Forord

Denne afhandling er udarbejdet på Aalborg Universitet, Cand.Merc.Jur uddannelsens 10. Semester, og er dermed min kandidatafhandling.

Harvard metoden er brugt til notation af kilder i afhandlingen: [forfatter/organisation, årstal, sidetal]. Kilder angivet før punktum henviser til foregående sætning, mens kilder angivet efter punktum henviser til foregående afsnit.

Der skal gives en stor tak til min vejleder Charlotte Bagger Tranberg for at stå til rådighed, også uden for de afsatte timer, samt for den sagkyndige vejledning.

Afhandlingen behandler de juridiske problemstillinger, der opstår ved overførsler af personoplysninger fra Danmark og andre EU-lande til et land uden for EU og EØS samarbejdet. Særligt herunder analyseres virkningen af en foreliggende aftale mellem EU og USA kaldet "'Safe Harbor", om behandlingen af personoplysninger ved overførsel af disse til USA.

1 Indledning

De færreste er klar over, hvor meget deres dagligdag berøres af persondataretten. Vi registrer på daglig basis vore personlige data hos virksomheder, organisationer og sågar, når vi går på offentlige overvågede gader. Specielt ved færdsel på Internettet registreres tusinder og atter tusinder af oplysninger om brugerne. Disse oplysninger er reguleret på EU niveau af databeskyttelsesdirektivet[1] og i Danmark gennem persondataloven[2], som har til formål, at sikre at disse oplysninger ikke bliver misbrugt på en sådan måde, at det kommer den registrerede brugers privatliv til skade.

Inden for EU har virksomheder, som registrerer persondata, således en lang række forpligtigelser, de skal tage højde for både ved behandlingen og ikke mindst overdragelsen af informationerne til tredjepart.

Specielt vedrørende overførelse af persondata til lande uden for EU, eller det, der i denne sammenhæng kaldes tredjelande, opstår der en masse komplikationer. Størstedelen af disse lande yder nemlig ikke et tilsvarende beskyttelsesniveau for den registrerede. Dette kan føre til integritetskrænkelser, markedsføringsmæssig misbrug af oplysningerne og identitetstyveri.

Nutidens omfattende kommunikationsmuligheder via Internettet har gjort overførsler af denne type let tilgængelige. Der kan derfor være langt fra den teoretiske beskyttelse direktivet yder og til

[1] RDir 95/46/EF
[2] Lov 2000-05-31 nr. 429 om behandling af personoplysninger

den faktiske beskyttelse, der opnås af EU borgernes oplysninger, specielt når det vedrører overførsler via internettet.
Nogle af de meget udbredte tjenester, hvor disse problemstillinger opstår, er de såkaldte sociale netværk, hvor millioner af mennesker deler deres personlige oplysninger med resten af netværket. Når denne type hjemmesider oprettes uden for EU, betyder det, at man som EU-borger overdrager dataen til et tredjeland. Brugeren fraskriver sig i denne sammenhæng ofte de rettigheder, de har gennem direktivet.

Området med overførsler til tredjelande er efterhånden karakteriseret som en klassisk problemstilling i persondataretten, da der stadig forekommer stor uklarhed, om hvorledes denne type databehandling skal håndteres.
I en verden hvor globalisering og internationalisering stadig er voksende, udgør persondata en meget vigtig ressource, og er derfor et område der tildeles større og større opmærksomhed, da beskyttelsens reelle effekt formindskes i takt med den teknologiske udvikling.
Man har i det seneste årti arbejdet meget på at undgå kommercielle barrierer for udveksling af denne type data mellem EU og resten af verdenen. Specielt overfor USA har der været fokus herpå, da USA udgør et meget vigtigt marked. Derfor har man, specielt til det amerikanske marked, lavet en ordning der hedder Safe Harbor, der har til formål at begrænse disse barrierer.

1.1 Problemformulering

Har direktivet 95/46/EF en reel beskyttende virkning på EU borgernes personoplysninger, ved overførsel af disse til tredjelande, og er *safe harbor*-ordningen en garanti for et tilsvarende beskyttelsesniveau, ved dataoverførsler til USA?

1.2 Afgrænsning

I denne afhandling vil de grundlæggende principper i persondataretten blive gennemgået. Dog kun i det omfang, at det har relevans for forståelsen af de problemstillinger, der opstår ved overførsler af persondata til tredjelande, og dermed bidrager til forståelse af problemformuleringen.
For yderligere at afgrænse afhandlingen, er koncentrationen rettet mod den private sektor. Dette skyldes at, den konkrete problemformulering i denne afhandling særligt vedrører de online dataoverførsler, der sker fra private i Danmark og EU til virksomheder og organisationer i udlandet. Dette betyder ikke, at reglerne for det offentlig ikke vil blive berørt. Dog kun i det omfang, at det er nødvendigt for forståelsen af persondatarettens principper.RDir 2002/58/EF om behandling af personoplysninger i den elektroniske kommunikationssektor, er et direktiv, der er vedtaget, som et supplement til Databeskyttelsesdirektivet. Det er dog primært rettet mod telesektoren, og er dermed ikke relevant i forhold til denne afhandlings problemformulering, og på samme grundlag undladt heri.

2 Metode

2.1 Retskilder og litteratur

Afhandlingen er udarbejdet ved hjælp af tre typer retskilder. Lovgivning, retspraksis og ikke mindst administrativ praksis. Lovgivningsmæssigt berører emnet både national-, EU- og folkeret i form af persondataloven, databeskyttelsesdirektivet og Den Europæiske Menneskerettighedskonvention (EMRK). Nogle få sager ender ved domstolene, men langt de fleste sager kommer ikke længere end til den administrative praksis, som i Danmark varetages af Datatilsynet. Der vil ligeledes blive anvendt udtalelser og andre skrivelser fra Datatilsynet, ligesom skrivelser fra EU institutioner og specielt herunder artikel-29 gruppens udtalelser vil blive brugt som kilder.
Problemformuleringen vil blive besvaret på baggrund af en analyse af den gældende lovgivning, holdt op imod de tilgængelige udtalelser og litterære værker, der behandler emnet om behandling af persondata.

2.2 Historik

Persondataloven er en relativ ny lovgivning der, på baggrund af databeskyttelsesdirektivet 95/46/EF, blev implementeret i Danmark med virkning fra juli 2000. Nærmere om begrundelsen for udarbejdelsen af direktivet, se da afsnit 4.2 - Formål.

Loven erstattede hermed de tidligere registerlove: Lov om offentlige registre[3], og Lov om private registre[4], der trådte i kraft 1. januar 1979. Hermed var Danmark blandt de første lande til at indføre lovgivning om persondatabeskyttelse. Norge, Sverige og Vesttyskland var sammen med Frankrig nogle af de lande, der også indførte lovgivning på området [Nielsen og Waaben, 2008, s. 13].

Da direktivet blev vedtaget i 1995 nedsatte justitsministeriet i 1996 "registerudvalget", der udarbejdede betænkning 1345/1997 – om behandling af personoplysninger. I kølvandet af denne betænkning fulgte en lang og vanskelig periode på 3 år for at implementere direktivet i dansk lovgivning. Der blev udarbejdet 3 lovforslag, jf. L 82, L 44 og L 147.[5] De to første lovforslag nåede aldrig til 2. Behandling i folketinget, mens det tredje med modifikationer blev til det, vi i dag kender som persondataloven. De udfordringer registerudvalget stod overfor, var bl.a. at tage stilling til, om databeskyttelsen fortsat skulle reguleres adskilt i forhold til offentlige og private, samt om elektronisk og manuel registrering skulle adskilles. Udvalget opnåede enighed om en lovgivning, der skulle samle alle områder i én lovgivning, men der blev dog alligevel foretaget nogle vidtgående ændringer i det sidste lovforslag, inden det blev vedtaget. Ændringer indebar bl.a. stramning af reglerne om videregivelse af oplysninger til markedsføringsmæssige formål, samt forbrugernes indsigtsmuligheder ved en sådanne videregivelser, jf. PDL § 6, stk. 2-4 og § 36.

[3] Lov 08-06-1978 nr. 294
[4] Lov 08-06-1978 nr. 293
[5] L 82 (Folketingstidende 97/98 2. Samling, tillæg A, s. 1945-2096) L 44 (98/99, tillæg A, s. 943-1094) L 147 (99/00, tillæg A, s. 3971 ff.)

Bemærkelsesværdigt er også de særlige regler i § 8, der vedrører videregivelse af oplysninger inden for det sociale område. Særreglerne i denne bestemmelse danner nu rammerne om kategorien semi-følsomme oplysninger, som behandles grundigere i afsnit 3.1.2 - personoplysninger. [Nielsen og Waaben, 2008, s. 14 ff] Den nye persondatalov er betydeligt mere vidtgående end de tidligere registerlove, der kun omfattede registrering og videregivelse af personers oplysninger [Blume, 2006, s. 20].

2.3 Forrangsprincippet og direkte virkning

For en forståelse af EU's retsakters virkning på dansk lovgivning, gennemgås de fundamentale principper i dette afsnit. Særligt behandles virkningen af direktiver i forhold til implementering og direkte virkning.

2.3.1 Forrangsprincippet

Europæisk retspraksis siger, at EU-retten har forrang for national lovgivning. Første gang EF-domstolen gjorde dette klart var i Costa mod ENEL sagen fra 1964, jf. C-6/64. Dommen omhandlede en italiensk nationalisering af el-industrien, hvor Costa mente, at denne nationalisering var i strid med traktatens bestemmelser. Den italienske stat mente, at en national instans var forpligtet til at anvende den nationale lovgivning. Domstolen klargjorte i denne forlæggelse for første gang, at EU-retten har forrang for national lovgivning. Præmisserne blev opsummeret således:

»af alt dette fremgår det, at den af traktatens affødte ret, der hidrører fra en autonom retskilde, på grund af sin selvstændige natur, må gå forud for en hvilken som helst national bestemmelse, idet den ellers ville miste sin fællesskabskarakter, og i det selve grundlaget for Fællesskabet ellers ville være bragt i fare;«[6]

Afgørelsen faldt på, at EU's retsakter ville miste sin effektivitet, og medføre forskellig virkning i de enkelte medlemsstater. Hvis man accepterede denne retstilling, ville man samtidig bryde bestemmelsen om forbud mod forskelsbehandling af borgerne i medlemsstaterne, jf. TEF artikel 12. [Sørensen, 2008, s. 175 ff.]

2.3.2 Direktivers virkning på national ret

Et direktiv adskiller sig fra andre EU retsakter på den måde, at det skal implementeres i de nationale lovgivninger. De øvrige retsakter, herunder traktater, forordninger og beslutninger, er umiddelbart anvendelige fra vedtagelsesøjeblikket, og har derfor direkte virkning. Et direktiv indeholder en implementeringsfrist for medlemsstaterne, og først når denne er foretaget, er direktivet gældende nationalt. Komplikationerne opstår i den situation hvor et direktiv ikke bliver implementeret rettidigt.

