er formålet med behandlingen. Det udtrykkes endvidere i forordningens 39. præambel, at princippet om gennemsigtighed netop tilsiger, *at enhver information og kommunikation vedrørende behandling af disse personoplysninger er lettilgængelig og letforståelig*, altså for den registrerede, og i forlængelse hertil, at den registrerede gøres bekendt med de risici, regler, garantier og rettigheder ved behandlingen af personoplysningerne, ved et klart og enkelt sprog. Hensigten heraf er således at tilsigte den registrerede forstår hvordan og hvorledes denne skal udøve sine rettigheder i forbindelse med en sådan behandling.

I forordningens 40. præambel udtrykkes det nærmere i forhold til en behandlings lovlighed, at personoplysninger bør behandles på grundlag af den registreredes samtykke, eller et andet legitimt grundlag, der er fastlagt ved lov. Når en EU-borger således opretter en brugerprofil på Alibaba.com websiden og giver sit samtykke hertil ved at trykke ”godkend” og ”gem”, vil Alibaba.com således opfylde sin pligt overensstemmende med forordningens artikel 5, stk. 1, litra a) i henhold til *lovlighed.*

Hertil skal Alibaba.com som dataansvarlig kunne påvise, at deres behandlinger er baseret på den registreredes samtykke, som nærmere udtrykket i forordningens 42. præambel, at den dataansvarlige således bør stille en samtykkeerklæring til rådighed som er udformet af eksempelvis Alibaba.com, jf. endvidere forordningens artikel 7, hvor forholdet om den dataansvarliges oplysningspligt uddybes nærmere i afhandlingens kapitel 8.1.

Virksomheder som Alibaba.com bør gøre det sig klart, hvilke formål oplysningerne indsamles til, navnlig saglige formål, når der indsamles oplysninger. I den situation, hvor den registreret har oprettet en brugerprofil på Alibaba.com websiden, og dermed selv lægger oplysninger op om sig selv, navnlig oplysninger om navn, opfyldes

tilvejebringelsen i henhold til proportionalitet, da oplysningerne om navn, adresse og e-mail-adresse indsamles til oprettelse af profil-bruger og endvidere profileres på brugeren i forhold til brugerens tidligere søgninger, mv.

5.3. Direktivets artikel 25 og Forordningens artikel 44

Direktivet og Forordningen indeholder hver et kapitel der handler om videregivelse af personoplysninger til lande uden for EU- og EØS-samarbejdet. Det er essentielt at undersøge hvorvidt betydningen i netop dét kapitel vil ændre sig i overgangen fra at være lovgivning i direktivet til at være lovgivning i forordningen.

Det essentielle skal ses i lyset af, at der inden for EU-retten er principperne om subsidiaritet og proportionalitet, som styrer EU's kompetence i forhold til national ret.

Princippet om subsidiaritet betyder, også kaldet nærhedsprincippet, at EU kun kan lovgive på de områder, hvor det ikke vil være tilstrækkeligt effektivt, at medlemsstaterne lovgiver individuelt. Altså skal EU kun lovgive, hvor det er nødvendigt. Spørgsmålet er således, om EU har overholdt subsidiaritetsprincippet i forhold til vedtagelsen af Databeskyttelsesforordningen. I henhold til at hensigten med forordningens ikrafttrædelse er at skabe konvergens imellem medlemsstaternes lovgivning på databeskyttelses-området, jf. forordningens pr. 2, og i overensstemmelse formålsfortolkningen i henhold til Chartrets artikel 8, stk. 1, har EU-lovgivernes således overholdt subsidiaritetsprincippet.
Det skal da bemærkes, at ud over at en forordning som udgangspunkt ikke må gennemføres i medlemsstaterne, vil medlemsstaternes modstridende lovgivning blive fortrængt af en forordning, hvorfor det vil være nødvendigt at ophæve denne lovgivning således, at der ikke opstår nogen usikkerhed om retstilstanden. Ophævelsen skal ske enten ved lov eller ved bekendtgørelse med hjemmel i lov.

På nuværende tidspunkt, hvor afhandlingen skrives, er det Databeskyttelsesdirektivets virkning, der er i kraft. Databeskyttelsesdirektivet er som for andre direktiver, et direktiv der er bindende for enhver medlemsstat, med det formål, at beskytte EU-borgernes

grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, jf. dir. art. 1, stk. 1, hvor det således er op til de enkelte medlemsstater, at lave deres egne love for, hvordan disse mål skal opnås.[139]

Databeskyttelsesforordningen vil da træde i kraft den 25. maj 2018. Forskellen fra et direktiv til en forordning har essentiel betydning, da en forordning, i forhold til et direktiv, er almengyldig, og endvidere, at der er tale om en egentlig afgivelse af suverænitet fra medlemsstaterne til EU. [140] Et direktiv er ikke almengyldig, jf. kapitel 1. Databeskyttelsesforordningen vil således være umiddelbart gældende i EU's medlemslande, således at retsvirkningen af forordningen indtræder uden national indarbejdelse, altså implementering, som det i sin tid krævede ved Databeskyttelsesdirektivets vedtagelse. At Databeskyttelsesforordningen ikke kræver national indarbejdelse betyder, at forordningen skaber rettigheder og pligter på lige fod med national lovgivning.[141] Forordninger vedtages som regel med henblik på, at skabe konvergens inden for et bestemt område, som skal gælde for alle medlemsstaterne, og dette stemmer således overens med Databeskyttelsesforordningens 2. præambel, der tilsiger, at forordningen i overensstemmelse med de grundlæggende rettigheder og frihedsrettigheder, netop har til formål at bidrage til *"styrkelse og konvergens mellem økonomierne inden for det indre marked og fysiske personers velfærd".*

Det bemærkes da, at forordningens 2. præambel læner sig tæt op ad direktivets 2. præambel. Der er dog den væsentlige forskel, at 2. præambel i direktivet tilsiger, at direktivet i overensstemmelse med de grundlæggende rettigheder og frihedsrettigheder, har til formål at bidrage til at *"sikre økonomiske og sociale fremskridt og til at fremme samhandelen og det enkelte menneskes velfærd".*

Ud fra ordlydsfortolkning, og i overensstemmelse med det generelle formål EU-forordninger har, navnlig at skabe harmonisering inden for et bestemt lovområde medlemsstaterne imellem, vurderes det, at EU-lovgivernes hensigt bag harmonisering af

[139] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 142)
[140] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 142)
[141] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 142)

Databeskyttelse, ikke længere kun kan begrundes i at ”sikre”, men at lovgivning om Databeskyttelse derimod kræver at ”styrke og skabe konvergens”. Der lægges endvidere vægt på begrebet *det indre marked* i forhold til i direktivet, der blot anvender begrebet ”samhandelen”. Dette stemmer således overens med Lissabontraktatens artikel 3 om Unionens mål, herunder stk. 1 om at fremme befolkningernes velfærd, og endvidere særligt stk. 3 om at *Unionen opretter et indre marked*. Således bestyrkes målet om en samlet Union, der skal beskytte EU-borgernes sikkerhed, navnlig sikkerheden i personoplysninger, i overensstemmelse med målet om at opretholde *det indre marked*. Dette stemmer endvidere overens med chartrets artikel 8, om beskyttelse af grundlæggende rettigheder.

Det vil endvidere blive undersøgt om der er sket overordnede ændringer i eksempelvis titler, herunder anvendelse af begreber og principper, og hertil hvorvidt de væsentligste artikler i henhold til problemstillingen har gennemgået ændringer.

Direktivets kapitel IV om *Videregivelse af personoplysninger til tredjelande*, navnlig artikel 25. Kapitlet indeholder artikel 25 om de generelle principper i forbindelse med overførsel af personoplysninger til tredjelande, og kapitel 26 om undtagelserne fra bestemmelserne i artikel 25.
Direktivets artikel 25, om *Principper*, består af stk. 1 om medlemsstaterne der fastsætter nærmere bestemmelser om videregivelse af personoplysninger til et tredjeland, stk. 2 om vurdering af beskyttelsesniveauet i et tredjeland, stk. 3 om medlemsstaterne og Kommissionen, der underretter gensidigt hinanden, stk. 4 om Kommissionens konstatering om et tredjelands manglende tilstrækkelighed i beskyttelsesniveau, samt stk. 5 om Kommissionen, der indleder forhandlinger i forlængelse af stk. 4, og stk. 5 om Kommissionens kompetence til at fastslå et tredjelands beskyttelsesniveau.

Forordningens kapitel V om *Overførsler af personoplysninger til tredjelande eller internationale organisationer*. Forordningens overskrift på kapitel V er mere uddybende i forhold til direktivets overskrift på sit kapitel IV. Årsagen til dette må ses i lyset af den drastiske udvikling samfundet har været igennem siden da, især i forhold til teknologiens essentielle betydning i alle henseender, jf. forordningens 6. præambel. I forhold til

overførsler af personoplysninger, har der endvidere forekommet voldsom vækst i bevægelse af oplysninger på tværs af landegrænserne, jf. for. pr. 5, og især i forhold til bevægelse på tværs af grænserne uden for Unionen, jf. for. pr. 116.
Forordningens kapitel V er endvidere mere uddybende, i forhold til direktivets kapitel IV. Kapitlet i Forordningen indeholder artikel 44, der fastsætter det generelle princip for overførsler, artikel 45 fastsætter bestemmelsen om overførsler, der er baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, og artikel 46 om overførsler omfattet af fornødne garantier, samt artikel 47 om bindende virksomhedsregler, og artikel 48, der udleder bestemmelsen om overførsel eller videregivelse uden hjemmel i EU-retten, samt artikel 49 om undtagelser i særlige situationer, og sidst i kapitlet er artikel 50, der fastsætter bestemmelse om et internationalt samarbejde om beskyttelse af personoplysninger.

Både direktivet og forordningen deler et todelt spektrum, at til trods for, at beskyttelsen af EU-borgernes grundlæggende rettigheder vægtes højt, så findes det lige så nødvendigt, at strømmen af personoplysninger på tværs af landegrænserne er nødvendig af hensyn til udbygningen af den internationale samhandel, jf. dir. pr. 56 og for. pr. 101.

I forhold til *"strømmen af personoplysninger"*, så dækker begrebet "overførsel" både den situation hvor en dataansvarlig i EU *videregiver* personoplysninger til en dataansvarlig uden for EU, og den situation, hvor en dataansvarlig i EU *overlader* en behandling af personoplysninger til en databehandler uden for EU, jf. forordningens art. 4, litra 2).

Tredjeland er ikke direkte defineret i Direktivet eller i Forordningen, og må således defineres ud fra hvad der *ikke* står i direktivet og endvidere ud fra dansk lovgivning, for at forstå definitionen på tredjeland.[142] Grunden til, at definitionen udredes ud fra Direktivet er, at Forordningens regler om overførsel af personoplysninger til tredjelande netop kendes i meget vidt omfang fra Direktivet, samt fra praksis i henhold til Direktivet.

[142] Afhandlingen har afgrænset sig fra dansk lovgivning, men finder det nødvendigt at anvende i forhold til at udlede definitionen på *tredjelande*, da Medlemsstaterne i henhold til Direktivet, netop selv skal lave nærmere bestemmelser i forhold til overførsel af personoplysninger til tredjelande, hvorfor det danske Datatilsynet anvendes:
https://www.datatilsynet.dk/erhverv/tredjelande/overfoersel-til-tredjelande/

Ud fra at direktivets artikel 1 udleder direktivets formål, og hertil direkte henvender sig til Medlemsstaterne, navnlig at "*Medlemsstaterne sikrer i overensstemmelse med dette direktiv"*. Endvidere findes det ud fra artikel 4 at medlemsstaternes anvendelse af de nationale bestemmelser der omfatter virksomheder eller organers aktiviteter inden for medlemsstaternes område, samt registeransvarlige, der ikke er etableret på pågældende medlemsstats område, men på et sted, hvor dens nationale lovgivning gælder i henhold til folkeretten, samt at der af en registeransvarlig, som ikke er etableret inden for EU, men som med henblik på behandling af personoplysninger anvender midler, uanset om det er elektronisk eller ikke-elektronisk, som befinder sig på den pågældende medlemsstats område. Sammenholdt med direktivets artikel 25 vedrørende *overførsel til tredjelande*, må det således forstås at *tredjelande* omfatter lande uden for EU- og EØS-samarbejdet. Ligeledes kan det fastslås i henhold til danske Datatilsynets vejledning om *overførsel til tredjelande*, at et tredjeland forstås som en stat der hverken indgår i det Europæiske Fællesskab, eller har indgået aftale i det Europæiske Økonomiske Fællesskab, altså et EØS-land.[143]

Det udledes af direktivets art. 25, stk. 1, at medlemsstaterne selv har ansvaret for at fastsætte nærmere bestemmelser om videregivelse af personoplysninger til at tredjeland, og at disse overholdes. Grundlæggende er direktivet således i overensstemmelse med TEUF art. 288, og i henhold til hensynet til det tilsigtede mål, bindende for enhver medlemsstat, sådan at de nationale myndigheder er overladt til at bestemme form og midler for gennemførelsen. Det tilsigtede mål i direktivets artikel 1, er at beskytte *fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, i forbindelse med behandling af personoplysninger.* [144] Dette er således i overensstemmelse med dets præambel 10, der forlyder, at skulle *sikre overholdelsen af de grundlæggende rettigheder og frihedsrettigheder, navnlig den ret til privatlivets fred*[145].

[143] Datatilsynet: Overførsel til tredjelande:
https://www.datatilsynet.dk/erhverv/tredjelande/overfoersel-til-tredjelande/
[144] Ulla Neergaard & Ruth Nielsen; EU Ret (2016, s. 223)
[145] Direktiv 95/46/EF, præambel 10

Direktivet er ikke blot udstedt til at overholde Medlemsstaterne imellem, men er derimod også tilsigtet ved overførsel til tredjelande.

Artikel 25, stk. 1 udleder endvidere et krav i forhold til overførsel af personoplysninger til tredjelande, navnlig at *det pågældende tredjeland sikrer et tilstrækkeligt beskyttelsesniveau,* og således udledes dette til, at der må skelnes mellem *sikre* og *usikre* tredjelande.

I Forordningens kapitel V skelnes der ligeledes mellem *sikre tredjelande*, jf. artikel 45, og *usikre tredjelande*, jf. artiklerne 46, 47, og 49. Selve begrebet "sikkert tredjeland" og begrebet "usikkert tredjeland" er ikke direkte nævnt i hverken direktivet eller i forordningen, men er derimod betegnelser, der er almindeligt anvendt i praksis[146], jf. eksempelvis Schrems-sagen.

Det gælder for både Direktivet og Forordningen, at der ved sikre tredjelande kan som udgangspunkt ske en overførsel uden videre, hvorimod en overførsel til usikre tredjelande kræver, at der fastsættes fornødne grantier eller at nogle særlige undtagelser finder anvendelse.[147]

Når virksomheder som Alibaba.com overfører personoplysninger til et tredjeland, skal virksomheden være opmærksom på, at de europæiske datatilsyn, i regi af den såkaldte Artikel 29-gruppe, i 2016 har opstillet fire essentielle europæiske garantier, der *altid* skal efterleves, uanset om Alibaba.com overfører personoplysninger til sikre eller usikre tredjelande. Garantierne er udledt af praksis, jf. Schrems-sagen, fra EU-Domstolen, hvoraf det følger, at (1) myndigheder i tredjelandes adgang til og brug af personoplysninger hidrørende fra EU skal ske på grundlag af klare, præcise og tilgængelige regler, jf. ligeledes for. art. 46, stk. 1, (2) myndigheder i tredjelandes adgang til og brug af personoplysninger hidrørende fra EU skal være nødvendig og proportional og indgrebet i de registreredes ret til beskyttelse af deres privatliv, (3) at

[146] Datatilsynet: Vejledning om overførsel af personoplysninger til tredjelande (s. 4)
[147] Datatilsynet: Vejledning om overførsel af personoplysninger til tredjelande (s. 5)

der skal være en uafhængig og effektiv tilsynsmyndighed i tredjelandet, og (4) at der skal være tilgængelige og effektive retsmidler for de registrerede i tredjelandet.[148]

5.3.1. Overførsel til tredjelande

Når Alibaba.com overfører personoplysninger til USA for oplagring, er der en del forhold som virksomheden skal iagttage.