Databeskyttelsesdirektivets implementeringsfrist lød på tre år, som betød, at de enkelte medlemsstater skulle indskrive direktivet i national lovgivning inden 24. oktober 1998, , jf. Databeskyttelsesdirektivets artikel 32, stk. 1. I Danmarks tilfælde skete dette først i juli 2000, jf. ovenfor i afsnit 2.2. Her var altså en toårig pe-

[6] Præmis opsummering i sag C-6/64 (præmisserne er ikke nummereret)

riode, hvor de nævnte komplikationer opstod. Når fristen er overskredet, betyder det, at direktivet alligevel giver de danske borgere rettigheder på trods af den manglende implementering. Rettighederne kan dog kun påberåbes *vertikalt*, altså overfor myndighederne, men aldrig *horisontalt*, overfor andre private. Det skyldes, at et direktiv er en retsakt, der som udgangspunkt forpligter medlemsstaterne, og manglende eller for sen implementering kan ikke fritage en stat for de i direktivet indeholdende forpligtelser. Omvendt kan det ikke forventes, at private overholder bestemmelser, der endnu ikke er indskrevet i den nationale lovgivning. [Sørensen, 2008, s. 142 ff.]

Når der opstår tvivl om fortolkning af et EU-retsakt, kan det forelægges for EF-domstolen, som et præjudicielt spørgsmål, jf. TEF art. 234. En længere række præjudicielle afgørelser ved EF-domstolen har behandlet spørgsmålet om privates retsstilling på det horisontale niveau, når implementering af et direktiv er blevet udsat. I sag C-443/98 *Unilever Italia*, hvor denne var leverandør af madolie til *Central Food*, levede produktet ikke op til en italiensk særlovgivning om etikettering. Direktiv 83/189 krævede, at sådanne tekniske forskrifter skulle notificeres, og den italienske særlovgivning var dermed i strid med direktivet. Det præjudicielle spørgsmål, der blev forelagt for domstolen, lød på om private kunne forpligtiges af en lovgivning, hvis vedtagelse var blevet udsat. Med andre ord, om et direktiv, der havde overskredet sin implementeringsfrist, kunne forpligte private. Spørgsmålet blev besvaret således, jf. Dommens præmis nr. 52:

»... det påhviler en national ret under behandlingen af en borgerlig sag mellem private vedrørende kontraktlige rettigheder

og forpligtigelser at afslå at anvende en national teknisk forskrift (direktivet red.), der er vedtaget i en periode, hvor vedtagelsen er udsat, således som fastsat i artikel 9 i direktiv 83/189«[7]
I dette konkrete eksempel gav direktivet, altså hverken rettigheder eller forpligtigelser overfor private, jf. Præmis nr. 51.

I grove træk kan det opsummeres, at EU-borgere kan støtte ret på et direktiv overfor offentlig myndigheder, som det oprindeligt er udformet. Det gælder efter implementeringsfristens udløb, uanset om denne ikke er overholdt. Efter implementeringen er foretaget, skal den nationale lov anvendes, men fortolkes i overensstemmelse med direktivet[8]. Opstår der tvivl om de to retsakters overensstemmelse, kan det forelægges som præjudicielt spørgsmål ved EF-Domstolen, som herefter klargører hvilken fortolkning, der er gældende.

2.4 Formål

Udgangspunktet for beskyttelsen af personoplysninger findes i den europæiske menneskerettighedskonvention (EMRK). Konventionens artikel 8 har til formål at sikre respekt for privat- og familielivets fred. Ligeledes kan FN's menneskerettighedskonventions artikel 17 nævnes, selvom erklæringen ikke er juridisk bindende for staterne. De to artikler lyder således:

[7] C-443/98 – Præmis 52
[8] Dette princip kaldes også fortolkningsforpligtigelsen, jf. Sørensen, 2008, s. 152

EMRK artikel 8:	*Stk. 1. Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance* *Stk. 2. Ingen offentlig myndighed må gøre indgreb i udøvelsen af denne ret, medmindre det sker i overensstemmelse med loven og er nødvendig i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder.*
FN's MRK artikel 17:	*1. Ingen må udsættes for vilkårlig eller ulovlig indblanding i sit privatliv eller familieliv, sit hjem eller sin brevveksling, eller for ulovlige angreb på sin ære eller sit omdømme.* *2. Enhver har ret til lovens beskyttelse mod sådan indblanding eller sådanne indgreb.*

Opretholdelse af disse menneskerettigheder sammenholdt med de voksende muligheder for elektronisk dataoverførsler har altså været grundlaget og argumentet for indførelsen af databeskyttelsesdirektivet. Behovet for øget beskyttelse af personoplysnin-

ger har i takt med teknologiudviklingen været voksende de seneste tre årtier.

Den grundlæggende menneskerettighed om privatlivets fred nævnes også indledningsvis i databeskyttelsesdirektivets: *»Medlemsstaterne sikrer i overensstemmelse med dette direktiv beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, i forbindelse med behandling af personoplysninger.«*, jf. Art. 1, stk. 1. I forlængelse heraf må medlemsstaterne ikke opsætte hindringer for fri udveksling af personoplysninger inden for EU, jf. art 1, stk. 2.

Formålsbeskrivelsen i persondataloven stemmer ikke overens med direktivets, og lyder i stedet på, at skulle erstatte de tidligere nævnte registerlove med en generel lovgivning, der sikrer et højt beskyttelsesniveau for den enkelte borger [”virksomhed og persondata”, Tranberg, 2007, s. 228].

Til trods for den manglende lighed i formålsbeskrivelsen tjener den danske persondatalov alligevel til samme formål som direktivet, og med henvisning til afsnittet om forrang og direkte virkning kan enhver EU-borger anmode om, at en bestemmelse i den nationale implementering bliver sammenholdt med ordlyden i direktivet i det tilfælde, hvor der opstår tvivl om disse to retsakters forenelighed.

Retten til privatlivets fred har altid haft den udfordring at skulle være forenelig med ytringsfriheden i EMRK artikel 10, også nedenfor om massemediernes ytringsfrihed, der kan fratage rettigheden om persondatabeskyttelse for den registrerede. Databeskyttelsesdirektivets artikel 9 havde til formål at give de enkelte medlemsstater bemyndigelse til at lave lovregulering, der skulle

forene rettighederne om privatlivets fred med ytringsfriheden for massemedierne. Se videre herom i afsnittet anvendelsesområde nedenfor.

2.5 Anvendelsesområde

Som nævnt ovenfor reguleres behandlingen af persondata i persondataloven, som er et udspring af EU's databeskyttelsesdirektiv 95/46/EF. Direktivets geografiske udstrækning rækker til fællesskabets medlemsstater, mens de nationale lovgivninger, implementeret på baggrund af direktivet, anvendes på national plan, jf. Art. 4.
Anvendelsesområdet lyder i direktivet såvel som i persondataloven på, at gælde behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling og ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.
Hertil kommer også ikke-elektronisk systematisk behandling inden for det private område, som indeholder oplysninger om økonomiske forhold, samt øvrige oplysninger, der med rimelighed kan forlanges unddraget offentligheden, jf. PDL § 1, 2. Grunden til at det offentlige ikke inddrages i denne bestemmelse skyldes, at dette område fortsat reguleres af forvaltningsloven, offentlighedsloven og arkivloven.
For helt at kortlægge lovens anvendelsesområde er det vigtigt at forstå, hvornår der er tale om *persondata*, hvad der karakteriseres som *databehandling* samt hvornår, der er sket en *overdragel-*

se af persondata. Falder en konkret sag udenfor lovens definitioner af disse begreber, vil det ligeledes falde uden for lovens anvendelsesområde. Se nærmere om definitionerne i afsnit 3.

Persondatalovens § 2, stk. 2 - 10 indeholder undtagelser, hvor denne ikke finder anvendelse. En behandling af persondata, der udelukkende anvendes til rent private aktiviteter, er eksempelvis ikke omfattet, jf. § 2, stk. 3. Størstedelen af undtagelserne er dog en varetagelse af ytringsfriheden, jf. § 2, stk. 2 og stk. 6-10.

Stk. 2 dækker den "almindelige" ytringsfrihed i EMRK artikel 10, som bl.a. blev anvendt i Datatilsynets j.nr. 2000-216-0005, hvor Dansk Folkeparti på partiets hjemmeside offentliggjorde navne på 3.218 personer, som havde fået tildelt dansk indfødsret. Selvom sagens omstændigheder som udgangspunkt, var omfattet af persondatalovens anvendelsesområde, var der her tale om en undtagelse efter § 2, stk. 2, da det blev karakteriseret som en meningstilkendegivelse.

Stk. 6 – 10 er hjemlet i direktivets artikel 9 og giver massemedierne en række fritagelser for forpligtigelserne i persondataloven. I Datatilsynets j.nr. 2008-219-0133, hvor ansatte på bocentret Ringbo henvendte sig til datatilsynet vedrørende behandlingen af deres personoplysninger i forbindelse med en Tv-udsendelse. Udsendelsen, der blev produceret af Bastard Film A/S, blev vist på Danmarks Radio, og omhandlede forholdene på bocentret. Optagelserne var optaget med skjult kamera og dermed uden de ansattes samtykke. Datatilsynet konkluderede, at Bastard Film A/S var omfattet § 2, stk. 10 og dermed fritaget fra forpligtigelserne i persondataloven, da databehandlingen var sket i et journalistisk øjemed. Fritagelsen medfører dog stadig forpligtigelser om data-

sikkerhed, jf. §§ 41, 42, og er disse nødvendige tekniske foranstaltninger ikke overholdt, kan det fortsat føre til erstatnings- og strafansvar, jf. § 69.

2.6 Geografiske område

Persondataloven finder anvendelse ved behandling af persondata, der udføres af en dataansvarlig etableret her i landet, forudsat at aktiviteterne ikke finder sted uden for Det Europæiske Fællesskab,[9]jf. PDL § 4, stk. 1. Hovedreglen er altså, at databehandlingen skal ske på dansk grund, før loven er gældende. Skulle en dataansvarlig, der er etableret på dansk grund, behandle personoplysninger i et andet EU-land, er det fortsat den danske lov, der skal anvendes. Sker behandlingen uden for EU, er det uden for lovens (og direktivets) virkning, da disse betragtes som tredjelande. Forholdene omkring tredjelande behandles i næste kapitel.
Bestemmelsen om lovens geografiske anvendelsesområde har en række undtagelser, hvor området alligevel udvides. Disse undtagelser behandles senere i kapitel 6.

[9] Begreberne *behandling, dataansvarlig*

3 Persondataretten

3.1 Grundbegreberne

PDL § 3 indeholder legaldefinitionerne på de begreber, man arbejder med inden for persondataretten. For overblikkets skyld er de mest centrale definitioner derfor beskrevet nedenfor[10]
Definitionerne udspringer af Direktiv 95/46 artikel 2, med undtagelse af nr. 9, om definitionen på et tredjeland.

3.1.1 Den registrerede

Det måske mest åbenlyse element inden for persondataretten, som også indgår i definitionen af personoplysninger, jf. Afsnit 3.1.2., er defineret som *»en identificeret eller identificerbar fysisk person«.* En beskrivelse der ikke giver anledning til den store tvivl. Ud fra den omtalte ret til privatlivets fred er det altså det enkelte individs privatliv, der er grundlag for denne lovgivning, og dermed ikke juridiske personer der tales om, når begrebet *den registrerede* anvendes. Der forekommer dog en enkelt undtagelse til denne afgrænsning. Nemlig at enkeltmandsvirksomheder kan falde ind under definitionen *den registrerede*, da det kan være svært at afskille det private fra det erhvervsmæssige [Blume, 2006, s. 17].

[10] For en uddybende kommentar til disse definitioner se: Peter Blume "Behandling af persondata – en kritisk kommentar", s. 63 ff.

3.1.2 Personoplysninger

»Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede)«, jf. PDL § 3 (1)

Formuleringen lægger altså op til en meget bred fortolkning af begrebet persondata, da det alene er et krav, at informationen skal kunne knyttes til en identificerbar person. Der foreligger således ikke et krav om, at oplysningerne skal knyttes til et navn. Et journalnummer, personnummer eller fingeraftryk er nok til, at de karakteriseres som persondata efter lovens definition. Med andre ord behøver det identificerbare ikke være alment kendt. Det er tilstrækkeligt, at nogle enkelte personer har kendskab til sammenkoblingen mellem den registrerede data og en person. Direktivet anvender også en mere uddybende definition, der gør det nemmere at gennemskue begrebet. Artikel 2 litra A har følgende tilføjelse til definitionen, i forhold til PDL: *»...; ved identificerbar person forstås en person, der direkte eller indirekte kan identificeres, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet«*

Persondataloven skelner mellem tre typer af persondata. *Almindelige, følsomme* og semi-*følsomme* personoplysninger. Den sidstnævnte er en kategori, der ikke er at finde i direktivet. Kategorien er opstået på baggrund af de tidligere registerlove, som fandt enkelte oplysninger særligt beskyttelsesværdige. Som side-

bemærkning kan det diskuteres om hvor vidt dette strider mod direktivet. [”Virksomhed og persondata”, Tranberg, 2007, s. 231]
§ 7 siger udtømmende hvad, der karakteriseres som følsomt persondata. Det gælder oplysninger om racemæssig og etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold samt oplysninger om helbred og seksuelle forhold. Dette er implementeret uændret fra direktivets artikel 8, og udgangspunktet bliver således, at data der ikke falder ind i de nævnte kategorier i denne bestemmelse, skal betragtes som almindelige oplysninger. Beskyttelsen her findes i artikel 7, svarende til PDL § 6. Men som nævnt ovenfor, bliver enkelte typer almindelige oplysninger tildelt større beskyttelse i Danmark, end det er tilfældet i direktivet. De såkaldte semi-følsomme oplysninger drejer sig om Strafbare forhold, væsentlige sociale problemer, samt andre private oplysninger, som ikke er nævnt i § 7, stk. 1, jf. § 8, stk. 4.

3.1.3 Dataansvarlig

Denne kan i modsætning til den registrerede være en juridisk person såvel som en privat person. Der kan også være tale om en offentlig forvaltning, en institution eller et andet organ, der alene eller sammen med andre afgør til hvilket formål og med hvilke hjælpemidler, der må foretages behandling af oplysninger, jf. PDL § 3 (4).
Definitionen er nødvendig, da det ikke er ligegyldigt hvem, der er den ansvarlige for behandlingen, og hvem der rent faktisk foreta-

ger behandlingen. Som det ligger i ordet er den dataansvarlige ansvarlig for behandlingen af de registrerede oplysninger, og dermed den, som har retten til at disponere over disse.

3.1.4 Behandling

»Enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres genstand for«, jf. PDL § 3 (2)

Igen anvender loven en meget bred fortolkning, der principielt betragter enhver handling med persondata som værende databehandling. Dette burde gøre begrebet nemt at anvende, da alt, hvad man foretager sig med den registrerede data, vil falde ind under denne definition. I forhold til problemformuleringen i denne afhandling kan det dermed også konkluderes, at en overførsel af data til et tredjeland[11] i lovens forstand karakteriseres som en behandling. Problematikken opstår, når man herefter skal definere begrebet overførsel og dermed afgøre, om der er tale om en behandling.[12]
Direktivets tilsvarende legaldefinition af databehandling er mere uddybende end den danske version og giver følgende eksempler på hvad databehandling kan være: Indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse ved transmission, formidling eller en hver anden form for overladelse, sammenstilling eller samkøring

[11] Se afsnit 3.1.6 - Tredjeland
[12] Se afsnit 6.2.1 – Definition (på overførsel)

samt blokering, slettelse eller tilintetgørelse, jf. art. 2 litra b. Denne omfattende opremsning giver en del forståelse for den danske simplificering, da direktivets definition ikke er udtømmende. Direktivets definition kan dog være et godt redskab til forståelse af begrebets bredde.

3.1.5 Databehandler

På samme måde som den dataansvarlige, kan databehandleren være en fysisk eller juridisk person, offentlig myndighed, institution eller ethvert andet organ. Databehandleren er blot en enhed, der på vegne af den dataansvarlige, behandler de registrerede data, jf. PDL § 3 (5). Her opstår altså en fuldmagtslignende tilstand, hvor behandleren arbejder ud fra instrukser fra den dataansvarlige. Det betyder, at ansvaret fortsat bliver hos den dataansvarlige, og at der ikke er sket en videregivelse i persondataretlig forstand. [”virksomhedens persondata”, Tranberg, 2007, s. 232]

3.1.6 Tredjeland

Et tredjeland er i denne sammenhæng en stat, som ikke indgår i Det Europæiske Fællesskab, og som ikke har gennemført aftaler, der er indgået med det Det Europæiske Fællesskab, og som indeholder regler svarende til Databeskyttelsesdirektivet, jf. PDL § 3 (9). Vigtigt i denne sammenhæng er, at der er tale om EØS-lande. Dvs. at Norge og Island er eksempelvis ikke at betragte som tred-

jelande. Dog vil Grønland og Færøerne blive betragtet som tredjelande, da de ikke indgår i dette samarbejde.

Persondataloven giver mulighed for, at der kan ske overførsel til et tredjeland i det omfang, at beskyttelsesniveauet i det gældende land er svarende til direktivets. I praksis betyder det, at det bliver en konkret vurdering af tredjelandets beskyttelsesniveau i de enkelte sager. Nogle lande er dog på forhånd udnævnt af kommissionen som værende *sikre lande* med tilstrækkeligt beskyttelsesniveau. Listen, der sidst blev opdateret pr. 1. Juni 2008, indeholder følgende lande:[13]

- Schweiz
- Canada (begrænset anvendelsesområde)
- Argentina
- Guernsey
- USA (gælder kun oplysninger vedr. flypassagerer. Se dog afsnittet om *safe harbor*)
- Isle of Man
- Jersey

Listen er udarbejdet i af Europa-kommissionen i samarbejde med Artikel 29-gruppen[14]. Den opdateret liste kan findes på datatilsynets hjemmeside, jf. note 13.

[13] http://www.datatilsynet.dk/erhverv/tredjelande/sikre-tredjelande/ - Datatilsynets skrivelse om sikre tredjelande.
[14] Se afsnit 4.2 – Artikel 29-Gruppen

3.2 Artikel 29 Gruppen

Efter direktiv 95/46/EF er der nedsat en gruppe til at behandle spørgsmål om beskyttelse af personer i forbindelse med behandling af personoplysninger. Gruppen består af repræsentanter fra hver af de myndigheder, der er udpeget til at føre tilsyn med behandling af persondata. I Danmarks tilfælde er det en repræsentant fra datatilsynet, der udvælges som repræsentant i artikel 29 gruppen, jf. artikel 29, stk. 1-2. Samtidig er kommissionen repræsenteret. Gruppen kan sidestilles med datatilsynets virkning i Danmark på EU-niveau. Dens arbejdsopgaver er specificeret i artikel 30, og indeholder i grove træk, som en rådgivende uafhængig enhed at bidrage med information til kommissionen om spørgsmål, der vedrører behandling af persondata samt at føre tilsyn med medlemslandenes lovgivning. På den måde skal de sikre at sikkerhedsniveauet ikke afviger i nogle EU-medlemslande. Artikel 29-gruppen har udgivet dokumenter, der vedrører overførsler af persondata til lande uden for fællesskabet. Særlig i relation til problemformuleringen i denne afhandling, har gruppen udsendt en skrivelse vedrørende SNS hjemmesider (Social Network Services), og om de retlige forhold ved databehandling på sådanne sites. [15]

Artikel 29-gruppens arbejde har stor betydning for fortolkning af persondataretten, da den, som øverste organ under kommissionen, fastsætter rammerne for databehandling. Gruppens dokumenter vil blive behandlet grundigere senere i denne afhandling.

[15] WP-163

4 Forpligtigelser ved behandling

Med de grundlæggende begreber på plads vil dette kapitel nu behandle de forpligtigelser, Persondataloven stiller til den dataansvarlige og databehandleren. I første omgang sker denne beskrivelse uden det grænseoverskridende aspekt, og kapitel 6 vil i stedet fokusere på denne problemstilling.
Forpligtigelserne er overordnet udformet som en række principper, der skal overholdes ved registrering, efter registrering, ved behandling og frem til sletning af oplysningerne.

4.1 God databehandlingsskik

Dette første princip er den helt overordnede regel, der knytter sig til behandling af personoplysninger. Lovens § 5, stk. 1, siger i al sin enkelthed at: *»Oplysninger skal behandles i overensstemmelse med god databehandlingsskik«*[16]. Formuleringen udspringer af direktivets krav til medlemsstaterne om at fastsætte bestemmelser, der sikrer, at personoplysninger bliver behandlet *»rimelig og lovligt«*, jf. art. 6, stk. 1 litra a. Bestemmelsen er således en slags generalklausul, som vi eksempelvis kender tilsvarende i markedsføringslovens § 1 om god markedsføringsskik, der i øvrigt ofte kan anvendes ved overtrædelse af reglerne i PDL. Det skyldes, at en overtrædelse ofte er sket i forbindelse med, at oplysningerne anvendes til markedsføringsmæssige formål. PDL har

[16] Jf. PDL § 5 stk. 1

direkte til formål at beskytte mod bl.a. denne type anvendelse af persondata, jf. § 6, stk. 2.

Selvom en generalklausul som denne i manges øjne kan virke alt for overordnet og intetsigende, så er det den udbredte holdning, at en sådan bestemmelse er nødvendig i takt med konstant teknologiske udvikling, som også nævnes indledningsvis i denne afhandling. I Internettets tidsalder findes der hele tiden nye anvendelsesgrundlag for netop personoplysninger, og ikke mindst måder at behandle disse på. En generel bestemmelse som denne er derfor nødvendig, for at dommeren eller tilsynsmyndigheden kan finde lovhjemmel for såkaldt ordentlig opførsel, i forbindelse med behandlingen af personoplysninger.[17] Bestemmelsen vil således "samle op" på de databehandlinger, som ikke er sket rimelig og lovligt, men som ikke direkte overtræder kravene i § 5, stk 2-5 og §§ 6-13.

4.2 Oplysningspligt

De generelle regler om den dataansvarliges oplysningspligt opdeles i to scenarier.[18] Tilfældet, hvor oplysningerne er indsamlet hos den registrerede, og tilfældet, hvor oplysningerne er indsamlet ved en tredjepart. Oplysningspligten i disse scenarier reguleres af hhv. § 28 og 29.

Det sidstnævnte vil typisk være oplysninger der er hentet gennem offentligt tilgængelige kilder, mens det førstenævnte tilfæl-

[17] Denne holdning understøttes også af Charlotte B. Tranberg, jf. Tranberg: Nødvendig behandling af persondata, s. 112 ff.