Ud over de ovennævnte generelle forhold i afhandlingens kapitel 6, navnlig forordningens kapitel II, eksisterer der en række specifikke forhold, som en virksomhed skal forholde sig til. Disse forhold træder i kraft i særlige tilfælde, særligt hvis virksomheden, den dataansvarlige eller databehandleren overfører personoplysninger ud af EU, hvis der altså inden for branchen er særlige certificeringer, som skal efterleves, eller hvis der er særlige regler for visse branchers behandling eller på nationalt plan. Således skal virksomheden være opmærksom på, om der er særlige forhold der gør sig gældende for virksomhedens behandling af personoplysninger, særligt ved overførsel af oplysningerne til tredjelande uden for EU.

Her skal Alibaba.com overholde EU-reglerne i forhold til om personoplysningerne overføres til et tredjeland uden for EU- og EØS-samarbejdet. Da personoplysningerne overføres til USA, som er et land uden for EU- og EØS-samarbejdet, må det vurderes om USA er defineret som et sikkert tredjeland. Det må således vurderes til, at gennemførelsesafgørelsen endvidere vil stemme overens med de opstillede betingelser som Kommissionen skal opfylde i Databeskyttelsesforordningens artikel 45, stk. 2

I henhold til Kommissionens gennemførelsesafgørelse (EU) 2016/1250 om tilstrækkeligheden af beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred, har Kommissionen fastslået USA beskyttelsesniveau som værende tilstrækkelig i henhold til Databeskyttelsesdirektivets artikel 25, stk. 6

[148] Article 29 Working Party: WP 254 rev.01 (s. 8)

Ved at Alibaba Groups datterselskab Alibaba.com og Alibaba Cloud har tiltrådt aftalen i henhold til EU-U.S. Privacy Shield, jf. endvidere Kommissionens (EU) 2016/1250, kan Alibaba således opretholde lovligheden i overførsel af persondata fra EU til USA.[149] Så længe de europæiske datterselskaber i henhold til Kinas manglende oplistning som værende et *sikkert tredjeland*, findes det ulovligt for disse datterselskaber, at overføre EU-borgeres personoplysninger til Alibaba Group i Kina. Lovligheden opretholdes dog ved overførsel til afdelingen i USA gennem EU-U.S. Privacy Shield.

6. Den registreredes rettigheder

Det fremgår af direktivets artikel 7, om *principper vedrørende grundlaget for behandling af oplysninger*, at behandling af personoplysninger kun må finde sted hvis den registrerede har afgivet klar samtykke. Formålet med de registreredes rettigheder er blandt andet, at skabe åbenhed om, hvem der behandler oplysningerne om de registrerede, at give de registrerede muligheder for at få indsigt i hvilke oplysninger, der behandles om dem, samt at give de registrerede muligheder for at kræve, at urigtige oplysninger slettes, berigtiges, endvidere.

Som udgangspunkt er det den dataansvarlige, der skal sørge for at iagttage de registreredes rettigheder, hvorfor en eventuel dataansvarligs databehandler ikke kan pålægges et selvstændigt ansvar for at iagttage rettighederne. Der er dog ikke noget til hinder for, at en databehandler, efter aftale med den dataansvarlige, samt instruks fra denne, at iagttage de registreredes rettigheder på den dataansvarliges vegne og under dennes ansvar.

Det kan i øvrigt være en forudsætning for, at en dataansvarlig kan iagttage de registreredes rettigheder, at en databehandler medvirker i et vist omfang. Dette kan være i tilfælde som når der skal slettes eller berigtiges oplysninger, der fysisk befinder sig hos databehandleren, herunder på dennes servere eller lignende.

[149] På Privacy Shield websiden er Alibaba.com og Alibaba Cloud oplistet som værende tiltrådt EU-USA aftalen, således at overførsler landene imellem er på lovligt grundlag: https://www.privacyshield.gov/participant_search

6.1. Virksomhedens oplysningspligt til den registrerede

I databeskyttelsesforordningens artikel 13 og 14 skelnes der mellem den situation, hvor den dataansvarlige indsamler personoplysninger hos den registrerede selv, jf. art. 13, og den situation hvor den dataansvarlige indsamler oplysninger om den registrerede hos andre end den registrerede selv, jf. art. 14. Afhandlingen vil gå nærmere i dybden med forholdet om indsamling af personoplysninger fra den registrerede selv, og vil ikke behandlere forholdet om indsamling fra andre end den registrerede selv, jf. afgrænsningen, afsnit XXX.

En dataansvarlig bør som udgangspunkt iagttage sin oplysningspligt over for en registreret ved *skriftligt* at give den registrerede de oplysninger, som den pågældende har krav på at få. Dette er med henblik på, at den dataansvarlige bedst vil kunne dokumentere, at oplysningspligten er blevet iagttaget.

I de tilfælde, hvor den registrerede anmoder om at modtage oplysningerne mundtligt, bør den dataansvarlige således sørge for at kunne dokumentere, at den dataansvarlige har modtaget en anmodning om at give oplysningerne mundtligt, og sikre den registreredes identitet samt, at den dataansvarlige har givet oplysningerne til de registrerede.

I forhold til Alibaba-casen, hvor oplysningerne skal gives elektronisk, da den registrerede formodes selv at have henvendt sig elektronisk eller giver oplysningerne via en elektronisk formular.

For at en virksomhed kan iagttage sin oplysningspligt, er det vigtigt, at oplysningerne gives til den registrerede. Dette betyder, at virksomheden som dataansvarlig skal tage aktive skridt til at give oplysningerne, hvorfor det ikke vil være tilstrækkeligt, at have oplysningerne liggende på en webside eller lignende, som den registrerede selv skal finde.

Ved iagttagelse af oplysningspligten, er der ikke krav om, at oplysningerne skal gives i bestemt format eller lignende. Det er således op til virksomheden selv, at vurdere,

hvordan oplysningerne mest hensigtsmæssigt gives til den registrerede. her skal virksomheden tage hensyn til de konkrete omstændigheder ved indsamlingen, ved eksempelvis om indsamlingen sker gennem en blanket, en webside, en app, eller som led i sagsbehandling, m.v.

I henhold til Alibaba-casen har indsamling af personoplysninger via en webside således relevans, hvorfor dette vil uddybes nærmere. Ved indsamling af personoplysningerne på websiden, kan virksomheden give en registreret de krævede oplysninger ved hjælp af standardtekst i pop-up meddelelser, der aktiveres ved den registreredes udfyldelse af onlineformularer, m.v. I pop-up meddelelserne kan eksempelvis være links til bagvedliggende oplysninger i form af tekster, videoer eller lydfiler, som gør det muligt for den registrerede at navigere hen til netop de oplysninger, der er mest interessante og relevante for den pågældende. Det er dog under alle omstændigheder vigtigt for virksomheden, at sørge for, at oplysningerne er tydeligt fremhævede og fra start giver den registrerede et klart overblik.

Ved at en virksomhed holder sig til de nævnte forpligtelser ved iagttagelse og eksemplet der er nævnt i henhold til indsamling på webside, kan virksomheden således overholde kravet om, at oplysningerne skal gives på en tydelig, kortfattet og letforståelig måde. Oplysningerne, som virksomheden er forpligtet til at give, skal altså være tydeligt adskilt fra andre oplysninger.

Endvidere indebærer kravet om oplysningernes forståelighed også, at indholdet af oplysningerne skal kunne forstås af et gennemsnitligt medlem af den tilsigtede målgruppe. Dette kan virksomheden opnå, ved at supplere de skriftlige oplysninger med billeder eller ikoner, der kan danne et bedre overblik for den registrerede, eller oplysningerne kan gives gradvist i forbindelse med, at den registrerede bliver taget igennem en ansøgningsblanket eller lignende, for at gøre de mange oplysninger mere overskuelige.

6.1.1. Tidspunktet for at opfylde oplysningspligten

Personoplysningerne der indsamles hos den registrerede selv, er de tilfælde hvor vedkommende selv, enten på virksomhedens opfordring eller uopfordret, indgiver oplysningerne. I dette tilfælde er udgangspunktet således, at virksomheden skal give oplysningerne samtidig med, at oplysningerne indsamles fra den registrerede, og de skal endvidere som udgangspunkt kun gives én gang. Hvis den registrerede derimod skal udfylde en ansøgning, blanket eller lignende og indlevere til virksomheden, anbefales det, at oplysningerne gives i selve ansøgningen eller blanketten. Derimod i andre tilfælde, hvor den registrerede selv, uanset om det er uopfordret, henvender sig til virksomheden, skal oplysningerne gives snarest muligt, dog inden for 10 dage.[150]

I forhold til Alibaba-casen, har det særligt relevans, at oplysningerne gives samtidig med, at der indsamles oplysninger fra den registrerede, da det i henhold til casen foregår på webside, Alibaba.com.

Det skal kort nævnes, at hvis en virksomhed har indsamlet personoplysninger om en registreret hos andre end den registrerede selv, eksempelvis hos andre dataansvarlige, så skal virksomheden give oplysningerne så tidligt som muligt efter indsamlingen. Dette vil normalt betyde inden for 10 dage.[151]

6.1.2. De nærmere oplysninger som skal gives til den registrerede

Når personoplysninger indsamles hos den registrerede selv, har virksomheden pligt til at opgive grundlæggende oplysninger om sig selv. Oplysningerne indeholder nærmere information om virksomheden og kontaktoplysninger, samt identitet, hos hvem den registrerede i givet tilfælde henvender sig til eller behandles af. På samme måde skal den registrerede således have oplysninger om identitet og kontaktoplysninger på en eventuel

[150] Datatilsynets fortolkning i Databeskyttelsesforordningen – En introduktion til de kommende, nye regler om beskyttelse af personoplysninger, oktober 2017, og Vejledning om de registreredes rettigheder, af Datatilsynet (marts 2018)

[151] Datatilsynets fortolkning i Databeskyttelsesforordningen – En introduktion til de kommende, nye regler om beskyttelse af personoplysninger, oktober 2017 og Vejledning om de registreredes rettigheder, af Datatilsynet (marts 2018)

repræsentant i Unionen, navnlig Alibaba Groups dattervirksomheder, der er etableret rundt omkring i Unionen.

Hvis virksomheden har udpeget en databeskyttelsesrådgiver, den såkaldte DPO, skal virksomheden give den registrerede kontaktoplysningerne på denne.
Efterfølgende skal virksomheden give den registrerede oplysningerne om formålene med sammen med retsgrundlaget for behandlingen. Hvis en behandling foretages som følge af national lovgivning, skal virksomheden oplyse den registrerede hvilken lovgivning og relevante bestemmelser i denne.

Når virksomheden overfører personoplysningerne til et *tredjeland*, udløser det en pligt til at give den registrerede en række oplysninger. Virksomheden har således pligt til at oplyse hvorvidt personoplysningerne overføres til at sikkert- eller et usikkert tredjeland. Hvis tilfældet er, at personoplysninger skal sendes til et usikkert land, skal den registrerede ligeledes oplyses om, på hvilket grundlag overførslen til tredjelandet sker.

Endvidere har virksomheden pligt til at lave en konkret vurdering om hvilke oplysninger den registrerede ydermere skal blive belyst om. Dette kræver, i henhold til kravene om, at den dataansvarlige skal sikre rimelig og gennemsigtig behandling, at denne vurderer tidsrummet for, hvor længe det findes nødvendigt for virksomheden at beholde og opbevare personoplysningerne. I forlængelse heraf har den dataansvarlige pligt til at oplyse den registrerede om de rettigheder, som vedkommende netop har i henhold til databeskyttelsesforordningen, navnlig retten til at anmode indsigt i de oplysninger, der behandles, og retten til at få berigtiget eller at få slettet oplysningerne, eksempelvis som følge af, at de er urigtige.

Når den registrerede har givet samtykke til behandlingen af personoplysningerne, skal den dataansvarlige ligeledes give den registrerede oplysning om, at vedkommende kan trække sit samtykke tilbage.

Den dataansvarlige har endvidere pligt til at oplyse den registrerede om retten til at indgive en klage over behandlingen til en tilsynsmyndighed, eksempelvis i Danmark vil man kunne indgive klage til Datatilsynet eller Domstolsstyrelsen.

I forhold til Alibaba Group, der anvender automatiske afgørelser, navnlig profilering, har virksomheden pligt til at vurdere, hvorvidt den registrerede skal belyses om meningsfulde oplysninger i forhold til logikken bag den type behandlinger, der foretages, altså ved automatikken eller profileringen. Ligeledes bør virksomheder som Alibaba Group lave konkrete vurderinger om betydningen, samt de forventede konsekvenser der kan forekomme ved behandling gennem profilering.

6.1.3. Undtagelser fra oplysningspligten

Den dataansvarlige kan benytte sig af undtagelser fra oplysningspligten, hvis den registrerede allerede er bekendt med de forannævnte oplysninger, som virksomheden er forpligtiget til at indgive efter konkret vurdering. Dette kræver dog, at den dataansvarlige har sikret sig, at den registrerede er bekendt med oplysningerne, og endvidere, at den registrerede til en hver tid er i stand til at dokumentere hvilke oplysninger, hvornår de er indgivet og hvordan de er indgivet. Dette kræver endvidere, at den dataansvarlige sikrer sig, at der ikke er sket ændringer i oplysningerne, siden den registrerede sidst modtog dem.

Den dataansvarlige kan endvidere undlade at indgive oplysningerne til den registrerede af legitime hensyn, navnlig i henhold til afgørende hensyn til statens sikkerhed, forsvaret, den offentlige sikkerhed og forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger. Altså legitime hensyn som primært hjemles i henhold til national lovgivning.

6.2. Den registreredes ret til indsigt

I forordningens artikel 15 udledes den registreredes ret til indsigt, som for det første indebærer, at den registrerede har ret til at se de personoplysninger, der behandles af en

virksomhed, og for det andet retten til at modtage en række oplysninger om den eller de behandlinger, som virksomheden foretager.

Formålet med retten til indsigt i artikel 15 er, at skabe mere gennemsigtighed omkring hvordan en virksomhed anvender eksempelvis personoplysningerne i sit it-system, og at den registrerede har muligheden for at kontrollere at de anvendte personoplysninger er korrekte og behandles lovligt.

Når den registrerede anmoder om indsigt i personoplysningerne der bliver behandlet, har virksomheden pligt til at imødekomme anmodningen, og har dermed pligt til at give vedkommende indsigt i indholdet af de personoplysninger, som bliver behandlet om den pågældende. Dette efterkommes enten ved at udlevere kopier af de originale dokumenter, eller ved at kopiere oplysningerne om den registrerede over i et nyt dokument, uanset om de sendes via elektronisk post, eller ved at give den registrerede elektronisk adgang gennem vedkommendes egen PC.

Virksomheden må kun udlevere oplysninger der vedrører den registrerede selv. Hvis der i dokumentet indgår oplysninger om andre personer, så skal virksomheden enten sløre dem eller fjerne dem, således at andre personers personoplysninger ikke udleveres til uvedkommende.

Når den dataansvarlige imødekommer den registreredes anmodning om indsigt, er det ikke nok at sende indholdet af de oplysninger som bliver behandlet. Virksomheden har endvidere pligt til at oplyse den registrerede om formålene med behandlingen, og dertil oplyse den registrerede om de berørte kategorier af personoplysningerne. Dette betyder, at virksomheden skal oplyse om, hvorvidt de indsamlede oplysninger er almindelige personoplysninger, oplysninger om straffedomme og lovovertrædelser, eller særlige kategorier af personoplysninger, altså de følsomme personoplysninger. Hertil skal virksomheden oplyse den registrerede om de modtagere, som personoplysningerne er eller vil blive videregivet til, særligt hvis modtagerne findes i tredjelande. Virksomheden skal også oplyse om det estimerede tidsrum, som personoplysningerne vil blive behandlet og dermed opbevaret.