[18] Vedrørende de *specielle* regler, se da Nielsen og Waaben, 2008, s. 358

de, og mest relevante i denne sammenhæng er, når registreringen sker på den registreredes eget initiativ.
En registrering, der sker via en hjemmeside på Internettet, hører således til det første scenarie og reguleres af § 28.
§ 28 opstiller en række minimumskrav til, hvad den registrerede skal oplyses om ved registrering. Det omhandler den dataansvarliges identitet samt databehandlerens identitet (hvis denne ikke er samme person), formålene med den behandling hvortil oplysningerne er bestemt samt yderligere oplysninger, der i den konkrete situation er nødvendige for at varetage den registreredes interesser, jf. § 28 (1-3). Specielt omkring formålsbeskrivelsen stiller PDL høje krav til at denne skal være *udtrykkelig* og *saglig*, jf. § 5, stk. 2.[19]

4.3 Krav om datakvalitet

Loven stiller en række krav til den dataansvarlige, når det kommer til kvaliteten af den data, der registreres. Med andre ord er bestemmelsen et krav om, at »behandling af oplysninger skal tilrettelægges således, at der foretages fornøden ajourføring af oplysningerne«, jf. § 5, stk. 4 1. pkt.. [20] Bestemmelsen fungerer i samspil med § 37, der giver den registrerede mulighed for at gøre indsigelse i forhold til de oplysninger, der er registreret om personen. Det indebærer, at den registrerede kan kræve oplysningerne rettet, slettet eller blokere oplysninger, der måtte vise

[19] se afsnit 4.6 – Finalitéprincippet
[20] Bestemmelsen er baseret på RDir 95/46/EF art. 6, stk. 1, litra d

sig at være urigtige, vildledende eller på lignende måde er behandlet i strid med lov eller bestemmelser udstedt i medfør af lov, jf. § 37.[21]

I praksis vil det dog sjældent forekomme, at urigtige oplysninger bliver slettet, da den registreredes interesse bliver overskygget af den dataansvarliges behov for at bevare de oplysninger, der oprindeligt var grundlaget for en aftaleindgåelse. [Nielsen og Waaben, 2008, s. 153]

4.4 Samtykke

Reglerne om samtykke er helt essentielle, når man beskæftiger sig med databehandling, og en dataansvarlig kan som udgangspunkt altid behandle oplysninger, hvis denne har den registreredes udtrykkelige samtykke. Dog er det vigtigt, at forpligtigelserne i § 5, stk. 2-5 ligeledes skal være overholdt, jf. nedenfor. For virksomheder, der har registreret oplysninger om tusinder af individer, kan dette samtykke være meget besværlig at indsamle, og med den begrundelse kan det nemt forekomme, at denne forpligtigelse bliver "undladt".

Et samtykke er i lovens forstand *»enhver frivillig , specifik og informeret viljetilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling«*, jf. § 3 (8).

Grunden til at viljeserklæringen tildeles så stor betydning, skyldes, at den lovhjemler en databehandling, uanset om der er tale

[21] for yderligere uddybning af den registreredes rettigheder, se kapitel 5.

om følsomme (og semi-følsomme) eller almindelige oplysninger, jf. § 6, stk. 1 (1) og § 7 stk. 2 (1). Vedrørende de følsomme oplysninger, som tidligere nævnt indeholder oplysninger om racemæssig, etnisk baggrund, politisk, religiøs eller filosofisk overbevisning samt tilhørsforhold til foreninger og helbredsoplysninger, er reglen om samtykke således en af undtagelserne til, hvornår denne type oplysninger alligevel må behandles. De almindelige oplysninger, som er alt andet end de ovennævnte, kan ligeledes altid ske, på baggrund af et samtykke.

I fortolkningen om hvorvidt der foreligger en viljeserklæring, sker dette bl.a. ud fra en analog fortolkning af det aftaleretlige begreb. [22] Kort fortalt indebærer dette at den registrerede selv, eller ved evt. fuldmagt, har udført en aktiv handling for at blive registreret. Der foreligger således ikke et formkrav. Viljeserklæringen kan ske både skriftlig og mundtlig, men i forhold til problemformuleringen i denne afhandling er det vigtigt at bemærke, at en handling eksempelvis ved udfyldelse af en blanket på Internettet, også er at betragte som et samtykke til registreringen. Det sker som regel ved, at brugeren accepterer nogle vilkår ved at krydse af i en tjekboks, og herefter sende oplysningerne elektronisk til modtageren.

Som det fremgår af definitionen, skal denne handling være frivillig. Igen kan der foretages en analog fortolkning til obligationsretten, som bl.a. indebærer, at der ikke må være tale om tvang, og at personens sindstilstand kan have indvirkning på vurderingen [Tranberg, 2007, s. 165]. Ordene specifik og informeret stiller

[22] Nærmere herom i Tranberg: Nødvendig behandling af personoplysninger, s. 161 ff.

krav til modtageren om, at der klart og tydeligt ved registrering oplyses hvad, der præcist gives samtykke til. I relation til Internettet er der her tale om disse nævnte vilkår, som brugeren accepterer. Disse oplysningskrav gennemgås umiddelbart nedenfor.

Datatilsynet har i forskellige afgørelser behandlet, hvornår et samtykke opfylder de krav, der stilles i PDL. En af de mere grundigere behandlinger skete i en afgørelse fra 2004[23], hvor Datatilsynet blev bedt om at vurdere en samtykkeerklærings overensstemmelse med persondataloven. Forespørgslen kom fra Foreningen af Statsautoriserede Revisorer, der havde udarbejdet en erklæring, hvor ansatte kunne samtykke til, at deres arbejdsgiver måtte behandle deres personoplysninger og overføre disse til et tredjeland (i denne sammenhæng USA). Behovet for overførslen til USA skyldtes, at en amerikansk lov[24] krævede revisorers registrering i et register kaldet PCAOB for at kunne føre tilsyn med aktieselskaberne revisorer, og dermed sikre udarbejdelsen af informative, retvisende og selvstændige revisionsprotokoller. Efter dansk lovgivning (PDL) har den registrerede til enhver tid ret til at gøre indsigelse mod, at der sker behandling af denne oplysninger, og kan i forlængelse heraf tilbagekalde sit samtykke, jf. § 35 og § 38. Datatilsynet fandt det tvivlsomt, at et samtykke i denne sammenhæng reelt ville kunne tilbagekaldes, da arbejdsgiveren i tilfælde af en tilbagekaldelse ikke ville kunne fjerne oplysningerne fra det amerikanske register. Datatilsynets afgørelse lød der-

[23] 2003-233-0028
[24] Surbanes Oxy Act of 2002

for på, at et sådan samtykke ikke ville opfylde lovens krav[25] om, at dette skal være "informeret", og arbejdstageren burde som minimum være informeret om, hvorvidt en tilbagekaldelse reelt er mulig eller ej. Vurderingen fra Datatilsynet er også lavet på baggrund af en proportionalitetsvurdering som behandles nedenfor i afsnit 4.5 om proportionalitetsprincippet [26]

Udgangspunktet med samtykke, som en nødvendighed for at en databehandling kan finde sted, fraviges i en række situationer. Nøgleordet i denne sammenhæng er "nødvendigheden" af behandlingen. De regler i §§ 6 – 8 der indeholder dette nødvendighedskrav, kræver således en konkret vurdering af behandlingens nødvendighed. Dette sker i form af en proportionalitetsvurdering, jf. nedenfor.

4.5 Proportionalitetsprincippet

God databehandlingsskik er som tidligere nævnt den overordnede regel, når der foretages databehandling. Herunder kommer så en proportionalitetsvurdering, som primært udspringer af § 5, stk. 3. *»Oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.«*

Et princip, der kort fortalt bygger på, at en dataansvarlig ikke må indhente oplysninger, der ikke er nødvendige for at opnå formå-

[25] jf. § 3 (8)
[26] jf. 2003-233-0028 – afsnit "3." midtfor

let med registreringen. Datatilsynet foretog en sådan proportionalitetsvurdering i en sag fra 2003[27], hvor en fagforening gjorde opmærksom på, at en virksomhed indsamlede kreditoplysninger om ansøgere, fra RKI Kredit Information A/S. Her blev det fastlagt af Datatilsynet, at disse oplysninger ikke anses for nødvendige i en proportionalitetsvurdering med mindre, der er tale om en særligt betroet stilling.

Proportionalitetsprincippet er, som tidligere nævnt, ligeledes et princip, der får betydning til de bestemmelser i § 6 – 8, der indeholder nødvendighedskriteriet.

4.6 Finalitéprincippet (FB)

Dette princip kaldes også *princippet om formålsbestemthed,* og er på niveau med proportionalitetsprincippet ligeledes en del af den overordnede betegnelse om god databehandlingsskik.

»Indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål. Senere behandling af oplysninger, der alene sker i historisk, statistisk eller videnskabeligt øjemed, anses ikke for uforenelig med de formål, hvortil oplysningerne er indsamlet«, jf. § 5, stk. 2.[28]

En virksomhed må altså kun behandle personoplysningerne efter de formål, der var angivet fra start. I tilfældet, hvor et samtykke har lovhjemlet behandlingen, er det således det formål, den registrerede har accepteret i samtykkeerklæringen. Hvis den dataan-

[27] 2003-631-0118
[28] Udspringer af Rdir 95/46/EF Artikel 6, stk. 1 litra b

svarlige på senere tidspunkt ændrer dette formål og behandler personoplysningerne på anden vis, vil dette være uforeneligt med denne bestemmelse, og ville i så fald kræve indhentning af samtykke på ny. Der gives dog den undtagelse, at dataen gerne må anvendes i historisk, statistisk eller videnskabeligt øjemed, uden at dette vil blive betragtet som en ændring af det oprindelige formål med behandlingen.

Formålet skal ligeledes være udtrykkelig og sagligt. Med ordet *sagligt* er vigtigt at have det ovenfor nævnte proportionalitetsprincip for øje. Udover at formålet skal være beskrevet grundigt, skal det altså vurderes om de registrerede oplysninger er for indgribende i forhold til, hvad de skal anvendes til. [Tranberg, 2007, s. 102 ff]

5 Den registreredes rettigheder

Dette afsnit har til formål at stille den registreredes rettigheder i perspektiv med de forpligtigelser, den dataansvarlige har. En uddybelse af disse rettigheder bliver dog foretages senere i det omfang, de har relevans for overførselsproblemet.