Hvis en virksomhed benytter automatiske afgørelser, særligt profilering, skal denne ligeledes oplyse om, at den registrerede er undergivet en sådan behandling. Virksomheden skal oplyse den registrerede om logikken i de automatiske afgørelser, som indebærer en beskrivelse af hvilke overvejelser, der ligger til grund for behandlingen, samt eksempelvis hvordan systemet i profileringen kommer frem til afgørelserne.

Hertil har virksomheden pligt til at informere den registrerede hvis personoplysningerne overføres til usikre tredjelande, og om de fastsatte fornødne garantier, der anvendes for databeskyttelsen.

6.2.1. Undtagelser fra indsigtsretten

Virksomheden kan afvise at imødekomme en anmodning om indsigt, hvis imødekommelsen er lovligt begrundet i henhold til forordningens artikel 15, stk. 4, da indsigten vil kunne krænke andres rettigheder og friheder. Dette kan eksempelvis være rettigheder og frihedsrettigheder der skal beskytte forretningshemmeligheder eller intellektuel ejendomsret, herunder navnlig den ophavsret, som for eksempel et program er beskyttet af. En virksomhed kan dog kun undtage de oplysninger, som kan indebære en krænkelse, således at den registrerede trods alt har ret til at få en kopi af alle andre personoplysninger.

6.3. Den registreredes ret til berigtigelse

En registreret har i henhold til forordningens artikel 16 retten til berigtigelse, som for det første indebærer, at vedkommende har ret til at få urigtige personoplysninger om sig selv rettet. For det andet har vedkommende ret til at få fuldstændiggjort ufuldstændige personoplysninger, under hensyntagen til formålene med en behandling, som kan ske ved at vedkommende fremlægger en supplerende erklæring. Virksomheden skal imødekomme den registreredes anmodning om at få fuldstændiggjort personoplysningerne med supplerende oplysninger, hvis dette indebærer, at virksomheden vil gøre sagen mere fuldstændig. Den dataansvarlige har i forbindelse

hermed pligt til at sikre, at personoplysninger berigtiges, hvis den ansvarlige bliver opmærksom på, at de er forkerte, samt at oplysningerne er fuldstændige og ajourførte, jf. forordningens artikel 5, stk. 1, litra d).

6.4. Den registreredes ret til at blive glemt

Retten til at blive glemt, altså retten til at få slettet personoplysninger om sig selv, er udledt i forordningens artikel 17. Den registrerede har således ret til at få sine personoplysninger slettet uden unødig forsinkelse, når ét af følgende forhold gør sig gældende: at det ikke længere er nødvendigt for virksomheden at have oplysninger om den registrerede af hensyn til formålene ved indsamlingen; at virksomheden har baseret behandlingen på et samtykke, men at den registrerede nu trækker dette tilbage; at virksomheden behandler oplysningerne uden hjemmel i forordningens kapitel II om *principper*; at virksomheden er forpligtiget til at slette oplysningerne som følge af EU-lovgivning eller national lovgivning i en medlemsstat; at virksomheden er forpligtet til at slette oplysningerne som følge af, at den registrerede udøver sin ret til indsigelse; at virksomheden er udbyder af en informationssamfundstjeneste, navnlig et socialt netværk, og at virksomheden som følge af at have baseret behandlingen af personoplysningerne på et samtykke i henhold til Værgemålsloven.[152]

Den dataansvarlige skal sikre sig, at personoplysningerne ikke kan genskabes, når disse skal slettes. Således skal virksomheden sikre, at oplysningerne er slettet fra virksomhedens backup, altså skal oplysningerne være slettet i virksomhedens systemer.

Ved imødekommelse af anmodning om sletning fra den registrerede, har virksomheden pligt til at underrette dem, som virksomheden har videregivet oplysningerne til, altså andre dataansvarlige, jf. underretningspligten i forordningens artikel 17, stk. 2. Dette er under hensyntagen til at træffe rimelige foranstaltninger i forhold til den teknologi, der er tilgængelig og omkostningerne ved implementeringen, for at underrette de

[152] LBK nr. 105 af 20/08/2007, Gældende

dataansvarlige, der fortsat behandler oplysningerne, at den registrerede har anmodet om, at få de pågældende personoplysninger slettet.

6.4.1. Undtagelser fra retten til sletning

Der er i forordningens artikel 17, stk. 3 oplistet en række undtagelser til retten til at få slettet personoplysninger slettet. Dette er navnlig i situationer, hvor virksomhedens behandling er nødvendig for at overholde en lovlig forpligtelse eller hvor behandlingen er nødvendig i henhold til samfundets interesse eller en opgave. Dette er primært offentlige myndigheders behandlinger, som kan afvise en anmodning i henhold til denne undtagelse.

Endvidere er en virksomhed undtaget fra forpligtelsen til at slette, hvis behandlingen findes nødvendig i forhold til et retskrav der skal fastlægges, gøres gældende eller forsvares. Således kan virksomheden bibeholde personoplysninger i forbindelse med en retssag, navnlig retssag mod den registrerede.

6.5. Den registreredes ret til begrænsning af behandling

I henhold til forordningens artikel 18 indebærer begrænsning af behandling, at den registrerede i visse tilfælde har retten til at få begrænset sine personoplysninger, hvis oplysningernes rigtighed bestrides, hvorfor virksomheden skal begrænse behandlingen, indtil den registrerede kan bekræfte rigtigheden. Hvis oplysningerne behandles på ulovligt grundlag, skal begrænsningen straks indtræffe. Hvis virksomheden ikke længere kan anvende personoplysningerne til behandling, men er nødvendige i henhold til at et retskrav skal fastlægges, gøres gældende eller forsvares, skal behandlingen ligeledes begrænses. Hvis den registrerede har gjort indsigelse mod virksomhedens behandling af personoplysningerne, skal behandlingen ligeledes begrænses, i en periode hvor det undersøges hvorvidt virksomhedens legitime interesser overstiger den registreredes legitime interesser i forhold til behandlingen.

Hvis behandlingen begrænses for en periode, indebærer denne, at virksomheden som udgangspunkt ikke må behandle dem, navnlig bruge dem, eller videregive dem.

I praksis betyder dette, at virksomheden skal gøre oplysningerne utilgængelige for brugerne af systemet, som virksomheden anvender, sådan at ingen kan anvende dem til enhver form for behandling, end at de opbevares på systemet.

Når den begrænsede behandling ophører, skal virksomheden underrette den registrerede i henhold til underretningspligten i forordningens artikel 19.

6.6. Den registreredes ret til dataportabilitet

Forordningens artikel 20 udleder en registreredes ret til dataportabilitet, som for det første indebærer, retten til at modtage sine personoplysninger, som den registreret selv har indgivet, i et struktureret, almindeligt anvendt og maskinlæsbart format til personlig brug uden hindring. For det andet indebærer det, at den registrerede har muligheden for at overføre personoplysningerne fra én dataansvarlig til en anden, således at personoplysningerne kan flyttes, kopieres og overføres fra et it-system til et andet.

Formålet bag dataportabilitet ligger i, at den registrerede skal have muligheden for øget egenkontrol over sine oplysninger, uanset om det er ønsket om at modtage- eller at overføre oplysningerne.

Den registrerede opnår retten til at modtage- og overføre sine oplysninger, når vedkommende selv har indgivet sine personoplysninger til virksomheden ved elektroniske anordninger, eksempelvis på en webside, samt at behandlingen foretages af virksomheden automatisk, og er baseret på et samtykke.

Når den registrerede vil gøre brug af sin ret til dataportabilitet, kræver det af virksomheden, at være opmærksom på, at andre rettigheder eller frihedsrettigheder ikke bliver krænket i forbindelse hermed. Dette indebærer, at hvis oplysningerne bliver overført fra én dataansvarlig til en anden, og der i oplysningerne indgår personoplysninger om tredjemand, må den modtagende dataansvarlig kun benytte

oplysningerne om tredjemanden til de samme formål, som den oprindelige dataansvarlige brugte dem til.

Den registrerede har ret til at modtage sine oplysninger på en måde hvorpå det gøres nemt for denne, at administrere og videresende sine personoplysninger. Altså har virksomheden pligt til at sende oplysningerne i *et struktureret, almindeligt anvendt og maskinlæsbart format*, jf. art. 20, stk. 1, 1. pkt.

6.7. Den registreredes ret til indsigelse

I henhold til forordningens artikel 21 har den registrerede til enhver tid retten til at gøre indsigelse mod behandling af sine personoplysninger, til trods for, at behandlingen er lovlig, når grundene vedrører den pågældendes særlige situation. Den særlige situation består da i tungtvejende, særlige og individuelle situation, som forpligter den dataansvarlige i at vurdere nødvendigheden af behandlingen på ny og dermed eventuelt stoppe behandlingen. En dataansvarlig kan dog undtages i at imødekomme indsigelsen, hvis denne ved lov er blevet pålagt at foretage den konkrete behandling.

Ved behandling i form af direkte markedsføring gælder, at den registrerede har ret til at gøre indsigelse mod denne behandling. Den registrerede kan endvidere gøre indsigelse mod behandling i forhold til profilering, hvis profileringen vedrører direkte markedsføring. Alibaba.com vil eksempelvis være omfattet, når profileringen foretages med henblik på at analysere forhold om den registreredes personlige præferencer eller interesser. Disse bliver da opfanget på websiden efterhånden som den registrerede viser interesse for eksempelvis bestemte varegrupper, idet denne søger på websiden. Således kan den registrerede gøre sin indsigelse gældende på et hvilket som helst tidspunkt, og omfatter al behandling af personoplysningerne med henblik på direkte markedsføring. Når den registrerede gør ret på sin indsigelse i forhold til direkte markedsføring, har Alibaba.com således pligt til at stoppe med at behandle oplysningerne til dette formål.

6.8. Den registreredes ret til ikke at være genstand for en afgørelse, der er baseret på profilering

Profilering, jf. forordningens artikel 22, består i at en virksomhed, Alibaba.com for eksempel, for det første underlægger en registreret en afgørelse, der alene er baseret på automatisk behandling, som hat retsvirkning eller på tilsvarende vis betydeligt påvirker vedkommende. For det andet består profileringen i, at den registrerede underlægges en automatisk behandling af sine personoplysninger, der består i at Alibaba.com som eksempelvis anvender oplysningerne til at evaluere bestemte personlige forhold vedrørende den registrerede, navnlig for at analysere eller forudsige forhold vedrørende den registreredes personlige præferencer, interesser, adfærd, samt den registreredes geografiske position, eller bevægelser.

I forhold til Alibaba.com, har retten i praksis den betydning for virksomheden, at denne som udgangspunkt ikke må træffe afgørelser, der alene er baseret på automatisk behandling eller profilering, når profileringen har retsvirkninger for eller betydeligt påvirker den registrerede. det kan dog diskuteres hvorvidt Alibaba.com's anvendelse af kundernes oplysninger til profilering, kan påvirke dem betydeligt eller skabe retsvirkninger for denne, da profileringen består i hvad den registreret har søgt efter på Alibaba.com websiden, og dermed sker en analyse på den registreredes varepræferencer.

Der er således to betingelser, som skal være opfyldt, for at en virksomhed som udgangspunkt ikke må træffe afgørelser, der alene er baseret på automatisk behandling eller profilering over for den registrerede. Den første betingelse består i, at profileringen skal have retsvirkning for eller påvirker den registrerede betydeligt, og andet betingelse består i, at profileringen indebærer en evaluering af den registreredes peronslige forhold. Profileringer vil altid indebære en evaluering af personlige forhold, navnlig præferencer og interesser i forhold til den registreredes anvendelse af Alibaba.com, men om hvorvidt profileringen vil påvirke den registrerede betydeligt eller vil have en retsvirkning, kan dog ikke altid betinges, da websiden udbyder salg af varer på globalt plan, under forudsætning af at varerne er lovlige i det land hvorfra den registrerede bestiller og køber.

6.8.1. Undtagelser fra retten til ikke at være genstand for en afgørelse, der er baseret på profilering

Den registreredes ret til ikke at være genstand for afgørelse, der er baseret på profilering, kan undtages i de tilfælde hvor det for virksomheden er nødvendigt for at indgå- eller opfylde en kontrakt, jf. forordningens artikel 22, stk. 2. Dette betyder konkret, at retten ikke gælder, hvis profileringen hos Alibaba.com er nødvendig for at indgå eller opfylde en kontrakt mellem denne og den registrerede.
I sådanne situationer kan Alibaba.com dog gennemføre en række foranstaltninger, for at beskytte den registreredes rettigheder. Det kan være svært at tolke, hvilke foranstaltninger en virksomhed som Alibaba.com skal foretage, når Alibaba.com har indhentet samtykke fra den registrerede. Man kunne dog eksempelvis forestille sig, at Alibaba.com kunne give den registrerede muligheden for at slå profileringen fra, under *profilindstillinger* på brugersiden. Ved at en virksomhed har gennemført passende foranstaltninger for at beskytte den registrerede, og dermed opfyldt sin pligt i henhold hertil, kan virksomheden således benytte sig af undtagelsen i forordningens artikel 22, stk. 2.

Hvis virksomheden derimod behandler følsomme personoplysninger, i henhold til forordningens definition i artikel 9 om *Behandling af særlige kategorier af personoplysninger*, netop i forbindelse med afgørelse eller profilering, kan det være sværere for virksomheden at fravige udgangspunktet om, at den registrerede har ret til ikke at være genstand for en sådan afgørelse og profilering. Der skal altså være tale om oplysninger om for eksempel race, politisk overbevisning eller helbredsoplysninger, jf. for. art. 9, stk. 1.

I sådanne tilfælde skal en virksomhed som Alibaba.com sikre sig, at profileringen sker på lovligt grundlag, altså at den registrerede har givet sit udtrykkelige samtykke, medmindre at behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser fastlagt i EU-retten, men dette kan næppe blive tilfældet, da Alibaba.com er kommerciel virksomhed, med henblik på salg af forbrugervarer.

Ikke desto mindre har virksomheder, der behandler følsomme personoplysninger, pligt til, at indføre passende foranstaltninger til beskyttelse af den registreredes rettigheder og

interesser. Disse kan bestå i, at virksomheden giver den registrerede mulighed for at opnå menneskelig indgriben, eksempelvis ved ansøgning om lånetilsagn fra en bank, hvor banken ikke må udføre automatisk afgørelse på kunden, eller ved at den registrerede gives mulighed for at fremkomme med sine synspunkter eller bestride en afgørelse, eller at virksomheden løbende foretager kontroller af, at systemet fungerer som det skal, dette kunne have særligt relevans for Alibaba.com i forhold til deres virksomhed, hvor der søges på kundernes præferencer ud fra tidligere handlinger samt køb, eller at virksomheden benytter sig af anonymisering så vidt som muligt.

6.9. Den registreredes rettigheder i henhold til overførsel til tredjelande

Direktivets formål fremgår af artikel 1 sammenholdt med anden- og tiende betragtning, som forlyder, at direktivet ikke blot har til formål, at sikre en effektiv og fuldstændig beskyttelse af fysiske personers frihedsrettigheder og grundlæggende rettigheder, navnlig retten til respekt for privatlivet i forbindelse med behandling af personoplysninger, men at der ligeledes skal sikres et højt beskyttelsesniveau af frihedsrettighederne og de grundlæggende rettigheder. Således fremhæves styrken ved chartrets artikel 7 om den grundlæggende ret til respekt for privatlivet og endvidere styrken ved chartrets artikel 8 om den grundlæggende ret til beskyttelse af personoplysninger.

Bestemmelserne i Databeskyttelsesdirektivet, for så vidt de omhandler behandling af personoplysninger, der kan krænke de grundlæggende frihedsrettigheder og navnlig retten til respekt af personoplysninger, nødvendigvis skal fortolkes under hensyntagen til de grundlæggende rettigheder, som er sikret ved chartret, jf. Österreichischer-sagen.[153]

I Forordningens artikel 1 udledes formålet, hvori det fastsættes i stk. 2, at forordningen beskytter fysiske personers grundlæggende rettigheder og frihedsrettigheder, og hertil retten til beskyttelse af personoplysninger.

[153] De forenede sager C-465/00, C-138/01 og C-139, Österreichischer Rundfunk m.fl.: præmis 68

6.9.1. De uafhængige tilsynsmyndigheder

I direktivets artikel 28, stk. 1 fremgår det, at medlemsstaterne pålægges pligten til at udpege nationale tilsynsmyndigheder med beføjelser til i fuld uafhængighed, at påse overholdelsen af Unionens regler om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger, der videregives til tredjelande. Dette stemmer endvidere overens med chartrets artikel 8, stk. 3, der netop giver hjemmel til oprettelse af en sådan myndighed, jf. endvidere TEUF artikel 16, stk. 2, om kontrol ved uafhængige myndigheder.

Artikel 51, stk. 1. i Forordningen stemmer således overens med direktivets artikel 28, hvor de uafhængige tilsynsmyndigheder er ansvarlige for at føre tilsyn med anvendelsen af forordningen, netop for at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling.
Forskellen imellem bestemmelsen i direktivet og i forordningen er netop, at medlemsstaterne selv har pligt til at fastsætte nærmere bestemmelser som de nationale tilsynsmyndigheder har pligt til at følge, og hvorimod tilsynsmyndighederne i henhold til forordningen, har pligt til at følge bestemmelserne i henhold til forordningen, jf. nærmere for. art. 51, stk. 2 og for. pr. 123, hvor formålet er at tilsynsmyndighederne således skal bidrage til ensartet anvendelse af forordningen.

I henhold til forordningens artikel 52, nærmere om tilsynsmyndighedernes *uafhængighed*, er formålet at sikre et tilsyn der er effektivt og pålideligt med henblik på, at styrke beskyttelsen af personer og organer. Målet er navnlig at sikre en ligevægt mellem de to modsættende, men fundamentale principper, navnlig princippet om at sikre beskyttelse af privatlivets fred og princippet om tjenesteydelsers frie bevægelighed, nærmere de hensyn, der styrer den frie udveksling af personoplysninger.

Det fremgår af direktivets artikel 28, stk. 3, at de nationale tilsynsmyndigheder er tillagt beføjelser der er nødvendige til at varetage de i direktivets 63. betragtning nævnte opgaver, herunder undersøgelses- og interventionsbeføjelser, navnlig når drejer sig om klager, samt beføjelser til at indbringe sager for en retsinstans. Tilsynsmyndighedernes beføjelser er dog i henhold til artikel 28, stk. 1 begrænset til kun at række over

behandlinger på den medlemsstats område som de hører ind under. Det fremgår dog af artiklens stk. 6, 2 pkt. at tilsynsmyndighederne tillægges beføjelse til at behandle sager i en anden medlemsstat mod anmodning, således at tilsynsmyndighederne opfordres til at samarbejde. Dette stemmer endvidere overens med forordningens artikel 52 sammenholdt med forordningens præambel 124-126, hvor det fremhæves, at en ledende tilsynsmyndighed og dertil medhjælpende tilsynsmyndigheder, bør tillægges beføjelser til at bidrage hinandens kompetencer til at varetage behandlinger, sådan at bindende afgørelser kan vedtages ved indgivne klager.

Tilsynsmyndighedernes beføjelser er begrænset i henhold til artikel 28, således at de ikke råder over nogen beføjelser i forhold til den behandling af personoplysninger, der foretages på et tredjelands område. Det fremgår dog af direktivets artikel 2, litra b), at den transaktion der består i at overføre personoplysninger fra en medlemsstat til et tredjeland, netop udgør en sådan behandling af personoplysninger foretaget på en medlemsstats område. Således rækker de nationale tilsynsmyndigheders beføjelser ud til et tredjelands område, når en EU-borgers personoplysninger, som omhandlet i artikel 2, litra b), er gjort til genstand for behandling ved overførsel fra medlemsstaten til tredjelandet.

6.10. Den registreredes klageadgang

Det fremgår af forordningens artikel 77, at EU-borgere har ret til at indgive klage til en tilsynsmyndighed, hvis denne finder, at en behandling af personoplysningerne vedrørende vedkommende har fundet sted. Kravet i artikel 77 er således, at vedkommende indgiver sin kage til tilsynsmyndigheden i den medlemsstat, hvor vedkommende har sit sædvanlige opholdssted, eller dér hvor den påståede overtrædelse har fundet sted.

Sammenholdt med forordningens artikel 79 har den registrerede adgang til effektive retsmidler over en dataansvarlig, særligt i forhold til casen, vil den registrerede således kunne indgive en klage til en tilsynsmyndighed, jf. artikel 77, hvor endvidere den registrerede skal have adgang til effektive retsmidler. Dette stemmer således overens med Chartrets artikel 47, der udleder retten til effektive retsmidler, samt adgang til en upartisk domstol, som værende en grundlæggende rettighed.

7. Alibaba-case og det Europæiske marked

Databeskyttelsesforordningen sigter mod at forene EU's databeskyttelseslovgivning og styrke EU's databeskyttelse for at imødekomme de nye privatlivsudfordringer, der følger med udviklingen af digitale teknologier. Forordningen vil have stor indflydelse på udenlandske virksomheder, der er rettet mod det europæiske marked. Med den kinesiske koncernvirksomhed [154], Alibaba Group, herunder Alibaba.com, som eksempel, der indsamler en store mængde elektroniske data på EU-markedet gennem AliExpress og overfører disse data til andre Alibaba-koncernrelaterede virksomheder i Alibabas e-handelsøkosystem for at fuldføre transaktioner eller foretage markedsføringsforskning, men oplagrer personoplysningerne, i det amerikanske datterselskab Alibaba Cloud i USA. Serverne der oplagrer personoplysninger er således beliggende i USA.

Forordningen fastsætter strenge standarder for beskyttelse af registrerede i Unionen, hvor særligt emnerne om ekstraterritorial virkning af forordningen, fortolkning af personoplysninger, de juridiske forpligtelser, der pålægges dataansvarlige og straf ved overtrædelse, har essentiel betydning for udenlandske virksomheder, der kommer ind på det europæiske marked, navnlig Alibaba Group.

7.1. Ekstraterritorial virkning af Databeskyttelsesforordningen

Forordningens artikel 3, stk. 1 tilsigter, at så længe den registeransvarlige eller processoren har en virksomhed i EU, og behandlingen af personoplysninger er inden for sit forretningsområde, skal den registeransvarlige eller processoren overholde forordningen, uanset hvor den virkelige behandling af aktiviteterne forekommer.

Begrebet *etablering* bør forstås bredt, så længe det effektivt behandler personoplysninger i forbindelse med virksomhedens mål, kan eksempelvis et kinesisk kontor på EU-markedet med kun én medarbejder betragtes som etablering i denne forstand.[155]

[154] Jf. Forordningens definition på Koncernvirksomhed i forordningens artikel 4, litra 19)
[155] *Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law*, Adopted on 16 December 2010, at page 11.

Endvidere bestemmer artikel 3, stk. 2, at den registeransvarlige eller processoren, der behandler personoplysninger i de registrerede i Unionen, skal overholde forordningen på to betingelser uanset om der er etableret en virksomhed i Unionen. De to betingelser omfatter, at 1) udbud af varer eller tjenesteydelser til sådanne registrerede i EU, uanset om der er behov for betaling af den registrerede 2) overvågning af brugernes adfærd, så længe deres adfærd finder sted inden for EU. Denne klausul er et af højdepunkterne i forordningen og er af stor betydning for de kinesiske virksomheder, især for internetfirmaer, der har til hensigt at gøre mere forretning i EU. Databeskyttelsesforordningen finder anvendelse på Alibaba Group, jf. for. art. 3, da den er målrettet mod EU-markedet eller overvåger EU-brugernes browsingaktiviteter.

7.2. Bred fortolkning af personoplysninger

Forordningens artikel 4 bestemmer, at personoplysninger er de oplysninger, som enten allerede har identificeret en fysisk person eller har mulighed for at gøre det direkte eller indirekte. Forordningen fortolker i vid udstrækning begrebet personoplysninger og hvad der betragtes som personoplysninger inden for forordningens anvendelsesområde. AliExpress anvender ikke kun transaktionsoplysningerne fra brugere, som for eksempel bankkonto, adresser og kontaktoplysninger. Disse betragtes som personlige data, men nogle internetdata som IP-adresse og enhedsidentifikatorer kan også identificeres som personlige data. For at afgøre, om visse data kan identificeres, skal alle midler, der med rimelighed forventes anvendt, tages i betragtning, således, at dataene ikke skal ses adskilt fra andre data, der er indehaver af den registeransvarlige eller processoren.

7.3. Tunge juridiske forpligtelser, der pålægges dataansvarlige eller processor

Forordningen leverer principperne om lovlighed, retfærdighed og gennemsigtighed, begrænsning af formål, data minimering, nøjagtighed, lagringsbegrænsning, integritet og fortrolighed samt ansvarlighed for behandling af personoplysninger og giver de registrerede ret til information og adgang, ret til berigtigelse ret til overførsel, ret til at

blive glemt, ret til begrænsning af forarbejdning, ret til begrænsning af profilering mv. En datakontroller eller processor skal respektere principperne og bistå de registrerede med at realisere deres rettigheder. Desuden skal dataansvarlige eller processorer omfatte privatlivets fred ved at udføre konsekvensvurderingen, udpege databeskyttelsesansvarlige eller repræsentanter og overholde personoplysningernes krænkelses- og underretningsansvar, for at mindske risikoen for krænkelse af privatlivets fred eller begrænse den skade, der er forårsaget af data-emner ved overtrædelser af privatlivets fred.

7.4. Tung straf

En tilsynsmyndighed kan beslutte at undersøge den registeransvarlige eller processoren alene eller efter at have modtaget den registreredes klage, og hertil afgøre, om der skal træffes en administrativ sanktion, og også træffe bødebeløbet fra sag til sag. Artikel 83 i forordningen fastsætter forskellige standarder for forskellige retsakter. For eksempel skal den dataansvarlige eller processoren, der ikke vedtager ordentlige tekniske eller forvaltningsmæssige foranstaltninger for at undgå eller mindske privatlivets overtrædelsesrisiko, blive bødet med 10.000.000 Euro eller 2 pct. af den globale omsætning, alt efter hvad der er højest. Den registeransvarlige eller processoren, der overtræder de grundlæggende principper for behandling af personoplysninger eller ikke beskytter den registreredes rettigheder, bødes med 20.000.000 Euro eller 4 pct. af den globale omsætning, alt efter hvad der er højest. Bortset fra tilsynsmyndigheden kan de registrerede også søge retsmidler mod dataansvarlige eller dataprocessorer og har hertil ret til, at blive kompenseret.

8. Alibaba-case - Anvendelse af EU-domme

I retspraksis binder domme som udgangspunkt dommens parter, men domme kan dog i nogle tilfælde skabe en retstilstand, som andre bliver bundet af fremover, således at dommene kan anvendes som en retskilde, jf. retskildelæren om regulering, retspraksis, samt retssædvaner og forholdets natur, hvor der ingen rangorden er. Inden for EU-ret gælder således *primær ret* og *sekundærret*, jf. afhandlingens afsnit 1.5.1. Domme kan

skabe ret eller understøtte ret, og domme kan ligeledes anvendes som retskilde i de tilfælde hvor der ikke er regulering eller hvor reguleringen ikke er klar og tydelig, som for eksempel ved generalklausuler. Domme anvendes ofte som retskilde sammen med andre typer af retskilder, herunder lovregler, men kan også fungere som selvstændige retskilder.[156] Endvidere kan domme danne præcedens.[157] Hvis en sag danner præcedens, vil den påvirke fremtidige retstilstand således, at domstolene tager hensyn til tidligere afsagte domme ved afgørelsen af en sag.[158]

Præjudikatværdien i en dom er dét forhold, hvor det vurderes hvor meget vægt der kan tillægges dommen som retskilde.[159] Jo højere præjudikatværdi, desto mere værdifuldt bliver det, at anvende dommen.[160] Ved vurdering af en doms præjudikatværdi skal dommen løse et generelt juridisk problem, for hvis problemet er for specifikt, kan dommen ikke med samme sandsynlighed anvendes som retskilde, *ratio decendi*. Endvidere bør dommens alder betragtes, da retstilstanden kan have ændret sig i forhold til ældre domme. Man bør således undersøge om der er kommet nyere domme som passer ind i forhold til samfundets udvikling. Ligeledes må enigheden eller dissens blandt dommere undersøges, for jo mere enighed blandt dommerne, jo større præjudikatværdi. Sidst har det også betydning hvor dommen kommer fra, byret, Landsret eller Højesteret, for jo højere domstol, jo større præjudikatværdi.

Der kan være argumenter for og imod anvendelse af domme som retskilder. Domme kan for det første være proces- og appelbesparende, og for det andet kan de styrke befolkningens tillid til Retten, og for det tredje skaber domme retfærdighed, altså lighed for loven. Disse er forholde som taler for anvendelse af domme som retskilder. Forholde der taler imod anvendelse af domme som retskilder består i for det første samfundsmæssig forandring, der skaber grunde til at ændre praksis, og for det andet kan domme forskyde fokus fra konkret til generel tvistløsning, og for det tredje kan domme forskyde magtfordelingen, ved at domstolene bliver lovgivningsskabende.

---

[156] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 178-180)
[157] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 178)
[158] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 196)
[159] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 180)
[160] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 180)

I analysen vil Österreichischer-sagens gennemtrængende præmisser blive anvendt til at understøtte anvendelsen af både Schrems-sagen og Google Spain-sagen igennem Alibaba-analysen. Endvidere vil generaladvokaternes udtalelser blive anvendt til at understøtte EU-Domstolens udtalelser som findes væsentlige i forhold til Alibaba-casen, og endvidere til at skabe diskussion, hvis generaladvokaterne altså har udtrykt uenighed i forholdet hertil.

Ved anvendelse af udtalelser fra generaladvokaterne, kan der skabes nuance i diskussionen om kendelserne i EU-Domstolene. Udtalelserne indeholder ofte mere omfattende teoretiske diskussioner end Domstolens domme. [161] Retskildeværdien i generaladvokaternes udtalelser kan være tvivlsomme[162], hvorfor de i analysen blot vil anvendes til at belyse andre synspunkter og overvejelser ved analysen af Alibaba-casen.

9. Alibaba-casen - Österreichischer-sagen, C-465/00

Denne sag vedrørte en pligt i østrigsk ret, som offentlige institutioner, der er undergivet Rechnungshofs (den østrigske rigsrevision) revision, havde til at give meddelelse om de indkomster og pensioner over en bestemt størrelse, som de udbetalte til deres ansatte og tidligere ansatte, samt om modtagernes navne med henblik på udarbejdelse af en årsberetning, der skulle forelægges for Nationalret (Nationalrådet), Bundesrat (Forbundsrådet) og for Landtagen (delstatsparlamenterne) og stilled til rådighed for offentligheden.

Domstolen fandt, at formålet med den østrigske ordning, navnlig at lægge pres på offentlige institutioner for at få dem til at holde lønningerne inden for rimelighedens grænser, var legitimt såvel i henhold til Databeskyttelsesdirektivets artikel 6, stk. 1, litra b), om at oplysninger kun må indsamles til udtrykkeligt angivne og legitime formål, og anførte endvidere, at det var op til den forelæggende domstol at efterprøve, om offentliggørelsen var nødvendig og stod i rimeligt forhold til dette formål, samt at

[161] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 192)
[162] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 192)

undersøge, om et sådant formål ikke kunne opfyldes lige så effektivt ved mindre indgribende midler.

Domstolen udtalte endvidere, at hvis en bestemmelse om behandling af personoplysninger er uforenelig med EMRK artikel 8, om retten til respekt for privatliv og familieliv, så kan bestemmelsen heller ikke opfylde proportionalitetskravet i direktivets artikel 6, stk. 1, litra c) og artikel 7, litra c) og e).