Lovens kapitel 9 omhandler den registreredes indsigtsret, og gennemfører dermed direktivets bestemmelser i kapitel 2, afdeling 10.
Indsigtsretten virker i sammenspil med de forpligtigelser den dataansvarlige skal overholde, jf. ovenfor. *»Fremsætter en person begæring herom, skal den dataansvarlige give den pågældende meddelelse om, hvorvidt der behandles oplysninger om vedkommende.«,* jf. § 31, stk. 1, 1. pkt.
2. pkt. angiver et minimumskrav til, hvad der kan kræves indsigt i. Disse er som ved den dataansvarliges oplysningspligt, krav om hvilke oplysninger der behandles, formålet, samt kategorierne af modtagere af oplysningerne. Som en tilføjelse skal den dataansvarlige oplyse, hvor de tilgængelige oplysninger stammer fra, jf. § 31, stk. 1 (1-4). Indsigtsmulighederne er altså ganske store for den registrerede, og dette har til formål at sikre en høj kvalitet, og skabe åbenhed i den databehandling, der finder sted. Der stilles ikke krav til, at en person skal angive hvilke oplysninger, denne ønsker indsigt i. En henvendelse om en sådan indsigt, *skal* alt-

så imødekommes af den dataansvarlige [Tranberg – "virksomhed og persondata", 2007, s.257]

Lovens kapitel 10 indeholder en række *øvrige rettigheder* for den registrerede. Kun de relevante i forhold til afhandlingens problemformulering er fremhævet her. En af disse rettigheder, er retten til, til enhver tid, at gøre indsigelse mod, at oplysninger om vedkommende gøres til genstand for behandling, jf. § 35. I forlængelse heraf findes også retten til at tilbagekalde et samtykke, jf. § 38. Her kan igen nævnes dommen "Sarbanes Oxy Act", hvor denne rettighed ikke kunne overholdes, da det ikke reelt var muligt at tilbagekalde samtykket, det førte til, at Datatilsynet fandt, at samtykkeerklæringen ikke var acceptabel.[29] Under lovens kapitel 10, hører ligeledes, den tidlige nævnte indsigelsesret, der efter § 37 giver den registrerede ret til at få oplysninger, rettet, slettet eller blokeret i tilfælde af, at disse oplysninger er urigtige eller i strid med gældende ret.

[29] 2003-233-0028

6 Overførsel til tredjelande

Dette afsnit har til formål at behandle de problemstillinger der opstår i det øjeblik, at personoplysningerne bliver overført til et land udenfor EU og EØS, hvor tvister ved behandlingen dermed skal afgøres efter importlandets jurisdiktion.

6.1 Overførselsproblemet

Som beskrevet indledningsvis i denne afhandling er muligheden dataoverførsler på internationalt niveau meget vigtig, da de repræsenterer en meget vigtig ressource. På det private område udgør personoplysninger en stor indtægtskilde. Samtidig er interessen for, at disse databehandlinger sker uden udnyttelse og krænkelse af individets privatliv, af naturlige årsager prioriteret meget højt. En retlig regulering af disse to interessekonflikter, er derfor nødvendig. Dette skyldes specielt, at der findes såkaldte *data havens*, som er et udtryk for lande, der slet ikke har lovgivning, der beskytter den registrerede ved behandling af persondata. Mulighederne for behandling i sådanne lande er således ubegrænset, og den registreredes privatlivsbeskyttelse bliver ikkeeksisterende.[Blume, 2006, s. 11 og 23]

6.2 Overførsel

6.2.1 Definitionen

Som det tidligere blev fastlagt, er en overførsel at betragte som en behandling efter definitionen i § 3 (2). Med det på plads, er det dog nødvendigt at definere en *overførsel*, da der ikke findes en legaldefinition herpå.

Udtrykket *overførsel* er en samlet betegnelse for tre typer af overdragelse. *Videregivelse, overladelse,* og *intern anvendelse.*

Videregivelse er et udtryk for overdragelse til tredjemand. Altså en tredjepart end de i forvejen involverede parter, nemlig den registrerede, den dataansvarlige, databehandleren samt de eventuelle folk herunder, som har bemyndigelse til at behandle oplysningerne.[30] *Overladelse* dækker over den overdragelse, der sker til en databehandler og de herunder tilhørende folk med bemyndigelse til at behandle oplysningerne. Til sidst dækker begrebet også over den dataansvarliges interne brug af oplysningerne. For kort at opsummere dækker begrebet *overførsel* altså enhver situation, hvor en person (eller juridisk person) kommer i besiddelse af oplysningerne. [Nielsen og Waaben, 2008, s. 345]

Det er dog nødvendigt at knytte en kommentar til internetoverførsler. Når data overføres på denne måde, sker der nogle tekniske hændelser, der kan medfører at dataen "mellemlander" på servere i tredjelande. Dette bliver efter EF-Domstolens praksis ikke anset, som overførsel til et tredjeland, da det kræver en grad af permanens. I det tilfælde at disse mellemled registrerer oplys-

[30] jf. PDL § 3 (6)

ningerne, vil det således være omfattet af reglerne. [Nielsen og Waaben, 2008, s. 345][31]

6.2.2 Hvornår er der sket overførsel til tredjeland?

Særligt når en databehandling medfører tilgængelige oplysninger på Internettet, kan det virke svært at afgøre, om der er tale om en overførsel til tredjelande. Problemstillingen blev bl.a. taget op i sagen C-101/01 – Lindquist, hvor en kvinde (Bodil Lindquist), der beskæftigede sig med forberedelse af konfirmander, havde oprettet en hjemmeside med oplysninger om hendes 18 kollegaer i sognet. Disse havde til formål at gøre konfirmationsforberedelsen lettere for menighedsmedlemmerne. Lindquist offentliggjorde bl.a. navne, efternavne, telefonnumre og i et enkelt tilfælde, at en kollega var sygemeldt pga. beskadiget fod. I forbindelse med en ankesag blev der forelagt en række præjudicielle spørgsmål ved EF-Domstolen, et af disse spørgsmål skulle klargøre, om der var tale om en overførsel til tredjeland, ved at lægge informationerne tilgængelige på en hjemmeside.[32] Domstolen udtalte *»…at der ikke foreligger en "videregivelse til et tredjeland af personoplysninger" i den forstand, hvori udtrykket er anvendt i artikel 25 i direktiv 95/46…«.*[33] Et af hovedargumenterne, for denne afgørelse var, at Lindquist ikke direkte havde sendt oplysningerne til en modtager i et tredjeland, men at disse kun var overdraget i det øjeblik, at en person i et tredjeland skulle foreta-

[31] se også Tranberg – Virksomhed og persondata, 2007, s. 363
[32] C-101/01 – præmis nr. 52
[33] C-101/01 - præmis nr. 71

ge de nødvendige operationer for at få adgang til dem. De blev således ikke automatisk sendt til et tredjeland.[34]

Det er dog tvivlsomt, hvorvidt dette eksempel kan konkludere, at personoplysninger uploadet på Internettet, aldrig ville være at betragte som en overførsel til tredjelande. Der skal ske en konkret vurdering af sagens omstændigheder, og det er ikke umuligt, at en *offentliggørelse* på Internettet vil bliver betragtet som en overførsel. En dom, der delvist modsiger EF-Domstolen i spørgsmålet, er U.2007.334 Ø – Hvor nogle indscannede pantebreve var gjort tilgængelige på en virksomheds hjemmeside. Disse breve indeholdte to personers cpr-numre, og virksomheden blev dømt for at have foretaget en *videregivelse* efter PDL § 11, stk. 3, der udtrykkeligt siger, at offentliggørelse af personnumre ikke er tilladt uden samtykke fra den registrerede.

Det er min personlige vurdering, at en offentliggørelse på Internettet i højere grad i fremtiden, vil blive regnet for en overførsel til tredjelande. Især når man ser det i lyset af søgemaskinernes stadig voksende evne til på meget kort tid at gøre information tilgængeligt for brugeren. I modsætning til i dag var det mere utænkeligt i 2001, hvor Lindquist dommen blev afsagt, at man ville finde frem til den omtalte data, selvom man søgte efter det. Der er dog stadig ingen praksis, der endegyldigt understøtter denne påstand.

[34] C-101/01 – Præmis nr. 60

6.3 Tredjelandets beskyttelsesniveau

Den overvejende hovedregel, hvis man ønsker, at overføre personoplysninger til et tredjeland lyder, at *»Der må kun overføres oplysninger til et tredjeland*[35]*, såfremt dette land sikrer et tilstrækkeligt beskyttelsesniveau«*, jf. § 27, stk. 1.

Det forudsættes således, at al overførsel til lande inden for EU frit kan ske, da disse i overensstemmelse med direktivet har indført regler, der sikrer et tilstrækkeligt beskyttelsesniveau, dog skal der fortsat være tale om en databehandling, der falder indenfor direktivets anvendelsesområde. [Nielsen og Waaben, 2008, s. 344]. Det efterfølgende kapitel behandles den problemstilling der opstår, når man ønsker at overføre personoplysninger til et tredjeland, som ikke har lovgivning der sikrer et tilstrækkelig beskyttelsesniveau.

[35] se afsnit 3.1.6 – Tredjeland, for definitionen herpå

7 Safe Harbor

7.1 Optakt

EU og USA har begge en tungtvejende kommerciel interesse i, at overførsler af personoplysninger er mulige mellem de to unioner. Interessen for beskyttelse af privatlivets fred og den individuelles integritet, er da også tilstede begge steder. Dog med vidt forskellige tilgange til, hvorledes den retlige regulering skal foregå. I modsætning til EU's tilgang, som er beskrevet i denne afhandling, bygger det amerikanske system på en *sektor-specifik* tilgang, som betyder, at den bygger på lovgivning, regulering og selvregulering[36]. Der er med andre ord ingen general lovgivning om persondatabeskyttelse. USA er derfor at betragte som et tredjeland, da de ikke opnår det *tilstrækkelige beskyttelsesniveau* som er nødvendig efter direktivets art. 25 og PDL § 27, og for at en dataoverførsel må finde sted. Problemet bliver kun endnu større af det faktum, at USA som et føderal land, er delt op i delstater, med individuelle lovgivninger. Det betyder at der ikke kan garanteres samme beskyttelsesniveau i de enkelte stater.[37]

For at bygge en bro mellem disse to forskellige tilgange, til databeskyttelse, har EU- Kommissionen, i samarbejde med *U.S. Department of Commerce*, udarbejdet *Safe Harbor* – aftalen (med

[36] www.export.gov/safeharbor - Den officielle hjemmeside for "U.S. Department of commerce"

[37] Nærmere om denne problemstilling i Blume, 2006, s. 92, om "føderale lande"

virkning fra 26. Juli 2000). *Safe Harbor Privacy principles*, som er den amerikanske betegnelse, går i al sin enkelthed ud på, at amerikanske virksomheder kan vælge at tiltræde denne ordning, og på den måde blive anerkendt som "sikkert tredjeland" i direktivets forstand. Ved at tiltræde ordningen, samtykker virksomheden således til, at behandle personoplysninger, efter de principper som ordningen forlanger.

I forhold til hvor lovhjemlen til denne ordning findes, er der en anelse uenighed.

Med lovhjemmel i direktivets art. 26, stk. 2[38], giver Safe Harbor løsningen, virksomheder med hjemsted i en EU-medlemsstat, en mulighed for at overføre personoplysninger til virksomheder i USA, forudsat at de har tiltrådt ordningen, og dermed forpligtiget sig til, at *yde tilstrækkelige garantier for beskyttelse af de registreredes rettigheder*.[Andersen, 2005, s. 629] Denne mening støttes dog ikke op af Peter Blume, der mener at lovhjemlen findes i art. 25, stk. 1, og altså ikke art. 26, stk. 2. Det sker ud fra den begrundelse, at Safe Harbor modellen er en særegen aftale, der ikke kan sammenlignes med en situation, hvor et tredjeland godkendes som tilstrækkeligt. Påstanden underbygges også af, at Safe Harbor ordningen ikke har været omgivet af den samme ro, som godkendte tredjelande. [Blume, 2006, s.143] Et tredje og sidste udsagn går på, at hjemlen findes i art. 25, stk. 6, der giver Kommissionen ret til at fastlå, hvis et land yder et tilstrækkeligt beskyttelsesniveau [Nielsen og Waaben, 2008, s. 347]. Dette sidste

[38] svarende til PDL § 27, stk. 4

udsagn er sandsynligvis det mest korrekte, da Safe Harbor netop eksisterer på baggrund af en beslutning fra Kommissionen.
Listen af amerikanske virksomheder der har tiltrådt Safe Harbor modellen, er offentlig tilgængelig på *Federal Trade Commission's* officielle hjemmeside.[39] Listen huser, pr. 1. August 2009, 1872 virksomheder. Et antal, når man ser på USA's størrelse, der må siges at være meget beskedent. Dog finder man store selskaber som Microsoft, Apple, Yahoo, og ikke mindst Facebook på listen. I Forhold til netop Facebook.com, der med over 200 millioner brugere, udgør verdens største, såkaldte *Social Network Service (SNS)*, vil der nedenfor blive set nærmere på de juridiske problemstillinger der opstår, ved driften af en sådan hjemmeside

7.2 Indholdet af Safe Harbor

Dette afsnit har til formål, at behandle de principper, som amerikanske virksomheder forpligtiger sig til at overholde, når de tiltræder Safe Harbor. Ordningen bygger på 7 hovedprincipper: Notice, choice (opt out), onward transfer, access, security, data integrity og inforcement. Eller på dansk: Oplysningspligt, valgfrihed, videre overførsel, adgang, sikkerhed, Dataintegritet (relevans) og håndhævelse.[40] Disse hovedprincipper danner i samspil med 15 FAQ (Ofte stillede spørgsmål), rammerne omkring Safe Harbor ordningen.

[39] www.export.gov/safeharbor
[40] www.export.gov/safeharbor - Herunder "Safe Harbor documents" (de 7 hovedprincipper i Safe Harbor)

Virksomhederne, skal således *tilmelde* sig denne ordning. Dette sker enten gennem Federal Trade Commission, eller ved at virksomheden tiltræder en certificeringsordning gennem f.eks. TrustE.[41] Denne registrering skal gentages årligt.
Det efterfølgende, gennemgang er lavet på baggrund af Kommissionens beslutning vedrørende Safe Harbor, jf. 2000/520/EF[42], samt den amerikanske version, der er offentliggjort af U.S. Federal Trade Commission[43]. Disse to kildehenvisninger er naturligvis baseret på den samme aftale, men sammenligning af ordlyden, er alligevel nødvendig, da amerikanske virksomheder følger den formulering der er gjort tilgængelig for dem.

1. Notice (Oplysningspligt)

> I stil med den oplysningspligt der indgår i EU-direktivets art. 10, forpligtiger tiltrådte virksomheder sig til, at oplyse til hvilke formål deres oplysninger indsamles, og behandles. De skal oplyse hvorledes den registrerede kan henvende sig, i tilfælde af henvendelser og klager, samt hvem oplysningerne bliver overdraget til. Disse oplysninger skal oplyses, klart og tydeligt, første gang en person anmodes om at levere personoplysninger, eller hurtigst muligt herefter, dog under alle omstæn-

[41] www.truste.com
[42] EF-Tidende nr. L 215 af 28/8 – 2000, s. 7 – 47 (bilag I) – Dokumentet indeholder de 7 hovedprincipper, de 15 FAQ'er, samt den dialog der er foregået i aftalens indgåelsesface.
[43] jf. note 39

digheder inden at oplysningerne anvendes til et andet formål, end det oprindeligt blev indsamlet. Dette princip stemmer altså, i høj grad, overens med den oplysningspligt vi kender.

2. Choise (Valgfrihed)

Dette andet princip, har to elementer. En *opt out(1)* og en *opt in (2)* regel.

(1)Organisationer der har tiltrådt Safe Harbor ordningen, skal give den registrerede mulighed for, at fravælge, at oplysningerne må videregives til tredjepart, eller anvendes til formål, der viger fra det oprindelige formål, der blev givet samtykke til, eller som er godkendt på et senere tidspunkt. I denne situation kræver det, at den registrerede på eget initiativ *fravælger* denne type behandling af oplysningerne.

(2) For følsomme oplysninger[44] skal tiltrådte virksomheder indhente en accept, hvis disse oplysninger skal videregives til tredjepart, eller bruges til et formål, der viger fra det oprindelige formål, eller et formål der er givet samtykke til på et senere tidspunkt. Her kræves således ikke en aktiv handling, fra den registrerede, for at undgå behandling af

[44] som defineret i RDir 95/46/EF art. 8, stk. 1

denne type data. Men derimod en aktiv handling før at behandlingen må finde sted.

3. Onward Transfer (Videre Overførsel)

Dette tredje princip, har til formål at sikre, at oplysningerne ikke bliver overdraget til en tredjemand, som ikke yder et tilstrækkeligt beskyttelsesniveau, på samme måde som direktivets art. 25 gør det. Udgangspunktet er derfor, at de tiltrådte virksomheder skal overholde de ovenfornævnte principper, om oplysningspligt og valgfrihed, før en videregivelse kan finde sted. Udgangspunktet fraviges dog, i det tilfælde at der er tale om en tredjepart, der fungerer som *mellemmand* og udfører opgaver på vegne af den dataansvarlige, og i henhold til dennes instrukser. I dette tilfælde er det tilstrækkeligt at den dataansvarlige sikrer sig, at mellemmanden overholder principperne i Safe Harbor, er omfattet af direktivet, eller på anden hvis er kvalificeret som havende tilstrækkelig beskyttelse, med hjemmel i direktivet. Disse tredjemænd vil, i tilfælde af brud på principperne, ikke blive holdt ansvarlige, med mindre de gennem aftale, er gået med hertil.

4. Security (Sikkerhed)

Det fjerde princip pålægger de tiltrådte virksomheder, at træffe en række foranstaltninger for at beskytte disse oplysninger mod tab, misbrug, uautoriseret adgang, videregivelse, ændring eller ødelæggelse.

Dette princip er ikke tidligere berørt i denne afhandling, men udspringer af direktivets art. 17, stk. 1, der i den danske implementering siger, at »*den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommende kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere*«[45]

I relation til internettet, betyder det, at en dataansvarlig, gennem programmeringen, skal sikre at personoplysninger, ikke bliver tilgængeligt for almenheden. Dette skete bl.a. i en sag, hvor en Teknisk skole, gennem en manglende teknisk foranstaltning, offentliggjorde 11 elevers cpr-numre på skolens hjemmeside[46].

5. Data integrity (Dataintegritet)

[45] PDL § 41, stk. 3
[46] 2009-631-0071

Dette princip svarer delvist til de bestemmelser i direktivet, der stiller krav til datakvaliteten af den registrerede data, jf. art. 6, stk. 1, litra d.[47] Samtidig har princippet spor af proportionalitetsprincippet samt finalité-princippet.

Proportionalitetsprincippet fremgår af ordlyden: *Personoplysninger skal i medfør af principperne være relevante i forhold til de formål, hvortil de anvendes.* Finalité-princippet fremgår således: *Et foretagende må ikke behandle personoplysninger på en måde, der ikke er i overensstemmelse med det formål, hvortil de oprindeligt er blevet indsamlet.* Til sidst stiller princippet krav til datakvaliteten med kravet om, at de tiltrådte virksomheder, *i det omfang det er nødvendigt*, skal *træffe passende foranstaltninger for at sikre, at oplysningerne er pålidelige, nøjagtige, fuldstændige og ajourførte.*

6. Access (Indsigt)

Dette sjette princip bygger på de bestemmelser i direktivets kapitel 2 afdeling V,[48] og pålægger de tiltrådte virksomheder, at efterkomme den registreredes ret til indsigt i de oplysninger der er registreret om dem. De er således forpligtet til, at be-

[47] se afsnit 4.3 – krav om datakvalitet
[48] se kapitel 5 – Den registreredes rettigheder

svare en henvendelse fra en privatperson, omkring oplysninger de har registreret om denne.

7. Enforcement (Håndhævelse)

Det syvne og sidste princip vedrører håndehævelsen af, at de tiltrådte virksomheder overholder de 6 ovenstående principper. En håndhævelse, hvis tilstedeværelse er nødvendig for at Safe Harbor får en reel virkning. Dette skal sikre den effektive beskyttelse af privatlivets fred, give de registrerede mulighed for at gøre indsigelser, samt fastlægge en række konsekvenser, hvis principperne ikke overholdes. Bestemmelsen forpligter den amerikanske regering til at indføre nogle mekanismer, der som minimum skal omfatte *let tilgængelige, overkommelige, og uafhængige indsigelsesprocedurer.* Disse mekanismer skal gøre det muligt at undersøge, og afgøre om der er tale om et brud på principperne, og fastsætte en evt. erstatningsstørrelse. Kravet til disse sanktioner lyder, i aftalen, på at skulle være *af en sådan karakter, foretagenderne til at overholde principperne.*

Safe Harbor Modellen er ligeledes bygget på de nævnte 15 *ofte stillede spørgsmål*, der fungerer som retningslinjer, til yderligere forståelse af principperne. Disse spørgsmål vil ikke blive gen-

nemgået systematisk, da de bygger på de ovenfor nævnte principper.

Artikel 29-gruppen har i hele forhandlingsforløbet, fulgt debatten tæt, og har løbende tilkendegivet en utryghed ved ordningen og en utilfredshed over ikke, at være blevet tilstrækkelig inddraget til trods for at den officielt gav udtryk for tilslutning. [Blume, 2006, s. 144, note 36] Efterfølgende har gruppen ligeledes offentliggjort en handlingsplan, for udarbejdelse af en rapport, der havde til formål at evaluere ordningens virkning i praksis. Handlingsplanen blev offentliggjort ved udløb, af ordningens første løbeperiode i 2002, hvor gruppen gjorde status for ordningens virkning i praksis. Gruppen ønskede bl.a., at indsamle opdateret og specifikke oplysninger om de tiltrådte virksomheders evne til, at fremme gennemsigtigheden overfor de registrerede.[49] Siden dette oplæg til en grundig analyse af Safe Harbor ordningens virkning, er der ikke blevet offentliggjort nogle dokumenter, der afslører resultaterne af denne analyse. Om dette skyldes, at dokumentet aldrig blev udarbejdet, eller ikke har set dagens lys, af politiske årsager må, indtil nu, forblive i det uvisse.

Til trods for den omfattende skepsis over for Safe Harbor aftalen, er der ingen tvivl om, at aftalen fører et væsentligt højere beskyttelsesniveau med sig. Et af problemerne er bare, at aftalen, der kan karakteriseres som en sui generis aftale, principielt er diskriminerende i forhold til andre tredjelande, og dermed repræ-

[49] WP-62

senterer en selvmodsigelse i forhold til direktivet. [Blume, 2006, s. 145]

Et andet problem ved modellen, er de fortolkningsforskelle der unægtelig vil opstå. Her tænkes specifikt på, at den ordlyd der anvendes i Safe Harbor principperne, kan fortolkes meget forskelligt. I en fortolkningssituation er det amerikansk lovgivning der er gældende, og en sådan fortolkning vil derfor næppe leve op til de krav EU-retten stiller gennem direktivet. Denne problemstilling behandles yderligere i afsnittet nedenfor, omkring sociale netværks tjenester på Internettet.