Således fremgår af sagens præmis 68, at bestemmelserne i direktiv 95/46, for så vidt de omhandler behandling af personoplysninger, der kan krænke de grundlæggende frihedsrettigheder og navnlig privatlivets fred, nødvendigvis skal fortolkes under hensyntagen til grundrettighederne, som ifølge fast retspraksis hører til de almindelige retsgrundsætninger, Domstolen skal beskytte.

Præjudikatværdien i Österreichischer-sagens findes, at vægte meget højt, da sagen anvendes i både Schrems-sagen og Google Spain-sagen, hvor der henvises navnlig i forhold til spørgsmålet om overholdelse af princippet om privatlivets fred og de grundlæggende frihedsrettigheder, jf. EMRK art. 8. EU-Domstolen praktiserer dog ikke *stare decisis* doktrin, altså, at EU-domstolens domme ikke er bindende præjudikater for den selv, hvorfor Domstolen hen ad vejen kan udtale sig modsættende i kommende lignende sager, eventuelt som følge af samfundets udvikling. Dette er i forhold til, at sagen er fra 2003, og der sidenhen har sket udvikling i forhold til teknologi og den øgede vækst i datastrømme.

Sagen har dog været anvendt en del i både Google Spain-sagen og i Schrems-sagen, som er henholdsvis fra maj 2014 og oktober 2015. Der er altså minimum 11 år fra Österreichischer-sagen til de to andre domme, hvor der har været store udviklinger i både teknologien og selve anvendelsen af teknologien. Det er navnlig sagens præmis 68 om fortolkningen af Databeskyttelsesdirektivet, der skal overholde princippet om de grundlæggende rettigheder og især privatlivets fred, der anvendes og nævnes i Schrems-sagens præmis 38 og Google Spain-sagens præmis 68, hvor de netop pointerer, at Databeskyttelsesdirektivets indhold skal fortolkes under hensyntagen til de grundlæggende rettigheder, som endvidere er sikret ved chartrets artikel 8.

Det må således fastslås, at præjudikatværdien i Österreichischer-sagen vægtes meget højt, navnlig i forhold til sagens præmis 38, som er flittigt anvendt i andre sager, herunder Schrems-dommen og Google Spain-dommen. Dette skal endvidere ses i lyset af, at dommen er fra 2003, så sagen er forholdsvis gammel. Det er bemærkelsesværdigt, nærmere i forhold til de problemstillinger der opstår ved beskyttelsen af fysiske personers private oplysninger og udviklingen i teknologien og hertil strømme af personoplysninger på tværs af landegrænser, herunder videregivelse til tredjelande. I forbindelse hermed kan det dog statueres, at dommens præmis 38 pointerer og fastsætter hvor vigtig og grundlæggende EMRK artikel 8 og chartrets artikel 8 er i forhold til fortolkningen af Databeskyttelsesdirektivets indhold.

10. Alibaba-case - Google Spain-sagen, C-131/12

I sag C-131/12, Google Spain, dom af 13. maj 2014, har EU-Domstolen fastslået, at der ikke skal meget til, før der er tale om behandling af personoplysninger, der foretages *som led i en virksomheds aktiviteter*, når en dataansvarlig i et tredjeland etablerer en filial eller et datterselskab i en medlemsstat, når aktiviteterne hos henholdsvis den dataansvarlige og henholdsvis filialen eller databehandleren er uløseligt forbundne.[163] I sagen fandt EU-Domstolen bl.a., at databeskyttelsesdirektivets artikel 4, stk. 1, litra a), skal fortolkes således, at en behandling af personoplysninger foretages som led i aktiviteter, der inden for en medlemsstats område udføres af en dataansvarligs virksomhed eller organ som omhandlet i bestemmelsen, når en søgemaskineudbyder etablerer en filial eller et datterselskab i en medlemsstat, der skal sørge for reklame og salg af reklameplads i søgemaskinen, og hvis aktivitet er rettet mod indbyggerne i denne medlemsstat.[164]

Google Spain-sagen anvendes i analysen til at belyse begreberne, som oplistet i dommens indledning, da disse vurderes til at have særligt relevans i forhold til afhandlingens problemstilling, med særlig henblik på Alibaba-casen, hvor begreberne vil blive anvendt analogt. Dommens problemstilling er anderledes fra Alibaba-casen og altså

[163] Sag C-131/12, Google Spain, præmis 50-60
[164] Sag C-131/12, Google Spain, præmis 60

afhandlingens problemstilling. Principperne, der er afklaret i dommen, stemmer dog overens i forhold til principperne der ønskes afklaret, jf. afhandlingens problemformulering.[165] De opstillede principper omhandler Databeskyttelsesdirektivets materielle og territorielle anvendelsesområde, behandling af oplysninger på websider, oplysningernes pålidelighed, samt grundlaget for behandling af oplysninger. Dommen behandler endvidere principperne om *Den registreredes indsigelsesret* og *Tilsynsmyndighed*, men dette vil ikke anvendes i denne del af analysen, da de behandles nærmere i kapitel 6 og videre i kapitel 12 i analysen ved Schrems-dommen.

Analysen understøttes af Österreichischer-dommen, der omhandler overholdelse af princippet om privatlivets fred og de grundlæggende frihedsrettigheder, jf. chartrets artikel 8, jf. endvidere EMRK artikel 8.

Afhandlingen vil endvidere anvende opbygningen i EU-Domstolens redegørelse, samt til at opstille faktuelle omstændigheder der gøres gældende i forhold til Alibaba Group og dattervirksomhederne, navnlig forholdet imellem dattervirksomhederne i Unionen og USA, og føres videre til analysen ved Schrems-dommen i næste kapitel.
Det materielle anvendelsesområde for direktiv 95/46 vil blive behandlet som det første i forholdet om Alibaba Groups og dennes internationale hjemmeside Alibaba.com. Endvidere vil *behandling af personoplysninger*, samt *registeransvarlig* blive uddybet nærmere, og ligeledes vil begrebet om *websideudbyder uddybes*, som dommen anvender ved sammenligning over for *søgemaskineudbyder*.

De faktiske omstændigheder består i Alibaba Group, som er moderselskabet, der endvidere har hjemsted i Kina, og det amerikanske datterselskab Alibaba Cloud, udbyder Cloud Computing Service, hvor koncernens indsamlede oplysninger oplagres, samt handelsplatformen Alibaba.com og datterselskaberne på Det Europæiske Unions marked, hvorfra der skabes forbindelse mellem det Europæiske marked ud til det globale marked, herigennem internetsiden, Alibaba.com.

[165] Jf. Afhandlingens *Problemformulering*

Alibaba.com indekserer på en sådan måde hvor en bruger kan have søgt på nogle bestemte varer, og herudfra indekseres på varegrupper eller lignende, der er direkte henvendt hjemmeside-brugeren. Hermed anvendes personoplysningerne til at opsnappe og analysere brugerens præferencer. På den internationale hjemmeside er der således global adgang, og der er da også nederst på hjemmesiden mulighed for at søge mere europæisk lokalt gennem den tyske version af hjemmesiden, samt den franske og hollandske m.v.[166] I og med at det amerikanske datterselskab Alibaba Cloud er en virksomhed, der udbyder *Database Services*[167] sammenholdt med at Alibaba Cloud LLC og Alibaba.com LLC *de facto* er registreret hos US Privacy Shield, og dermed indgået aftale med EU, formodes det, at Alibaba.com indsamler og oplagrer oplysninger i USA.

Det udledes i direktivets artikel 3, om anvendelsesområde, at direktivets anvendelsesområde finder anvendelse på behandling af personoplysninger ved hjælp af edb, jf. dir. art. 3, stk. 1, jf. endvidere for. art. 2, stk. 1 om automatisk databehandling. Hertil udledes forholdene om, hvorvidt direktivet finder anvendelse på datterselskaber der er etableret i en medlemsstat, og videregiver disse til en et andet datterselskab og/eller moderselskabet, når disse er etableret uden for Den Europæiske Union, selvom samarbejdet foregår på frivilligt grundlag.

Direktivets artikel 2, litra b) udleder, at *behandling af personoplysninger* er defineret som *"enhver operation eller række operationer – med eller uden brug af elektronisk databehandling – som personoplysninger gøres til genstand for…"*. dette stemmer overens med forordningens definition i artikel 4, litra 1) og litra 2). Domstolen har, jf. dommens præmis 26, allerede haft lejlighed til at fastslå, at en operation, der består i at lægge personoplysninger ud på en internetside, skal anses for en *"behandling"* som omhandlet i direktivets artikel 2, litra a). Denne præmis har relevans i forhold til Alibaba.com, når en EU-borger anvender hjemmesiden og lægger personoplysninger ud ved at oprette profil til et login. Det skal bemærkes, at man på hjemmesiden ligeledes kan "logge ind" via sin Facebook-konto, Google-konto, Linked-in-konto, eller Twitter-konto

[166] https://www.alibaba.com/?spm=a2700.7787031.a371k.8.9DhAUv
[167] https://www.alibabacloud.com/?utm_content=se_658817&gclid=EAIaIQobChMIrdLIkr3V2gIV1LgbCh2pCAiVEAAYASAAEgLmN_D_BwE

og det vil stadig have relevans, hvis altså brugeren har lagt oplysninger op af sig selv på de nævnte kontoer i henhold til definitionen i direktivets artikel 2, litra a) og forordningens artikel 4, litra 1) om *personoplysninger*.[168]

Alibaba.com er ikke en type søgemaskine som dommens omhandlede søgemaskine i Google-search. De har dog dét til fælles, at de er globale udbydere, men hertil ligger forskellen imellem dem, at Google-search er en søgemaskineudbyder, der er egnet til at indeksere websider fra hele verden, således at der på metodisk og systematisk vis identificeres og opstøves indhold af websider, og lagres midlertidigt på servere, hvorimod Alibaba.com er til som en handelsplatform, der indekserer varer og reklamer til profil-brugeren, ud fra hvad brugeren har søgt efter på hjemmesiden. Google Search som søgemaskineudbyder er mere omfattende idet oplysninger gøres tilgængelige for enhver internetbruger, end den behandling som Alibaba.com foretager, i og med handelsplatformen foretages på en internetside. De har dog alligevel nogle grundlæggende fællestræk i henhold til direktiv 95/46, særligt i henhold til direktivets artikel 2, litra b), da de begge på elektronisk vis, henholdsvis som søgemaskineudbyder og som handelsplatform, indsamler personoplysninger, jf. art. 2, litra a), som de begge dernæst *"selektionerer"*, *"registrerer"* og *"systematiserer* "inden for rammerne af sine indekseringsprogrammer, *"opbevarer* "på sine servere og i givet fald *"videregiver* "og *"overlader"* til sine brugere respektive.[169]

I henhold til direktivets definition af *den registeransvarlige* i artikel 2, litra d) og *dataansvarlige* i henhold til forordningens definition i artikel 4, litra 7), og i henhold til dommens præmis 33, så er Alibaba.com omfattet af definitionen i og med, at aktivitetens formål er afgjort i, at indsamlingen, samt oplagring, af personoplysningerne er til, for at internetbrugere, altså brugere af Alibaba-platformen, kan have en konto på platformen til brug af handel på internetsiden. Således er det formålet med og hjælpemidlerne til den behandling af personoplysninger, som udgøres af Alibaba.com, der afgør, at udbyderen anses for at være *"registeransvarlig"* i henhold til nævnte artikel 2, litra d), jf. dommens præmis 33.

[168] Definitionen er nærmere uddybet i kapitel 5
[169] Jf. endvidere sag C-131/12, pr. 28

I og med at aktiviteten på internetsiden på Alibaba.com i henhold til artikel 2, litra b) og d), i henhold til forordningens artikel 4, litra 1) og litra 2) sammenholdt med litra 7), består i at samle oplysninger, indeksere disse, lagre dem, vil Alibaba.com's aktivitet kvalificeres som *behandling af personoplysninger*, som omhandlet i dir. artikel 2, litra b) og for. art. litra 2), når oplysningerne indeholder personoplysninger i henhold til dir. art. 2, litra a) og for. art. 4, litra 1), og endvidere vil Alibaba.com som værende handelsplatform, hvor registrering af oplysninger foregår, anses for at være *registeransvarlig* som omhandlet i direktivets artikel 2, litra d) og forordningens artikel 4, litra 7).

Det kan diskuteres hvor omfattende aktiviteterne på Alibaba.com er, i forhold til dommens omhandlede Google Search, der søgemaskineudbyder i henhold til dommens præmis 35, er mere omfattende i forhold til den behandling, som foretages af websideudgivere. Alibaba.com har dog både websider, der direkte henvender sig til EU-borgere gennem den tyske version[170], hvor der på forsiden er en reklame, der direkte henvender sig til de tyske kunder med en ung model, der er klædt i tysk traditionel folkedragt, og med to glas øl i hænderne, hvor man som webside-besøgende straks associerer til den tyske *Oktoberfest*. Endvidere den italienske version[171], hvor der på forsiden reklameres med en ung model klædt i sommertøj, det italienske flags farver er anvendt, med vin og druer, samt oste i baggrunden, således at den webside-besøgende straks associerer til den italienske sommer. Alibaba.com i sig selv er den internationale version på engelsk[172], hvorpå reklamerne er meget neutrale i forhold til den tyske version, henholdsvis den italienske version. Endvidere har Alibaba.com websider, der henvender sig direkte til USA, Indien, Tyrkiet, mv., således at Alibaba.com når vidt omkring globalt. Det formodes, at Alibaba.com's platform ikke er lige så omfattende som Google Search, i og med at Google Search udbydes som søgemaskine, og Alibaba.com derimod udbydes som en kæde af websider. Alibaba.com, altså platformen i sig selv, når dog ud til sine aktuelle kunder, samt mulige kunder, på global plan, hvorfor det vurderes, at

[170] Alibaba.com Germany: https://germany.alibaba.com/index.html
[171] Alibaba.com Italy: https://italy.alibaba.com/index.html
[172] https://www.alibaba.com

aktiviteterne, altså behandling af kunders personoplysninger, på websiden og i Alibaba.com-koncernen ligeledes kan vurderes som værende omfattende, som det udledes i dommens præmis 35, dog ikke i så væsentlig grad som Google Search.

Det udledes i dommens præmis 38, at en søgemaskines aktivitet *i forhold til* websideudgiveres aktivitet *i væsentligt større og yderligere grad* kan påvirke de grundlæggende rettigheder til privatlivets fred og beskyttelse af personoplysninger. Ud fra sammenligningen, har Domstolen altså indirekte dermed udledt, at websidegiveres aktivitet ligeledes kan påvirke *de grundlæggende rettigheder til privatlivets fred og beskyttelse af personoplysninger*, hvorfor Alibaba.com ligeledes i sin egenskab af den person, som afgør formålet med aktiviteten og hjælpemidlerne hertil, *inden for rammerne af sit ansvar, sine kompetencer og sine muligheder sikre, at den opfylder kravene i direktiv 95/46*, jf. dommens præmis 38. Dette er med henblik på, at de garantier som direktivet fastsætter i overensstemmelse med chartrets artikel 7 og 8, der tilstræber at beskytte EU-borgerens grundlæggende rettighed i forhold til privatlivets fred, samt beskyttelsen af personoplysninger, i forhold til at opnå en effektiv og fuldstændig beskyttelse af de berørte EU-borgere, rent faktisk kan gennemføres, jf. dommens præmis 38. I henhold til dette, er generaladvokaten ligeledes enig, jf. forslagets pkt. 40, der udleder, at udgiveren af websider, der indeholder personoplysninger, navnlig indtastningen af brugerprofil, er registeransvarlig for behandlingen af personoplysninger i direktivets forstand. Dette findes endvidere i overensstemmelse i forordningens forstand, sådan at udgiveren bliver bundet af alle de forpligtelser, som forordningen pålægger dataansvarlige.[173]

I forhold til dommens præjudikatværdi må det fastslås, at dommens problemstilling er snæver, men udleder trods alt undersøgelse af forholdene om en registeransvarlig i forhold til websider, register på websider, navnlig EDB-register, og endvidere forholdet om koncernvirksomheders repræsentanter i EU, når moderselskabet selv er registreret i et tredjeland uden for EU- og EØS-samarbejdet.