7.3 Sociale Netværks Tjenester

Flere større amerikanske virksomheder har valgt at tiltræde Safe Harbor ordningen, og som tidligere nævnt er Facebook Inc. en af disse virksomheder.

Gennem en hjemmeside på Internettet huser Facebook over 200 millioner registrerede brugere. Brugerne registrerer alt, lige fra navn og adresse, til personlige billeder og skrivelser om hverdagshandlinger. Hjemmesiden er derfor et af de mest omfattende registre i verden, og indeholder millioner og atter millioner af personlige oplysninger om brugerne. Det er derfor nærliggende, at se nærmere på de problemstillinger der opstår når de skal efterleve forpligtigelserne i Safe Harbor, som de tiltrådte d. 10/5-2007[50]

[50] www.export.gov/safeharbor - herunder "safe harbor list"

Datatilsynet i Danmark, der ellers i lang tid fraskrev sig, at behandle sager der vedrørte Facebook, da de mente det ikke var omfattet af Persondataloven, skrev en henvendelse til justitsministeren i november 2008, hvor de anmodede ministeren, om at afgøre hvorvidt Facebook var omfattet af Persondataloven[51], svaret var ikke afvisende, men oplyste at en kontakt til Facebook var nødvendig, for at afklare dette spørgsmål. På denne baggrund skrev Datatilsynet, i april 2009, et brev til Facebook, for at få opklaret en række spørgsmål omkring dennes håndtering af danskernes private oplysninger.[52]

Spørgsmålene, som Datatilsynet stillede, handlede om sletning af profiler, videregivelse af oplysninger til tredjepart, indhentelse af samtykke for behandlingen og ikke mindst hvilken jurisdiktion Facebook hørte under, eller med andre ord, om de var etableret som dataansvarlig i et EU-land. Svaret fra Facebook er endnu ikke kommenteret eller behandlet af Datatilsynet, men indeholdte bl.a., til spørgsmålet om jurisdiktion, denne kommentar:

> »*Facebook is not established as a data controller[53] in the European Community, nor do we have any equipment in Denmark. We do collect information from Danish citizens for processing in the U.S… … While Facebook is not a Data Controller, it aims to act in all instances with the respect*

[51] 2008-131-0012
[52] Henvendelsen til Facebook og svaret, kan læses på datatilsynets hjemmeside – www.datatilsynet.dk
[53] Dataansvarlig

> *that a data controller is expected to show to an individual's personal data.*«[54]

På trods af, at Facebook ikke mener de har en rolle som dataansvarlig, kan det midlertidig konkluderes, at de efter bestemmelserne i Databeskyttelsesdirektivet, ville blive betragtet således, jf. definitionen i art. 2 litra d. Safe Harbor ordningen tager dog ikke stilling til definitionen af en dataansvarlig, men anvender i stedet ordet *foretagendet*.[55] På dette punkt er der altså tale om en væsentlig svækkelse, af de registreredes rettigheder, hvis Facebook kan fraskrive sig rollen som dataansvarlig. I givet fald, ville Safe Harbor ordningen på dette punkt, langt fra yde et tilstrækkeligt beskyttelsesniveau.

Facebook skriver ligeledes i deres svar, at de ikke er etableret som dataansvarlig i et EU-land, og ikke har udstyr stående på dansk grund. Her opstår endnu et uafklaret spørgsmål. Kan Facebooks aktiviteter i Danmark tænkes, at høre under dansk jurisdiktion?
Artikel 29-gruppen offentliggjorde en skrivelse juni 2009, der havde til formål, at afklare nogle af disse spørgsmål.[56] Udover at gruppen gjorde det klart, at et SNS efter direktivet er den dataansvarlige, udtalte de sig også om hvilken jurisdiktion der var gældende. Til dette spørgsmål udtalte gruppen, at på baggrund af, at en SNS genererer store dele af deres indtægter på reklamer, der

[54] jf. note 52
[55] jf. 2000/520/EF – bilag 1
[56] WP-163 – on online social networking

tilpasses brugerne, ud fra de oplysninger de posterer på deres profiler, leverer de et stort marked for virksomheder der er interesseret i denne reklameplads. På denne baggrund mener artikel 29-gruppen, at deres aktivitet er "indkapslet" i en sådan grad, at de nationale regler finder anvendelse[57]. Denne opfattelse har Facebook bl.a. taget afstand fra, i det føromtalte brev[58] til Datatilsynet.

Kigger man på Persondatalovens geografiske anvendelsesområde, lyder udgangspunktet, at den dataansvarlige skal være etableret i Danmark, og aktiviteten skal ske inden for det Europæiske Fællesskabet, jf. § 4, stk. 1. Mere interessant er ordlyden af denne bestemmelses stk. 3 (2), der lyder at »*Loven gælder også for en dataansvarlig, som er etableret i et tredjeland, hvis indsamling af oplysninger i Danmark sker med henblik på behandling i et tredjeland*«
I den kommenteret persondatalov, gives der dog udtryk for, at der skal være tale om en *aktiv handling* fra den dataansvarlige i et tredjeland, der har til formål at tilskynde den registrerede at sende oplysningerne. Yderligere gives et eksempel, hvor en person bosiddende i Danmark *uopfordret* sender oplysningerne til et tredjeland. Det menes ikke, at en sådan situation ville blive omfattet af persondataloven. [Nielsen og Waaben, 2008, s. 137]

Der er ting der taler for og imod, at den danske lovgivning finder anvendelse i "Facebook-situationen". Ydereligere kan tilføjes Da-

[57] WP-163, s. 5
[58] www.datatilsynet.dk - Facebooks svar på henvendelse fra Datatilsynet

tatilsynets afgørelse, om netop persondatalovens anvendelse i forhold til et tredjeland, jf. 2000-631-0034, hvor en thailandsk virksomhed indsamlede data i Danmark. Afgørelsens vigtige punkt i denne sammenhæng var, at tilsynet lagde vægt på, at der var tale om et dansk domænenavn, og at siden henvendte sig til danskere. Facebook ejer domænet "www.facebook.dk"[59], og denne side må i høj grad siges at henvende sig til danskerne. Det ændrer altså på det forhold, at Facebook faktisk foretager en *aktiv handling* for at tilskynde danskere, at registrere sig. Det taler derfor også for at persondataloven finder anvendelse.

Hvis det forudsættes at disse iagttagelser stemmer, og persondataloven finder anvendelse, vil det samtidig betyde, at Safe Harbor modellens rolle bliver ikke-eksisterende, og at Facebook og andre sociale netværkstjenester, skal efterleve reglerne i direktivet, og ikke blot Safe Harbor reglerne (i tilfælde af at de er tiltrådt denne ordning).

7.3.1 Brugerens samtykke

Et vigtigt element, som de sociale netværkstjenester bygger deres retsgrundlag på, er samtykkeerklæringen. Ved at brugeren samtykker til de fremsatte vilkår ved oprettelsen af en profil, gives der således en accept af, at dennes personoplysninger må behandles på den konkrete hjemmeside. Denne fremgangsmåde, er som udgangspunkt, i overensstemmelse med principperne i Safe

[59] www.dk-hostmaster.dk

Harbor, og høj grad direktivets. Dog vil der her opstå et fortolkningsspørgsmål i forhold til samtykket, der giver anledning til komplikationer.

Til at illustrere dette, tages der udgangspunkt i den tidligere nævnte dom, om Sarbanes Oxy Act, jf. 2003-233-0028, som bl.a. drejede sig om et samtykkes gyldighed. Revisorer i et dansk selskab, gav sit samtykke til, at arbejdsgiveren måtte behandle deres personoplysninger. Samtykkeerklæringen indeholdte bl.a. et punkt som tillod arbejdsgiveren, at overføre personoplysningerne til et register i USA. I den amerikanske lov *The Sarbanes Oxy Act*, var dette et krav, hvis en revisor havde amerikanske aktieselskaber som klienter. Da overførslen til det amerikanske register fratog de danske revisorers mulighed for tilbagekaldelse af deres samtykke, fandt datatilsynet, at samtykkeerklæringen var i strid med god databehandlingsskik i § 5.

Facebook har i deres vilkår, en bestemmelse der giver dem mulighed for, at ændre betingelserne for databehandling, forudsat at brugeren bliver gjort opmærksom herpå. Det bemærkelsesværdige i denne sammenhæng er, at der ikke bliver indhentet et nyt samtykke, men at et normal *login* vil blive betragtet som et samtykke.[60] I forhold til fortolkningen af om dette samtykke lever op til kravene i persondataloven, ville Datatilsynet højst sandsynligt komme frem til den samme konklusion, som de gjorde i afgørelsen ovenfor. Nemlig at samtykkeerklæringen ikke lever op til kravet i persondataloven.

[60] www.facebook.com - herunder linket "vilkår"

Safe Harbor ordningen lægger ikke op til, at der kan ske fortolkning i forhold til direktivet, og vil derfor udelukkende blive fortolket efter ordlyden i Safe Harbor aftalen, som ikke stiller lige så store krav til begrebet samtykke. Dette eksempel illustrerer hvordan fortolkningen, på trods af en indgået aftale, kan have forskellige udfald i EU og USA.

7.4 Standardkontrakt - et alternativ til Safe Harbor

Safe Harbor er ikke den eneste metode, der muliggør en overførsel til USA. Dette kan også ske på et aftaleretligt grundlag, hvor importøren accepterer at leve op til det beskyttelsesniveau der kræves i Databeskyttelsesdirektivet. Direktivets artikel 26, stk. 4 siger, at medlemsstaterne træffer de nødvendige foranstaltninger for at efterkomme Kommissionens afgørelser om visse standardkontraktsbestemmelser, der yder tilstrækkelige garantier for beskyttelse af privatlivets fred, grundlæggende rettigheder og frihedsrettigheder samt for udøvelsen af de dertil knyttede rettigheder. Efter proceduren i artikel 31, stk. 2 og med lovhjemmel i art. 26, stk. 2, har Kommissionen offentliggjort disse standardkontraktsbestemmelser.[61] Kommissionens beslutning er tilgængelig vis Datatilsynets hjemmeside.[62]

[61] 2002/16/EC – Kommissionens beslutning om standardkontraktbestemmelser

[62] Det kan som sidebemærkning diskuteres, om Datatilsynet har truffet de nødvendige foranstaltninger for at efterkomme Kommissionens beslutning, som krævet i art. 26 (4), da tilsynets hjemmeside blot henviser til kommissionens side hvor standardkontrakterne er svært tilgængelige for den almene bruger.

I praksis betyder dette, at en virksomhed der ønsker at overføre data til et tredjeland, kan gøre dette såfremt de udarbejder en kontrakt der lever op til kravene i standardkontraktsbestemmelserne fastsat af Kommissionen, og herefter får kontrakten, og dermed overførslen, godkendt af den nationale tilsynsmyndighed. [Nielsen og Waaben, 2008, s. 354 ff.]Dette skette eksempelvis i Datatiljynets j.nr. 2005-841.0076, hvor en amerikansk koncern, anmodede om at overføre data fra deres filial i Danmark, til er tredjeland. Tilsynet tilføjede, at ændringer af kontrakten, eller afvigelser i behandlingsformålet, vil kræve en ny tilladelse.