[173] Forslag til afgørelse fra generaladvokat N. Jääskinen, fremsat den 25. juni 2013, sag C-131/12

I Schrems-dommen pointeres præmis 53, 66 og 74 i Google Spain-dommen, hvori forholdet om beskyttelsen af fysiske personers grundlæggende rettigheder belyses i henhold til behandlinger på eksempelvis websider, hvorfor dommen kan anvendes til problemstillingen i forhold til afhandlingens Alibaba-case og andre lignende sager hvad angår behandling af personoplysninger ved hjælp af EDB-data, og hvorfor endvidere, at præjudikatværdien vægtes højt.

Det kan udledes af analysen via Google-Spain sagen, at Alibaba Groups dattervirksomheder, der er etableret i henholdsvis England, Tyskland, mv. i henhold til direktivets artikel 4, stk. 1, litra a) sammenholdt med forordningens artikel 4, litra 1), litra 2), foretager behandling af personoplysninger som led af aktiviteter, der inden for Unionens område udfører virksomhed, som registeransvarlig/ dataansvarlig i henhold til direktivets artikel 2, litra d) sammenholdt med forordningens artikel 4, litra 7), i og med at websideudbyderen har etableret datterselskaber inden for Unionen, der skal sørge for reklamer og salg direkte henvendt til EU-borgere.

11. Alibaba-case - Schrems-sagen, C-362/14

Den 6. oktober 2015 afsagde EU-Domstolen dom i sag C-362/14, også kendt som Schrems-sagen, eller Facebook-sagen [174] . EU-Domstolen afgjorde heri, at EU-Kommissionens Safe Harbour-principper vedrørende overførsel af personoplysninger til USA er ugyldige.

Sagen begyndte, da den østrigske statsborger Maximillian Schrems klagede over Facebook til det irske datatilsyn. Baggrunden for klagen var Edward Snowdens afsløringer omkring overførsel af EU-borgernes personoplysninger til USA. Internetvirksomheder, som for eksempel Facebook, opbevarer en stor del af deres personoplysninger på servere i USA. Dette betyder konkret, at NSA[175] dermed fik adgang

[174] Afhandlingen anvender "Schrems-sagen" som reference.
[175] National Security Agency er en af USA's sikkerhedstjenester (efterretningstjenester). NSA har især til opgave at aflytte, indsamle og analysere alle former for kommunikation. Afhandlingen vil ikke gå nærmere i dybden med NSA, nærmere information kan forefindes på hjemmesiden: https://www.nsa.gov

til EU-borgeres personoplysninger gennem PRISM[176] overvågningsprogram. Det irske datatilsyn besluttede ikke at undersøge sagen, som var indgivet af M. Schrems, på grund af de eksisterende Safe Harbor-principper, hvorfor endvidere, at M. Schrems indbragte datatilsynets beslutning for den øverste irske retsinstans, High Court of Ireland. High Court bad efterfølgende EU-Domstolen om en præjudiciel afgørelse om, hvorvidt de nationale tilsynsmyndigheder var bundet af EU-Kommissionens afgørelse, sådan at, tilsynsmyndighederne ikke kan indlede behandling ved henvendelse fra EU-borgere.

Som almindelig internet bruger kan det være svært at gennemskue rammerne for internettet. Heri menes, at lige så snart en EU-borger afgiver enhver form for data, som for eksempel personoplysninger[177], kan det være svært for brugeren at kontrollere hvortil personoplysningerne måtte føres hen. Som Persondataforordningens 6.- og 7. præambel udtrykker det, så skaber den hastigt udviklende teknologi en masse udfordringer, da omfanget af indsamling, samt delingen af personoplysninger er steget betydeligt. Teknologien giver mulighed for såvel private selskaber som for offentlige myndigheder, at udnytte personoplysninger i hidtil uset omfang.

Helt konkret kan udfordringen ligge i, at hvis EU-virksomheder videresender oplysninger til tredjelande, uanset om det er for opbevaring eller til et moderselskab, at vurdere om et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, som svarer til EU's. I forhold til de forskellige nationers, altså tredjelandes, juridiske aspekter, samt fortolkninger af *at værne om privatlivets fred*, kan selve vurderingen, samt de aftaler som Kommissionen som for eksempel indgår, også skabe tvivl hos EU-borgerne. Tvivlen, som kan være iblandt EU-borgerne, er da senest i 2015 kommet til udtryk, netop i Schrems-sagen. Kommissionens indgåede aftale med USA, der har været baseret på Safe Harbor-principperne, blev da fundet som værende ugyldige af EU-Domstolen.[178]

[176] PRISM-programmet (Planning Tool for Ressource Integration, Synchronization, and Management-programmet), jf. præmis 22 i Screms-sagen. For nærmere uddybelse henvises til Kommissionens meddelelse KOM(2013) 847 endelig, der indeholder Kommissionens nærmere behandling og undersøgelse af Safe Habor-ordningens funktion.
[177] Personoplysninger defineret i henhold til Databeskyttelsesdirektivets art. 2, litra a, sammenholdt med Persondataforordningens art. 4, litra 1.
[178] Sag C-362/14

Sag C-362/14 anvendes analogt til afhandlingens Alibaba-case med henblik på at gå nærmere i dybden med problematikken i overførsel af personoplysninger som i udgangspunktet er fra EU til et usikkert tredjeland, uden for EU- og EØS-samarbejde, og endvidere vil forholdet om EU-borgernes mulighed for at påberåbe sig i henhold til dette, ligeledes blive behandlet nærmere. Forholdet om EU-borgernes klageadgang i tredjelandsforholde vægtes meget højt, da problemformuleringen netop lægger op til at få afklaret om hvorvidt *den kommende Persondataforordning har en reel beskyttende virkning på EU-borgernes personoplysninger ved overførsel af disse til tredjelande uden for EU?*

Schrems-dommen er afsagt i henhold til Databeskyttelsesdirektivet, som på daværende tidspunkt var gældende lov, og hvor Databeskyttelsesforordningen endnu ikke var vedtaget.[179] Afhandlingen vil således anvende Persondataforordningens bestemmelser i forhold til Alibaba-casen, således at der opstår en parallel anvendelse ved objektiv formålsfortolkning imellem direktivets artikler og forordningens artikler, jf. Centros-sagen, C-212/97, præmis 15.[180]

Endvidere understøttes analysen af Österreichischer-dommen, der omhandler overholdelse af princippet om privatlivets fred og de grundlæggende frihedsrettigheder, jf. chartrets artikel 8, jf. endvidere EMRK artikel 8.

Casen anvendes altså ved at læne sig op ad Schrems-dommen, dog ligger der en forskel i, at det i Schrems-dommen er nærmere omhandlet Safe-Habor-ordningen, da USA's beskyttelsesniveau undersøges, og EU-U.S. Privacy Shield siden juli 2016 har været gyldig. Safe-Harbor-ordningen er af dommen blevet ugyldiggjort, hvorfor den ikke længere finder anvendelse, men derimod er Privacy Shield-aftalen vedtaget pr. 12.07 2016, som dermed finder gyldighed i forhold til Alibaba-casen. Afhandlingen går dog ikke nærmere i dybden med Privacy Shield-aftalen, som anført i afgrænsningen[181], hvorfor den udelukkende anvendes som et gyldigt faktum.

[179] Databeskyttelsesforordningen, (EU) 2016/679, blev vedtaget pr. 27. april 2016
[180] Christina D. Tvarnø & Ruth Nielsen, Retskilder og retsteorier (2014, s. 256)
[181] Jf. *Afgrænsning* i afsnit 1.3.

De faktuelle omstændigheder der opstilles i Alibaba-casen er som i problemstillingen i Schrems-dommen, navnlig overførsel af personoplysninger i forholdet mellem et datterselskab der er stiftet inden for EU og modeselskabet, der er etableret i *et tredjeland*. I Alibaba-casen er datterselskaber oprettet i forskellige EU-medlemsstater[182], disse dækker over flere lande, og moderselskabet ligger i Kina, samt et mellemled, Alibaba Cloud, der er etableret i USA, således at datterselskaberne og moderselskabets forhold ren juridisk består[183]. Datterselskaberne gør det muligt for det kinesiske moderselskab at drive virksomhed inden for det Europæiske Unions marked, og hvor mellemleddet i USA gør det muligt for koncernen, at overføre personoplysninger fra EU til USA, hvor Cloud-virksomheden altså modtager helt eller delvist, samt opbevarer oplysningerne på servere, beliggende i USA.[184]

Dét forhold, at en EU-borger lægger sine personoplysninger ud på Alibaba.com er ikke en problemstilling i sig selv, hvis EU-borgeren i henhold til dir. 95/46 art. 7, litra a), har afgivet samtykke til *behandling af personoplysninger*, jf. endvidere for. art. 6, stk. 1, litra a). Problemstillingen, der kan opstå, ligger i dét forhold, hvor oplysningerne *overføres til tredjelandet*, USA. Problemstillingen bliver da nærliggende hvis der er tale om overførsel til et tredjeland, der i henhold til Kommissionen ikke er defineret som værende et land med tilstrækkeligt beskyttelsesniveau ved behandling af personoplysninger. I forlængelse hermed, opstår ligeledes spørgsmålet om hvorvidt EU-borgeren, hvis denne betvivler tredjelandets beskyttelsesniveau i henhold til EU's, kan opnå hjælp, således at beskyttelsen i praksis tilnærmelsesvis stemmer overens med den teoretiske beskyttelse, der forefindes i lovgivningen. Med hensyn til *tilnærmelsesvis* menes, at personoplysninger kan være anvendt i legitimt øjemed i henhold til for. art. 6, stk. 4, men vil ikke behandles nærmere, da Alibaba.com ikke kan henføres til at udføre webhandelsvirksomhed der, jf. endvidere for. art. 23, stk. 1, udgør en nødvendig og

[182] U.K. Office (U.K., Ireland and Norics), Italy Office (Italy, Spain, Portugal and Greece), Germany Office (Germany, Austria, Switzerland, Turkey and Eastern Europe), The Netherlands Office (The Netherlands, Belgium and Luxembourg):
http://www.alibabagroup.com/en/contact/offices
[183] Forholdet består via EU-US Privacy Shield-aftalen
[184] Jævnfør kapitel 7 formodes det, at Alibaba Cloud opbevarer EU-borgeres personoplysninger i overensstemmelse med EU-US Privacy Shield.

forholdsmæssig foranstaltning af hensyn til statens sikkerhed eller den offentlige sikkerhed mv., men derimod indsamles personoplysninger i erhvervsøjemed.

I overensstemmelse med Schrems-sagens præmis 27, så har enhver, der har bopæl på EU's område, og som ønsker at anvende Alibaba.com, er i forbindelse med sin registrering forpligtet til at indgå en aftale med Alibaba.com[185], henholdsvis tyske-, italienske- eller hollandske hjemmeside, som er datterselskaber til Alibaba Group Holding Limited, der selv har hjemsted i Kina. Personoplysningerne vedrørende Alibaba brugere, som har bopæl på Unionens område, overføres helt eller delvist til servere, der tilhører Alibaba Cloud LLC, også under Alibaba Group, og som befinder sig i USA, hvor de er genstand for en behandling. Spørgsmålet, der opstår i denne forbindelse er, om de nationale tilsynsmyndigheder, i henhold til artikel 28 i direktivet og endvidere i henhold til forordningens artikel 51, er fuldstændig bundet af en konklusion i en fællesskabsundersøgelse, navnlig EU-US Privacy Shield, der af Kommissionen er vedtaget i henhold til direktivets artikel 25, stk. 6, endvidere i henhold til forordningens artikel 45, der udtaler at USA's lovgivning og praksis indeholder tilstrækkelig beskyttelse for datasubjekter, der indeholder EU-borgers personoplysninger, når disse overføres til USA og gøres til genstand for behandling.

Det skal som det første udredes, at direktiv 95/46 skal fortolkes i overensstemmelse med de grundlæggende rettigheder, som er sikret ved Den Europæiske Menneskerettighedskonvention, også kaldet chartret, jf. Schrems-dommen, C-362/14, præmis 38, jf. endvidere domme Österreichischer Rundfunk m.fl., C-465/00, C-138/01 og C-139, EU:C:2003:294, præmis 68, Google Spain og Google, C-131/12, EU:C:2014:317, præmis 68, og Ryneš, C-212/13, EU:C:2014:2428, præmis 29. Det fremgår af direktivets artikel 1, samt betragtning 2 og 10, at direktivet har til formål at sikre en effektiv og fuldstændig beskyttelse af EU-borgeres frihedsrettigheder og grundlæggende rettigheder, særligt retten til respekt for privatlivet i forbindelse med behandling af personoplysninger, og hertil har direktivet også til formål at sikre et højt beskyttelsesniveau af netop disse frihedsrettigheder samt grundlæggende rettigheder, jf.

[185] Man kan på Alibaba.com hjemmesiden vælge forskellige versioner af hjemmesider, henholdsvis international, tysk, italiensk eller hollandsk, m.fl.: https://www.alibaba.com

Schrems-dommens præmis 39. Dertil har EU-Domstolen i praksis fremhævet betydningen af såvel EU-borgeres grundlæggende ret til respekt for privatlivet, som er sikret ved chartrets artikel 7, som den grundlæggende ret til beskyttelse af personoplysninger, der er sikret ved chartrets artikel 8, jf. dommens præmis 39, jf. endvidere dommen Google Spain og Google, C-131/12, EU:C:2014:317.

Dernæst må det vurderes i henhold til direktivets artikel 28 og forordningens artikel 51, hvor medlemsstaterne har pligt til at drage omsorg for, at der udpeges en eller flere offentlige myndigheder, hvilke beføjelser disse har i forbindelse med overførsel af personoplysninger. Det udledes i nævnte artikels, stk. 1, at tilsynsmyndigheden har i fuld uafhængighed pligt til at påse overholdelsen af Unionens regler om beskyttelse af fysiske personer i forbindelse med behandling af sådanne oplysninger. Hvis en EU-borger påberåber sig i henhold til nævnte artikel, er det således tilsynsmyndighedens pligt i medlemsstaten, jf. tilsynsmyndighedens beføjelse i dir. 95/46, art. 28, stk. 3, pind 1, at *iværksætte undersøgelser og bl.a. have adgang til de oplysninger, der gøres til genstand for en behandling og til at indsamle alle oplysninger, der er nødvendige for at varetage dens tilsynsopgaver*, jf. endvidere for. art. 57 om tilsynsmyndighedernes opgaver, for netop at fyldestgøre kravet i chartrets artikel 8, stk. 3 der tilsigter, at beskytte den grundlæggende ret til respekt for privatlivet, der er sikret ved chartrets artikel 7, samt den grundlæggende ret til beskyttelse af personoplysninger, der er sikret ved chartrets artikel 8, ved hjælp af en uafhængig myndigheds kontrol.

Artikel 28-myndighedernes *uafhængighed* er altafgørende i dén henseende, at Databeskyttelsesdirektivets formål skal fortolkes i henhold til chartrets artikel 8 om beskyttelse af personoplysninger, hvorfor oprettelsen har til formål, at sikre et effektivt og pålideligt tilsyn med overholdelse af reglerne i direktivet med henblik på, at styrke netop beskyttelsen af personer og organer, der måtte blive berørt af myndighedernes afgørelser, jf. Schrems-dommens præmis 41. Dette stemmer endvidere overens med direktivets 62. betragtning. Beskyttelsen skal da sikres i ligevægt imellem overholdelsen af den grundlæggende ret til respekt for privatlivet og overholdensen af de hensyn, der styrer den frie udveksling af personoplysninger, jf. dommens præmis 42.

I henhold til dir. artikel 28, stk. 1 og stk. 6 og endvidere for. art. 51, stk. 1 sammenholdt med art. 55 om tilsynsmyndighedens kompetence på egen medlemsstatsområde, afhænger tilsynsmyndighedernes beføjelser endvidere af i hvilken medlemsstat, der er foretaget behandling af personoplysninger. Således kan det diskuteres hvorvidt, medlemsstaternes tilsynsmyndigheder har beføjelse til at iværksætte undersøgelse hvis der er foretaget behandling af personoplysninger i et tredjeland uden for EU- og EØS-samarbejdet, når det af den nævnte artikel fremgår, at den nationale tilsynsmyndighed er *kompetent til på sin medlemsstats område*, jf. art. 28, stk. 6, 1. pkt, jf. endvidere forordningens art. 55, stk. 1. Det fremgår dog af direktivets artikel 2, litra b), at den transaktion der forekommer ved *"videregivelse ved transmission, formidling eller enhver anden form for overladelse"* er omfattet af direktivets definition af *behandling af personoplysninger*, endvidere i forordningens artikel 3, stk. 1, at forordningens territoriale anvendelsesområder ligeledes finder anvendelse på behandling af personoplysninger af en dataansvarlig som er etableret i Unionen, uanset om behandlingen finder sted i Unionen eller ej. . I henhold til dommens præmis 47, og sammenholdt med direktivets artikel 25, der udleder medlemsstaternes beføjelse til at fastsætte nærmere bestemmelse om videregivelse af personoplysninger til tredjelande, hvis tredjelandet sikrer et tilstrækkeligt beskyttelsesniveau, udledes det således, at de nationale tilsynsmyndigheder er *"tillagt beføjelse til at undersøge, om en videregivelse af personoplysninger fra den medlemsstat, som myndighederne henhører under, til et tredjeland overholder de ved direktiv 95/46 fastsatte krav*", jf. endvidere chartrets art. 8, stk. 3, samt direktivets art. 28, og forordningens artikel 51.

Generaladvokaten [186] har da udtrykt sig i forslagets pkt. 92, at til trods for at en tilstrækkelighedsbeslutning fra Kommissionen er at tillade overførsel af personoplysninger til det pågældende tredjeland, så er det ikke ensbetydende med, at EU-borgere ikke længere kan indbringe klager for tilsynsmyndighederne med henblik på at beskytte deres personoplysninger. Generaladvokaten var således enig i, at EU-borgere adgang til at indbringe klager for tilsynsmyndighederne skulle modtages og behandles til

[186] Forslag til afgørelse fra generaladvokat Y. Bot, fremsat den 23. september 2015 i Sag C-362/14

trods for en gyldig tilstrækkelighedsbeslutning fra Kommissionen, netop med henblik på at beskytte deres personoplysninger, der måtte være overført til et tredjeland.

Da det kan konstateres at de nationale tilsynsmyndigheder er pålagt beføjelse til at undersøge de forhold der måtte opstå ved overførsel af personoplysninger til tredjelande, indleder dette til at undersøge princippet om videregivelse af personoplysninger til tredjelande.

Det fremgår af direktivets 56. betragtning, at det er anerkendt, at videregivelse af personoplysninger fra Unionens medlemsstater til tredjelande er nødvendig af hensyn til udbygningen af den internationale samhandel. Sammenholdt med princippet om, at en sådan videregivelse kun må finde sted hvis tredjelandet sikrer et tilstrækkeligt beskyttelsesniveau, som opstillet i direktivets artikel 25, stk. 1, og i henhold til forordningens artikel 44, er det særligt interessant at undersøge, hvorvidt Alibaba.com har hjemmel til at overføre EU-borgernes personoplysninger fra EU til deres servere i USA.

Hertil fremgår det i direktivets artikel 25, stk. 1 sammenholdt med stk. 2 og stk. 3, endvidere i henhold til forordningens artikel 45, stk. 2 sammenholdt med stk. 4 om Kommissionens overvågning af tredjelandes løbende udvikling , at medlemsstaterne og/eller Kommissionen er pålagt at undersøge og kontrollere tredjelandes beskyttelsesniveau, hvortil EU-borgeres personoplysninger bliver gjort til genstand ved overførelse.

Kommissionen kan altså udstede afgørelse om tredjelandes beskyttelsesniveau i henhold til artikel 25, stk. 6 og i henhold til forordningens artikel 45, stk. 2, hvor medlemsstaterne i forlængelse hermed har pligt til at træffe foranstaltninger, der er nødvendige for at efterkomme afgørelsen, jf. dommens præmis 51. Dommens præmis 51 udleder endvidere, at Kommissionens afgørelse i overensstemmelse med TEUF artikel 288, stk. 4, er bindende for alle de medlemsstater, den er rettet til, herunder samtlige tilhørende organer, i det omfang som den bevirker, at der gives tilladelse til videregivelse af

personoplysninger fra medlemsstaterne til det af afgørelsen omfattede tredjeland, herunder USA.

Udgangspunktet er således, at de nationale tilsynsmyndigheder skal følge Kommissionens afgørelse [187] i henhold til Privacy Shield-Framework, hvortil Alibaba.com har indgået en gyldig aftale i forhold til de amerikanske myndigheder. Der gælder i princippet en formodning om, at EU-institutionernes retsakter er gyldige, og derfor afføder retsvirkninger, jf. dommens præmis 52. Endvidere findes afgørelsen gyldig, så længe EU-Domstolen ikke har fastslået den som værende ugyldig, hvorfor de uafhængige tilsynsmyndigheder ikke kan vedtage foranstaltninger, der er i strid med Kommissionens gennemførelsesafgørelse.

En gyldig afgørelse fra Kommissionen kan dog ikke forhindre EU-borgere i at indgive en anmodning til de nationale tilsynsmyndigheder, hvis deres personoplysninger er blevet til eller kan blive videregivet et tredjeland. Dette er i henhold til direktivets artikel 28, stk. 4 om beskyttelse af deres rettigheder og frihedsrettigheder i forbindelse med behandlingen af oplysningerne, jf. endvidere forordningens artikel 77 hvor enhver registreret har ret til at indgive klage til en tilsynsmyndighed, sammenholdt med forordningens artikel 57, litra f) at tilsynsmyndigheden har pligt til at behandle klager der indgives af en registrere. Endvidere er der ikke anført en undtagelse til direktivets artikel 28, stk. 4, hvorfor tilsynsmyndighedernes beføjelser i forhold til behandling af en EU-borgers anmodning bestyrkes yderligere, hvad angår Kommissionens afgørelser i henhold til direktivets artikel 25, stk. 6, jf. dommens præmis 55.

Hertil fremgår det af Domstolens faste praksis, jf. dommens præmis 60, at Unionen er en retsunion, hvorfor enhver retsakt fra institutionerne er undergivet kontrol med at værende forenelig med traktaterne, de generelle retsprincipper, samt de grundlæggende rettigheder, hvorfor endvidere, at Kommissionens afgørelse i (EU) 2016/1250 ikke kan undslippe en sådan kontrol, jf. direktivets artikel 25, stk. 6. Det er dog EU-Domstolen, som har enekompetence til at fastslå en sådan ugyldighed.[188]

[187] Kommissionens gennemførelsesafgørelse (EU) 2016/1250
[188] Jf. kapitel 2 om EU-institutionerne

Det kan således konstateres, at det påhviler de nationale uafhængige tilsynsmyndigheders pligt, at behandle en anmodning, når den indgives af en EU-borger, hvis personoplysninger er blevet, eller kan blive videregivet til et tredjeland, der har været genstand for Kommissionens afgørelse i (EU) 2016/1250, hvis altså EU-borgerens anmodning er begrundede i henhold til chartrets artikel 8, stk. 3 og artikel 47, sammenholdt med direktivets artikel 28, stk. 3, jf. dommens præmis 63-65. Dette stemmer endvidere overens med bestemmelsen i forordningens artikel 57, litra f) om tilsynsmyndighedernes pligt til at behandle pågældende registreredes klage.

I Schrems-dommen behandler EU-Domstolen ligeledes Safe Harbor-ordningen. EU-Domstolen afgjorde således, at Safe Harbor-principperne vedrørende overførsel af personoplysninger til USA som værende ugyldige, jf. dommens præmis 104 og Domstolens kendelse nr. 2.

Det centrale spørgsmål var, om de amerikanske retsregler omkring opbevaring af personoplysninger kunne betragtes som værende *tilstrækkelige* i forhold til beskyttelsesniveauet i Unionens Databeskyttelsesdirektiv. Safe Harbor-ordningens beskyttelsesniveau kunne ikke findes tilstrækkeligt, hvorfor USA som tredjeland, på baggrund af ordningen, heller ikke kunne findes som værende tredjeland der sikrer et tilstrækkeligt beskyttelsesniveau, og videregivelse af personoplysninger til landet måtte forbydes, jf. direktivets 57. præambel.

Safe Harbor-principperne blev kendt som værende ugyldige på baggrund af, at de ikke indeholdte et tilstrækkeligt beskyttelsesniveau, fordi det kræver ”klare og præcise regler, som regulerer rækkevidden og anvendelsen af et sådant indgreb og pålæg af minimum sikkerhedsforanstaltninger, således at de personer, hvis personoplysninger er omhandle, har tilstrækkelig garanti for, at deres oplysninger reelt er beskyttet mod risiko for misbrug og mod ulovlig tilgang til og brug af sådanne oplysninger”, jf. dommens præmis 91. Dommens præmis 91 sammenholdt med præmis 90, der udleder, at ”de berørte personer ikke rådede over administrative eller retlige midler, der kunne gøre det muligt for dem at få adgang til de oplysninger, der vedrørte dem, og til i givet fald at få disse berigtiget eller slettet”, hvorfor Safe Harbor-principperne ikke kunne kendes gyldige.

Heraf konkluderede afgørelsen for det første, at Safe Harbor-principperne var ugyldige, men at de nationale tilsynsmyndigheder oveni, ikke var forhindrede i, at undersøge et krav om beskyttelse af personoplysninger, selvom EU-Kommissionens afgørelse tillader en sådan videregivelse.

Afgørelsen om Safe Habor-princippernes ugyldighed har sidenhen ført til, at en ny aftale imellem EU og USA er trådt i kraft på, indtil videre, gyldige grundlag. EU-U.S. Privacy Shield som trådte i kraft august 2016, er en aftale mellem EU og USA, der blandt andet fastsætter et sæt af databeskyttelsesregler og sikkerhedsforanstaltninger, som de amerikanske virksomheder, der tilslutter sig ordningen, er forpligtet til at overholde. Således har Kommissionen fundet i gennemførelsesafgørelsen (EU) 2016/1250, at USA sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra EU til foretagender i USA under EU's og USA's værn om privatlivets fred, jf. gennemførelsesafgørelsens artikel 1, stk. 1.

Hvad angår forholdet om USA som et tredjeland, kan således konstateres i henhold til Kommissionens afgørelse, jf. dir. art. 25, stk. 1, 2 og 6 sammenholdt med dir. art. 31, stk. 2, at være et *sikkert tredjeland*, jf. endvidere (EU) 2016/1250, art. 1, stk. 1 om EU-U.S-Privacy Shield aftalen. Alibaba.com kan derfor på lovligt grundlag, videreføre personoplysninger til afdelingen i USA med henblik på opbevaring af oplysningerne, når de alminelige betingelser for lovlig behandling af personoplysninger ligeledes overholdes i henhold til direktivets kapitel II, og endvidere i forordningens kapitel II om principperne for behandling af personoplysninger, navnlig principperne om lovlighed, rimelighed og gennemsigtighed overholdes, og endvidere principperne om personoplysningernes rigtighed overholdes. Endvidere kan lovligheden styrkes i henhold til forordningens artikel 6 om lovlig behandling, hvor Alibaba.com stilles til ansvar som den *dataansvarlige*, som Alibaba.com således er forpligte til at følge, ud fra profil-brugernes samtykke på Alibaba.com websiden, jf. for. art. 1, stk. 1, litra a).

Præjudikatværdien i Screms-dommen kan være svært at vurdere, i og med at dommen er forholdsvis ny. Dommen fik da konstateret, at uanset Kommissionens beslutning om et tredjeland som værende et *sikkert tredjeland*, så skal tilsynsmyndigheder behandler

klager fra EU-borgere når disse er begrundet i vedkommendes tvivl om tredjelandet tilstrækkelighed af beskyttelsesniveau på området om personoplysninger. Dette skal ses i lyset af at Den Europæiske Unions Charter om Grundlæggende Rettigheder, navnlig artikel 8 vægtes gennemtrængende ved fortolkning af Databeskyttelsesforordningen.

12. Konklusion

Analysearbejdet i afhandlingen har vist, at forordningen i vidt omfang svarer til den gældende retstilstand efter Databeskyttelsesdirektivet med tilhørende praksis fra EU-Domstolen og Datatilsynet. Forordningens centrale bestemmelser om anvendelsesområde, definitioner, principper for behandling af personoplysninger, behandlingsregler, de registreredes rettigheder og behandlingssikkerhed stemmer i stort omfang til gældende ret efter Databeskyttelsesdirektivet.

Derudover indeholder forordningen bestemmelser, som er en nyskabelse i forhold tiden gældende retstilstand. Dette er eksempelvis bestemmelserne om databeskyttelsesrådgivere, konsekvensanalyse og fortegnelser over behandlingsaktiviteter, samt en udtrykkelig bestemmelse om "data protection by design".

Afhandlingens analyser er baseret på eksisterende retskilder. Hvor retstilstanden ikke kan anses entydig, skal de nationale domstole og de uafhængige myndigheder hente svar gennem praksis som den har været indtil nu. Det må forventes, at fortolkningen af forordningen på flere punkter i de kommende år vil blive udviklet gennem praksis fra bl.a. det med forordningen nyoprettede Europæiske Databeskyttelsesråd, EU-Domstolen, de nationale domstole, samt de nationale Datatilsyn. Den nuværende retstilstand er f.eks. baseret på meget få domme, og det må forventes, at der fremover vil komme flere domme fra bl.a. EU-Domstolen. I det omfang, der kommer bindende afgørelser fra EU-Domstole, nationale domstole, Databeskyttelsesrådet og den uafhængige tilsynsmyndighed mv., skal de nationale lovgivere analyser naturligvis læses i lyset af den nye praksis.[189]

[189] Afhandlingens kapitel 5

Ifølge artikel 288 i Traktaten om den Europæiske Unions Funktionsområde er der forskel på, om et område harmoniseres ved et direktiv eller en forordning. Det følger af TEUF artikel 288, 3. pkt., at et direktiv med hensyn til det tilsigtede mål er bindende for enhver medlemsstat, som det rettes til, men overlader det til de nationale myndigheder, at bestemme form og midler for gennemførelsen. Det indebærer blandt andet, at et direktiv som indeholder rettigheder og pligter for borgerne og virksomhederne, skal gennemføres enten ved lov eller ved en bekendtgørelse med hjemmel i lov, jf. afhandlingens kapitel 5.

Til forskel fra et direktiv er en forordning ifølge TEUF artikel 288, 1. og 2. pkt., almengyldig, og er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat. En forordning virker således som en lov i medlemsstaterne, og den glæder i den form, som den er vedtaget, og den må som udgangspunkt ikke gennemføres i national ret. Medlemsstaternes kan således ikke udstede bindende fortolkningsregler, selv om forordningen måtte give anledning til tvivl.[190] Medlemsstaterne vil imidlertid kunne udstede vejledninger, der efter deres karakter ikke er bindende, men blot anvendes til belysning ved tvivl.

Ud over at en forordning som udgangspunkt ikke må gennemføres i medlemsstaterne, vil medlemsstaternes modstridende lovgivning blive fortrængt af en forordning, hvorfor det vil være nødvendigt at ophæve denne lovgivning således, at der ikke opstår nogen usikkerhed om retstilstanden. Ophævelsen skal ske enten ved lov eller ved bekendtgørelse med hjemmel i lov.

Som følge af databeskyttelsesforordningens almengyldighed vil forordningen som udgangspunkt fortrænge de nationale regler, der regulerer de samme forhold som forordningen. Medlemsstaterne, som for eksempel Danmark, er dermed forpligtet til at indrette national lovgivning i overensstemmelse med forordningens bestemmelser med virkning fra den 25. maj. Der er imidlertid en række undtagelser i databeskyttelsesforordningen til dette udgangspunkt, idet visse regler i forordningen bestemmer, at medlemsstaterne inden for nærmere bestemte områder enten skal eller kan fastsætte nationale regler.