I samarbejde med artikel 29-gruppen, der for nyligt (Marts 2009) har lavet et udkast til en ny standard kontrakt[63], eller rettere en opdatering af den gamle Lovhjemlen til denne type kontrakter findes i art 26, stk. 4, og virker som en slags "retseksport", hvor en dataimportør forpligtiger sig til, at efterleve kravene i direktivet (eller regler svarende hertil).

En overførsel af persondata til et USA (et tredjeland) kan altså ske ved, at udarbejdelse af en kontrakt der overholder de af Kommissionen fastsatte krav. Det forudsættes dog, at der er tale om en lovlig behandling, i overensstemmelse med resten af lovens bestemmelser.[64] Det er uden betydning, at den amerikanske modtager er tiltrådt Safe Harbor ordningen. Det er dog utænkeligt at dette vil forekomme, da Safe Harbor gør, at en kontrakten ikke er nødvendig. Det kræver blot at man eksporterer oplysningerne til en af de få virksomheder der har tiltrådt ordningen. På baggrund af analysen i kapitel 7, er der dog tale om en bedre be-

[63] Standardkontrakten omtales i WP-161
[64] PDL § 27, stk. 5

skyttelse ved anvendelsen af disse standardkontrakter. Set med den registreredes øjne, er det derfor mest attraktivt, at der anvendes kontrakt, og dertilhørende tilladelse fra datatilsynet, når oplysninger overføres til tredjelande.

8 Konklusion

I 1998 trådte Europa parlamentet og Rådets Direktivet, 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, i kraft. I forbindelse med implementeringen af dette direktiv i Danmark, erstattede Persondataloven de tidligere danske registerlove.

Persondataretten bygger på en af det fundamentale menneskerettigheder, nemlig retten til privatlivets fred, jf. EMRK artikel 8. I nutidens teknologiske informationssamfund, hvor oplysninger nemt og hurtigt kan deles med tusindvis af mennesker, opstår der samtidig større muligheder for integritetskrænkelser og udnyttelse af privates oplysninger. Persondatarettens overordnede formål er derfor, at sikre at behandlingen af personoplysninger sker med en respekt for den registreredes privatliv og integritet, og at de følge heraf frit kan udveksles inden for EU.

Direktivet søger at opnå denne sikkerhed gennem en række principper der bygger på princippet om *god databehandlingsskik,* der indebærer, at *den dataansvarlige* og *databehandleren* skal overholde nogle etiske spilleregler, samt nogle forpligtigelser givet af lovgivningen.

Den reelle virkning af direktivet, bliver dog sat under højere og højere pres i takt med den teknologiske udvikling, da behovet og mulighederne for overførsler af personoplysninger til lande uden for direktivets geografiske anvendelsesområde (Tredjelande), stiger. Grunden til at oplysninger ikke frit kan overføres til tredjelande skyldes, at mange af disse lande ikke har tilstrækkelig lovgivning der regulerer behandlingen af personoplysninger. Hvis oplysninger frit kunne overføres til et land uden lovgivning på området, ville det betyde at direktivets virkning blev ikke-eksisterende.

Direktivet, der som udgangspunkt kun finder anvendelse inden for EU, har dog en række undtagelsesbestemmelser der muliggør, at personoplysninger må overføres, og dermed behandles i tredjelande. Hovedreglen er i denne sammenhæng, at der kun må overføres oplysninger til et tredjeland, såfremt dette land sikrer et tilstrækkeligt beskyttelsesniveau.

USA er et af de lande der betragtes som *tredjeland*, og hvor personoplysninger som udgangspunkt ikke må overføres til. Ved direktivets indførelse i 1998 opstod der hermed en kæmpemæssig handelsbarriere, som hverken EU eller USA var interesseret i, da begge parter har stor kommerciel interesse i, at personoplysninger kan overføres herimellem. På det grundlag opstod *Safe Harbor-modellen*, der er en specialaftale, der muliggør overførsel af personoplysninger til virksomheder, der tiltræder ordningen, og dermed registrerer sig som "Safe Harbor". De tiltrådte virksom-

heder tilkendegiver således, at de underlægger sig Safe Harbor principperne ved behandling af personoplysninger.

Safe Harbor principperne er et udtryk for en kompromis, der som udgangspunkt følger de tilsvarende principper i direktivet. Dog er der tale om nogle "blødere" regler, hvor kravene ikke er lige så stramme som i direktivet.
Dette betyder en svækkelse af den registreredes rettigheder, når personoplysninger overføres til amerikanske virksomheder, med hjemmel i Safe Harbor ordningen.

Problemerne ved Safe Harbor er specielt synlige når det vedrører overførsler gennem Internettet. De såkaldte SNS (Social Network services) repræsenterer nogle af de største databehandlere, hvor millionvis af brugere *offentliggør* personoplysninger via deres profil på en hjemmeside. Facebook Inc. er utvivlsomt den største SNS til dags dato, og i forhold til denne hjemmeside opstår to situationer der giver anledning til skepsis overfor Safe Harbor reglerne.

1. Datatilsynets afgørelse i Sarbanes Oxy Act sagen, gjorde det klart, at et samtykke, der ellers var givet efter de gældende regler i persondataloven om utrykkelighed, alligevel ikke levede op til princippet om god databehandlingsskik, da den registrerede derved mistede muligheden for, at tilbagekalde samtykket. Facebook har, i deres regler, forbeholdt sig retten til at ændre betingelserne for databehandling, uden at dette kræver et nyt samtykke. Her er,

i stil med Sarbanes Oxy Act sagen, tale om et samtykke, hvor der ikke kan gives garanti for, at den registreredes interesser er beskyttet.

2. Når en virksomhed drives gennem Internettet kan være svært at gennemskue hvilken lovgivning der finder anvendelse. I sagen om den Thailandske virksomheds indsamling af data i Danmark via Internettet, lød Datatilsynets afgørelse på, at persondataloven var gældende, da virksomheden foretog *aktive handlinger* for at danskere skulle registrere sig, samt at deres domænenavn var dansk (.dk). Med disse begrundelser er der således meget der taler for, at Facebook også er omfattet af persondataloven.

   Artikel 29-gruppens udtalelse om SNS hjemmesider understøtter ligeledes denne tankegang, på baggrund af, at siderne skaber et reklamemarked nationalt, og derfor skal respektere de nationale lovgivninger.

Den registreredes rettigheder bliver svækket væsentlig, i de tilfælde hvor kravene i Safe Harbor principperne bliver fortolket svagere af de amerikanske myndigheder.

Hvis punkt 2 ovenfor bliver en realitet, vil det medføre en total underminering af Safe Harbor ordningens virkning for en lang række virksomheder der driver virksomhed gennem Internettet.

Reglerne omkring Safe Harbor er generelt meget slørede og svære at gennemskue, og de bærer tydeligt præg af, at den har været

en nødvendighed af politiske og kommercielle grunde. I den nuværende retstilstand er persondataoverførsler til *Safe Harbor virksomheder* en svækkelse af EU-borgenes rettigheder, især fordi ordningen fremlægges som en *sikker overførsel*, hvor de tiltrådte virksomheder behandler data efter samme regler som i Europa. Det er midlertidig ikke helt tilfældet, og Safe Harbor har derfor et lidt misvisende billede udadtil.
Skulle der blive enighed om, at SNS hjemmesiders aktiviteter i EU-medlemslande skal reguleres af direktivet, vil det, indenfor denne branche, medføre en styrkelse af direktivets virkning, og dermed de registreredes rettigheder. Det vil unægteligt også føre en del protester med sig, fra amerikansk side.

Alternativet, når der overføres data til USA, er at udarbejde en kontrakt der lever op til kravene i Kommissionens *standardkontraktsbestemmelser*. På den måde øger man garantien for de registreredes rettigheders, og må på nuværende tidspunkt anses for den mest sikre metode.

9 Litteraturliste

Tranberg, Charlotte Bagger
Nødvendig behandling af personoplysninger
Forlaget Thomson
2007 – 1. Udgave, 1. oplag
1. udgave
ISBN: 978-87-619-1674-7

Blume, Peter
Retlig regulering af internationale persondataoverførsler
Jurist- og Økonomforbundets Forlag
2006
1. udgave
ISBN: 87-574-1363-0

Blume, Peter
Behandling af persondata – en kritisk kommentar
Jurist- og Økonomforbundets Forlag
2003
ISBN: 87-574-0866-1

Werlauff, Faber, Hansen, Hielmcrone, Rønfeldt, Schultz og Tranberg
Erhvervsjura Basisbog
Jurist- og Økonomforbundets Forlag

2007 – 1. Udgave, 1. oplag
ISBN: 978-87-574-1667-1

Nielsen, Kristian Korfits og
Waaben, Henrik
Lov om behandling af personoplysninger med kommentarer
Jurist- og Økonomiforbundets Forlag
2008 - 2. udgave, 1. oplag
ISBN: 978-87-574-1121-8

Andersen, Mads Bryde
IT-Retten
Mads Bryde Andersen og Gads forlag
2005 – 2. Udgave, 1. Oplag
ISBN: 87-13-04907-0 (e-bog) - ISBN: 87-13-04906-2 (fysisk bog)

Sørensen, Karsten Ensig og
Nielsen, Poul Runge
EU-Retten
Jurist- og Økonomiforbundets Forlag
2008 – 4. Udgave, 1. oplag
ISBN: 978-87-574-1669-5

9.1 Hjemmesider

www.datatilsynet.dk

www.export.gov/safeharbor

www.facebook.com/terms.php?ref=pf

9.2 Retskilder

9.2.1 Dansk ret

Lov 2000-05-31 nr. 429 - om behandling af personoplysninger

9.2.2 Eu-ret

95/46/EF	om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger
2002/16/EF	EFT nr. L 006 af 10/01/2002 s. 52 – 62 – Standardkontrakt til overførsel af persondata til tredjelande
2000/520/EF Harbor aftalen	EFT nr. L 215 af 25/08/2000 s. 7 – 47 – Safe

9.3 Domme og afgørelser

9.3.1 Danske domme

U.2007.334 Ø –	Offentliggørelse af cpr. numre på Internettet

9.3.2 EU domme

C- 6/64	Costa vs. E.N.E.L

C-101-01 – Lindquist

9.4 Afgørelser fra Datatilsynet

2008-219-0133 – Bocentret Ringbo

2003-233-0028 – Sarbanes Oxy Act of 2002

2009-631-0071 – Sikkerhedsbrist efter § 41, stk. 3 på Holstebro Tekniske Skole

2000-631-0034 – Thailandsk virksomheds indsamling af personoplysninger i Danmark, omfattet af persondataloven

2008-131-0012 – Henvendelse til Justitsministeriet om persondatalovens anvendelse i forhold til Facebook

2005-841.0076 – Godkendelse af kontrakt for overførsel af data til tredjeland

9.5 Dokumenter fra artikel 29 gruppen

WP-62 Udkast til arbejdsdokument om anvendelsen af Safe Harbor-aftalen i praksis

WP-163 Opinion 5/2009 on online social networking

WP-161 Udkast til ny standardkontrakt, ved overførsel til tredjeland.