[190] Afhandlingens kapitel 5

Det kan udledes af analysen via Google-Spain dommen, at Alibaba Groups dattervirksomheder, der er etableret i henholdsvis England, Tyskland, mv. i henhold til direktivets artikel 4, stk. 1, litra a) sammenholdt med forordningens artikel 4, litra 1), litra 2), foretager behandling af personoplysninger som led af aktiviteter, der inden for Unionens område udfører virksomhed, som registeransvarlig/ dataansvarlig i henhold til direktivets artikel 2, litra d) sammenholdt med forordningens artikel 4, litra 7), i og med at websideudbyderen har etableret datterselskaber inden for Unionen, der skal sørge for reklamer og salg direkte henvendt til EU-borgere.

Ud fra analysen via Schrems-dommen kan det konkluderes, at det påhviler de nationale uafhængige tilsynsmyndigheders pligt, at behandle en anmodning, når den indgives af en EU-borger, hvis personoplysninger er blevet, eller kan blive videregivet til et tredjeland, der har været genstand for Kommissionens afgørelse i (EU) 2016/1250, hvis altså EU-borgerens anmodning er begrundede i henhold til chartrets artikel 8, stk. 3 og artikel 47, sammenholdt med direktivets artikel 28, stk. 3, jf. dommens præmis 63-65. Dette stemmer endvidere overens med bestemmelsen i forordningens artikel 57, litra f) om tilsynsmyndighedernes pligt til at behandle pågældende registreredes klage.

Ved at Alibaba Groups datterselskab Alibaba.com og Alibaba Cloud har tiltrådt aftalen i henhold til EU-U.S. Privacy Shield, jf. endvidere Kommissionens (EU) 2016/1250, kan Alibaba således opretholde lovligheden i overførsel af persondata fra EU til USA.[191] Så længe de europæiske datterselskaber i henhold til Kinas manglende oplistning som værende et *sikkert tredjeland*, findes det ulovligt for disse datterselskaber, at overføre EU-borgeres personoplysninger til Alibaba Group i Kina. Lovligheden opretholdes dog ved overførsel til afdelingen i USA gennem EU-U.S. Privacy Shield, jf. afhandlingens kapitel 5.Alibaba.com kan derfor på lovligt grundlag, videreføre personoplysninger til afdelingen i USA med henblik på opbevaring af oplysningerne, når de alminelige betingelser for lovlig behandling af personoplysninger ligeledes overholdes i henhold til

[191] På Privacy Shield websiden er Alibaba.com og Alibaba Cloud oplistet som værende tiltrådt EU-USA aftalen, således at overførsler landene imellem er på lovligt grundlag: https://www.privacyshield.gov/participant_search

direktivets kapitel II, og endvidere i forordningens kapitel II om principperne for behandling af personoplysninger, navnlig principperne om lovlighed, rimelighed og gennemsigtighed overholdes, og endvidere principperne om personoplysningernes rigtighed overholdes. Endvidere kan lovligheden styrkes i henhold til forordningens artikel 6 om lovlig behandling, hvor Alibaba.com stilles til ansvar som den *dataansvarlige*, som Alibaba.com således er forpligte til at følge, ud fra profil-brugernes samtykke på Alibaba.com websiden, jf. for. art. 1, stk. 1, litra a).[192]

Som afsluttende del af konklusionen, kan det således konkluderes, at Databeskyttelsesforordningens ikrafttrædelse vil have forbedrende virkning for EU-borgernes beskyttelse af personoplysninger, særligt ved overførsel til tredjeland uden for EU- og EØS-samarbejdet. Til trods for at EU vægter det internationale samarbejde- og samhandel meget højt, så vægtes EU-borgernes sikkerhed i forhold til privatlivets fred og særligt beskyttelse af personoplysninger også meget højt. Dette skal ses i lyset af, at Forordningens indhold skal fortolkes i henhold til *Chartrets* artikel 8, stk. 1 om de grundlæggende rettigheder.
Ud fra forordningens kommende virkning, herunder harmoniseringen af lovgivningen om databeskyttelse, sammenholdt med forordningens artikel 77, at EU-borgere har ret til at indgive klage til en tilsynsmyndighed, vil forordningen skabe en forbedring i beskyttelse af EU-borgeres rettigheder, jf. afhandlingens kapitel 6. Dette er endvidere i forhold til forordningens artikel 79, der giver EU-borgeren adgang til effektive retsmidler over en dataansvarlig, særligt i forhold til casen, vil den registrerede således kunne indgive en klage til en tilsynsmyndighed, jf. artikel 77, hvor endvidere den registrerede skal have adgang til effektive retsmidler. Dette stemmer således overens med Chartrets artikel 47, der udleder retten til effektive retsmidler, samt adgang til en upartisk domstol, som værende en grundlæggende rettighed.[193]

13. Perspektivering

[192] Afhandlingens kapitel 11
[193] Afhandlingens kapitel 5

I konklusionen findes det frem til, at EU-lovgivningen fra Databeskyttelsesdirektivet til Databeskyttelsesforordningen vil forbedre og styrke beskyttelsen af EU-borgeres personoplysninger ved at harmonisere lovgivningen, så medlemsstaterne får én lovgivning at fortolke ud fra ved fremtidige sager om overførsel af oplysninger til tredjelande, navnlig usikre tredjelande.

I henhold til Schrems-dommens udfald er det særligt interessant at EU-Domstolen har afgjort at Kommissionens gennemførelsesafgørelse om Safe Harbor-ordningen som værende ugyldig, da dette indikerer, at til trods for, at afgørelser og udtalelser fra EU institutioner udsteder i tro om at overholde fortolkningen i henhold til Chartret, at dette ikke nødvendigvis findes som værende gyldigt i henhold til EU-Domstolen.[194] Særligt i forhold til den verserende sag om Donald Trumps præsidentkampagne, der kørte i 2014/2015, hvor det undersøges hvorvidt påstandene om brug af personoplysninger gennem Facebook, uden tilladelse fra de registrerede, til netop at fremme succes i præsidentkampagnen. Oplysningerne påstås at være blevet anvendt til analyse af de amerikanske borgere, særligt dem som forventedes ikke at stemme personligt på Trump, at der blev sendt reklamekampagner der kunne have en stærk indflydelse på ændringen af vælgernes præferencer.[195]
Det er særligt interessant i forhold til hvordan sagen vil ende, og om det endvidere vil have indflydelse inden for EU-regi og lovgivningen i forhold til personoplysninger, databeskyttelse og endvidere overførsel af personoplysninger til USA, og andre tredjelande uden for EU- og EØS-samarbejdet. Herunder menes særligt forholdet om EU's pligt ved vurdering og afgørelse om tredjelandes beskyttelsesniveau, hvor der muligvis kan pålægges yderligere tyngende vurderingskriterier. Det er ikke sikkert at EU finder det nødvendigt, at stramme vurderingskriterierne yderligere, men at man derimod forventer, at Forordningens indhold vil kunne opretholde EU's beskyttelse af EU-borgeres grundlæggende rettigheder i forhold til behandling af personoplysninger og endvidere overførsel af disse til tredjelande uden for EU- og EØS-samarbejdet.

[194] Sag C-362/14
[195] http://www.bbc.com/news/world-us-canada-43444791 og http://www.bbc.com/news/uk-43450127

14. Litteraturliste

14.1. Bibliografi

Retskilder og Retsteorier; Christina Tvarnø og Ruth Nielsen; Jurist- og Økonomforbundets Forlag (2014); 4. udgave, 1. oplag, København K

Få styr på metoden – Introduktion til juridisk metode og samfundsvidenskabelig projektmetode; Christina Tvarnø & Sarah Maria Denta; Ex Tuto Publishing A/S (2015); 1. udgave, 1. oplag, København

EU ret; Ulla Neergaard & Ruth Nielsen; Karnov Group A/S (2016); 7. udgave/1. oplag, København

Liberalising Trade in the EU and the WTO – A legal comparison; Sanford E. Gaines, Birgitte Egelund Olsen and Karsten Engsig Sørensen; Cambridge University Press (2012), Cambridge, United Kingdom

14.2. Retskilder

14.2.1. EU-ret

Lovgivning

Den Europæiske Unions Charter om Grundlæggende Rettigheder (2010/C 83/02)

Europa-Parlamentets og Rådets Forordning (EU) 2016/679, af 27. april 2016, om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse), (EØS-relevant tekst)

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

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV 2006/123/EF af 12. december 2006 om tjenesteydelser i det indre marked

Kommissionen

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET om udveksling og beskyttelse af personoplysninger i en globaliseret verden
http://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52017DC0007&from=EN

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
http://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016D1250&from=EN

KOMMISSIONEN NYE STYREFORMER I EU – EN HVIDBOG
KOM(2001) 428 endelig, (2001/C 287/01)
https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52001DC0428&from=DA

14.3. EU-domme og afgørelser

Sag C-362/14: Domstolens Dom (Store afdeling), 6. oktober 2015: »Præjudiciel forelæggelse – personoplysninger – beskyttelse af fysiske personer i forbindelse med behandling af disse oplysninger – Den Europæiske Unions charter om grundlæggende rettigheder – artikel 7, 8 og 47 – direktiv 95/46/EF – artikel 25 og 28 – videregivelse af personoplysninger til tredjelande – beslutning 2000/520/EF – videregivelse af

personoplysninger til USA – utilstrækkeligt beskyttelsesniveau – gyldighed – klage fra en fysisk person, hvis oplysninger er blevet videregivet fra Unionen til USA – de nationale tilsynsmyndigheders beføjelser«
I sag C-362/14, angående en anmodning om præjudiciel afgørelse i henhold til artikel 267 TEUF, indgivet af High Court (Irland) ved afgørelse af 17. juli 2014, indgået til Domstolen den 25. juli 2014, i sagen: Maximillian Schrems mod Data Protection Commissioner, procesdeltager: Digital Rights Ireland Ltd.

Forslag til afgørelse fra Generaladvokat Y. Bot fremsat den 23. september 2015, Sag C-362/14: Anmodning præjudiciel afgørelse indgivet af High Court of Ireland (Irland)

Forenede sager C-293/12 og C-594/12: »Elektronisk kommunikation – direktiv 2006/24/EF – offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet – lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af sådanne tjenester – gyldighed – artikel 7, 8 og 11 i Den Europæiske Unions charter om grundlæggende rettigheder«

Forenede sager C-465/00, C-138/01 og C-139/01: »angående en anmodning, som henholdsvis Verfassungsgerichtshof (sag C-465/00) og Oberster Gerichtshof (sag C-138/01 og C-139/01) (Østrig) i medfør af artikel 234 EF har indgivet til Domstolen for i de for nævnte retter verserende sager, (…)
at opnå en præjudiciel afgørelse vedrørende fortolkningen af 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 (EFT L 281, s. 31)«

Sag C-131/12: »Personoplysninger – beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger – direktiv 95/46/EF – artikel 2, 4, 12 og 14 – materielt og territorialt anvendelsesområde – søgemaskiner på internettet – behandling af oplysninger på websider – søgning i samt indeksering og lagring af disse oplysninger – ansvaret for udbyderen af søgemaskinen – virksomhed eller organ på en medlemsstats

område – rækkevidden af udbyderens forpligtelser og den berørte persons rettigheder – Den Europæiske Unions charter om grundlæggende rettigheder – artikel 7 og 8«

Forslag til afgørelse fra Generaladvokat N. Jääskinen fremsat den 25. juni 2013, Sag C-131/12: Anmodning om præjudiciel afgørelse indgivet af Audiencia Nacional (Spanien)

14.4. Artikel 29-gruppen, de europæiske datatilsyn

Adequacy Referential (WP 254 rev.01, 18/EN), Article 29 Working Part, adopted on 6 February 2018

14.5. Hjemmesider

EU-persondataforordningens betydning i forbindelse med markedsføring
https://www.itgovernance.eu/blog/dk/eu-persondataforordningens-betydning-i-forbindelse-med-markedsforing/

Persondataforordningen kommer – Hvad gør man? – Guide til virksomheder
http://www.horesta.dk/da-DK/Nyheder%20og%20Politik/Nyheder/Nyhedsarkiv/2017/08/~/media/Filer/Nyhedsarkiv/2017%202/Guide2%20(3).ashx

Data flows – Allowing free trade agreements to strengthen the GDPR
https://www.mannheimerswartling.se/globalassets/publikationer/data-flows.pdf

Persondataforordningen: Er du klar til de nye regler?
https://universe.ida.dk/tema/persondataforordningen/

Artikel: Hvordan påvirker EU-persondataforordningen dansk lovgivning?
https://www.bdo.dk/da-dk/faglig-info/advisory-publikationer/forensic-assurance/hvordan-paavirker-eu-persondataforordningen-dansk?utm_source=Facebook&utm_campaign=persondata&utm_content=retargeting

Trade in Services Agreement, TiSA:
http://ec.europa.eu/trade/policy/in-focus/tisa/

Report of the 21st TiSA negotiation round 2-10 November 2016:
http://trade.ec.europa.eu/doclib/docs/2016/november/tradoc_155095.pdf

14.6. Justitsministeriet/ Datatilsynet/ Folketingets EU-Oplysning

Vejledning om overførsel af personoplysninger til tredjelande, af Erhvervsstyrelsen, Digitaliseringsstyrelsen, Justitsministeriet og Datatilsynet

Vejledning om de registreredes rettigheder, af Datatilsynet (marts 2018)

Vejledning om Databeskyttelsesforordningen – En introduktion til de kommende, nye regler om beskyttelse af personoplysninger (oktober 2017)

Betænkning om Databeskyttelsesforordningen (2016/679) – og de retlige rammer for dansk lovgivning, Betænkning nr. 1565, af Justitsministeriet

Datatilsynet: Persondataloven – Hvilke oplysninger må registreres? Hvad må oplysningerne bruges til? Hvordan kontrollerer du oplysningerne?
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Persondatalovspjece/Persondatalovspjece.pdf

Databeskyttelse i EU
http://www.eu.dk/da/fakta-om-eu/politikker/telekommunikation/databeskyttelse

Data-flow
There are little to no multilaterally-agreed trade riles to ensure such predictability for cross-border data flows.

In the absence of such rules, legislators in each jurisdiction are free to adopt domestic laws that – either intentionally or unintentionally – restrict cross-border data flows to or from other countrues. Governments may introduce such restrictions for a variety of reasons, such as the protection of personal data or national security.
https://www.mannheimerswartling.se/globalassets/publikationer/data-flows.pdf

2018 EU Trade, Regulatory and Competition Trends _ Sheppard Mullin Richter & Hampton LLP – JDSupra
https://www.jdsupra.com/legalnews/2018-eu-trade-regulatory-and-67526/

2016C11_bdk_scm
https://www.swp-berlin.org/fileadmin/contents/products/comments/2016C11_bdk_scm.pdf

Bech-Bruun_Morgenmøde vedr Persondataforordning VM
http://www.bechbruun.com/~/media/Files/Videncenter/Kursusmateriale/2016/Bech-Bruun_Morgenm%C3%B8de+vedr+Persondataforordning+VM.pdf

How will the new European data protection reform impact Chinese companies
file:///C:/Users/mj/Downloads/How%20will%20the%20new%20European%20data%20protection%20reform%20impact%20Chinese%20companies.pdf

Have we passed peak data protection
https://www.dataiq.co.uk/blog/have-we-passed-peak-data-protection

datadigitalc17notes_e
https://www.wto.org/english/res_e/reser_e/datadigitalc17notes_e.pdf

Alibaba Group_ The Impact of GDPR on China's Enterprises _ HEFFELS SPIEGELER ADVOCATEN
http://spiegeler.com/alibaba-gdpr-china-privacy/

Data Protection In Europe_ GDPR Looms For Digital Finance & eCommerce
http://blog.mondato.com/gdpr/

GDPR matchup_ China's Cybersecurity Law
https://iapp.org/news/a/gdpr-matchup-chinas-cybersecurity-law/

New China Data Privacy Standard Looks More Far-Reaching than GDPR _ Center for Strategic and International Studies
https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr