Grænseoverskridende behandling af persondata og dataoverførsler til tredjelande med fokus på særlige reguleringsformer beregnet til den private sektor

Cross-border personal data processing and data transfers to third countries focusing on specific legal regulation forms designed for the private sector

af PERNILLE KIRK ØSTERGAARD

Specialet omhandler grænseoverskridende behandling af persondata, herunder overførsel af persondata til tredjelande med fokus på særlige reguleringsformer beregnet til den private sektor, heriblandt særlig fokus på reguleringsformen Binding Corporate Rules og en analyse af reguleringsformens relevans for multinationale koncerner. Til belysning heraf inddrages de relevante aspekter af behandlingsspørgsmålet, databeskyttelsesrettens kilder, de persondataretlige grundbegreber og det persondataretlige overførselsproblem.

Specialet behandler i afsnit 2 databeskyttelsesrettens kilder og fastslår, at der er en nær sammenhæng mellem den menneskeretlige og databeskyttelsesretlige regulering. Derudover gennemgås databeskyttelsesrettens kilder på det fællesskabsretlig plan, og spørgsmålet om fri dataoverførsel inden for EU behandles. Det konkluderes, at der eksisterer en overførselsfrihed inden for EU, men at denne frihed har forskellige begrænsninger på grund af forskelle i den nationale databeskyttelsesregulering.

I afsnit 3 defineres de persondataretlige grundbegreber, herunder behandlings- og overførselsbegrebet. Det konkluderes, at der foreligger et persondataretligt overførselsproblem, og at de særlige retlige reguleringsformer er et udtryk for et forsøg på en løsning af dette problem.

Afsnit 4 belyser overførsel af persondata til tredjelande. De forskellige forudsætninger for overførsel af persondata til tredjelande behandles, og de særlige reguleringsformer inddrages. Der foretages en kort juridisk analyse af udvalgte retlige spørgsmål vedrørende reguleringsformen Binding Corporate Rules. Det konkluderes, at de særlige reguleringsformer er et godt og nødvendigt supplement til de almindelige databeskyttelsesretlige regler, men at de hver især frembyder egne problemer i forhold til de parter, der skal benytte dem.

Afslutningsvist indeholder specialet en konklusion.

Indholdsfortegnelse

1. Indledning

Mange samfundsanalytikere er enige om, at verden siden efterkrigstiden og særligt inden for de sidste 40 år har gennemgået og stadig gennemgår nogle fundamentale forandringsprocesser, som i høj grad påvirker samfunds- og retsudviklingen. Disse forandringsprocesser betegnes ofte som internationalisering og globalisering. Der eksisterer ikke entydige definitioner af de to begreber, hvilket skyldes, at begge begreber er dynamiske og procesrettede, og som følge heraf til stadighed er under revision og udvikling[1]. Desuden kan begrebernes nærmere indhold ofte først afklares i forbindelse med en konkret fastlæggelse af hvilke problemstillinger, der ønskes analyseret og beskrevet. Internationalisering og globalisering kan dermed beskrives i mange dimensioner og med mange variabler. Således definerer eksempelvis Keohane & Milner internationalisering som observerbare strømme af varer, tjenesteydelser og kapital, der bevæger sig på tværs af landegrænserne[2], mens definitionen af globaliseringsbegrebet ofte tager udgangspunkt i Anthony Giddens' definition af begrebet[3]. Giddens fastslår, at globalisering er en intensivering af de verdensomspændende relationer, som medfører, at de geografiske grænser og fysiske lokaliteter mister deres betydning[4].

Drivkræfterne bag den øgede internationalisering og globalisering er blandt andet virksomhedernes stadigt stigende behov for at skabe nye markeder til afsætning af deres produkter og tjenesteydelser og muligheden for at flytte dele af virksomhedsfunktionerne såsom IT-drift til lande, der giver bedre rammebetingelser. Udviklingen bevirker desuden, at virksomhederne i den private sektor i stigende grad vælger at indgå i multinationale koncernstrukturer for at være bedre funderet til fremtidige erhvervsmæssige udfordringer og for at udnytte stordriftsfordelene i den stadig stigende konkurrence. Ved at etablere en koncernstruktur med et overordnet moderselskab, der er hjemmehørende i ét land, og med datterselskaber, der er hjemmehørende i andre lande, opnås der mulighed for, at de enkelte selskaber i koncernen kan fungere under forskellige jurisdiktioner. I retlig henseende udgør de enkelte koncernselskaber en selvstændig juridisk enhed med egne rettigheder og for-

1 Jf. blandt andet Keohane, R. O. & Milner, H. V. (1996): Internationalization and Domestic Politics, kapitel 1 og Kaspersen, L. B. [Ed.] (2005): Globalisering på vrangen, s. 9 f.
2 Jf. Keohane, R. O. & Milner, H. V. (1996): Internationalization and Domestic Politics, s. 3 f.
3 Jf. Kaspersen, L. B. (2005): Globalisering på vrangen, s. 226 samt Andersen, H. & og Kaspersen, L. B. [Eds.] (2005): Klassisk og moderne samfundsteori, kapitel 30.
4 Jf. Giddens, A. (1990): The Consequences of Modernity, s. 64.

pligtelser[5], og ofte vil de ikke være underlagt den samme nationale lovgivning, og det enkelte lands mulighed for juridisk regulering af koncerners internationale adfærd mindskes derfor. Det betyder også, at behovet for retlig regulering, som kan finde anvendelse på tværs af landegrænser, øges, da det ikke er ønskeligt at give koncerner mulighed for at forumshoppe.

Med internationaliseringen og globaliseringen er det moderne informationssamfund en realitet, og der er opstået et betydeligt behov for udveksling af oplysninger på tværs af landegrænser – ikke mindst fordi den internationale samhandel ikke kan fungere uden gensidig informationsudnyttelse og dataudveksling[6]. Især personoplysninger eller persondata[7], der defineres som alle typer oplysninger, der direkte eller indirekte kan relateres til en fysisk, levende person, og som kan anvendes til at identificere vedkommende, har i de seneste år fået enorm opmærksomhed. Denne opmærksomhed er blandt andet baseret på den betydning, persondata har for multinationale koncerner, idet koncerner ofte har et stort behov for at kunne håndtere mange forskellige typer persondata herunder human ressource data, kundedata og finansielle data for at få koncernen til at fungere ledelsesmæssigt og forretningsmæssigt optimalt. Den persondataretlige regulering, databeskyttelsesretten, er således yderst interessant set ud fra forskellige erhvervsmæssige betragtninger:

For det første har den teknologiske udvikling og Internettets udbredelse muliggjort en langt lettere udveksling af persondata end tidligere, da det i dag er muligt med et enkelt klik at sende persondataoplysninger af sted til eksempelvis et datterselskab i Indien. Afhængigheden af denne hurtige og konstante informationsudveksling betyder dog også, at enhver regulering, som forsøger at begrænse denne udveksling, kan få fundamental betydning for multinationale koncerner.
For det andet er EU et af de største markeder i verden, hvad angår global eksport og import af varer og tjenesteydelser[8]. Det betyder også, at såfremt der føres en restriktiv databeskyttelsesregulering, kan dette have en afsmittende effekt på en multinational koncerns bund-

[5] Jf. Krüger Andersen, P. (2008): Aktie- og anpartsselskabsret, kapitel 4 og 15.
[6] Jf. blandt andet Cécile de Terwangne i Gutwirth, S. [et al.], [Eds.] (2009): Reinventing Data Protection?, s. 177.
[7] Den officielle danske oversættelse af Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger (Databeskyttelsesdirektivet) anvender ordet personoplysninger. Specialet anvender dog betegnelsen persondata, idet denne betegnelse må anses for mere universel. Engelsksprogede lande benytter for eksempel betegnelsen personal data.
[8] Jf. nøgletal fra EU vedrørende den globale eksport.

linje, hvis koncernen i vid udstrækning benytter persondata som en handelsvare[9] og i kraft af den restriktive databeskyttelsesregulering bliver pålagt overførselsbegrænsninger og således ikke i samme omfang som tidligere kan handle med disse persondata.
For det tredje kan en tilstrækkelig kvalificeret og fleksibel databeskyttelsesregulering i eksempelvis et EU-medlemsland betyde, at det er attraktivt for multinationale koncerner at placere et datterselskab i det pågældende land med deraf følgende fordele for landet såsom flere arbejdspladser, selskabs-, moms- og afgiftsbeskatning med videre.

På baggrund af det ovenstående er det derfor vigtigt, at der åbnes op for grænseoverskridende dataudveksling blandt andet ved hjælp af en mere fleksibel databeskyttelsesregulering, for at den internationale samhandel kan fungere mest optimalt, men det er også vigtigt, at grundlæggende menneskerettigheder og den personlige integritet ikke krænkes i forsøget på at tilgodese virksomhedernes kommercielle og økonomiske interesser. Dermed er der tale om en svær balancegang, da det hverken er ønskværdigt med en for restriktiv eller en for lempelig regulering.
Udformningen af en kollektiv databeskyttelsesregulering er dog fortsat et område, der er præget af store udfordringer, da de mange forskellige databeskyttelsesretlige traditioner og nationale bestemmelser gør det svært at fastlægge og praktisere et universelt beskyttelsesniveau[10]. Store internationale organisationer som International Chamber of Commerce (ICC) har længe presset på for en retlig regulering – herunder alternativer til en retlig regulering – der muliggør, at multinationale koncerner kan håndtere persondata efter mere enkelte regelsæt[11]. Europa-Parlamentet har også behandlet spørgsmålet om forenkling af de retlige rammer for internationale dataoverførsler[12], og EU har i et vist omfang efterkommet det internationale erhvervsbetonede pres og medvirket til udviklingen af forskellige reguleringsformer til brug for grænseoverskridende behandling af persondata, herunder overførsel af persondata inden for koncerner.

[9] Et eksempel herpå er Google, der blandt andet sælger behavioural targeting. Behavioural targeting gør det muligt at målrette reklamebudskaber mod den besøgende baseret på den adfærd, den besøgende har vist på et website. Det inkluderer blandt andet også indsamling af persondata omkring de besøgende og identifikation af deres adfærd rundt på websitet og historik for andre besøgte websites.
[10] Blume, P. (2008): Databeskyttelsesret, s. 298 f.
[11] Jf. eksempelvis ICC – Policy Statement, s. 1, hvori der opfordres til udarbejdelse af alternative reguleringsmuligheder i forbindelse med overførsel af persondata inden for multinationale koncerner.
[12] Jf. Europa-Parlamentets betænkning om Europa-Kommissionens (Kommissionen) første beretning om gennemførelsen af databeskyttelsesdirektivet, punkt 11.

Behovet for at overføre persondata foreligger såvel i den offentlige som i den private sektor, men årsagerne til behovet er ofte meget forskellige. Mens det offentliges behov for overførsel af persondata hovedsageligt baserer sig på administrative hensyn, så er behovet i den private sektor især af økonomisk og kommerciel karakter. Gode og fleksible muligheder for persondataoverførsler må således betragtes som en forudsætning for, at den private sektor kan fungere optimalt i et moderne informationssamfund. Selvom der i et vist omfang er mange fællestræk ved de retlige problemer og overvejelser i forbindelse med persondataoverførsler inden for den private og den offentlige sektor, retter dette speciale sig udelukkende mod persondataoverførsel inden for den private sektor. Dette valg er truffet på baggrund af, at den grænseoverskridende behandling af persondata og de særlige reguleringsformer, der er udviklet i den forbindelse, har den største almene interesse i relation til den private sektor og belyser mange af de afvejninger, som almindeligvis har betydning for udformningen af databeskyttelsesretten, herunder afvejningen mellem på den ene side de kommercielle og økonomiske interesser i at kunne behandle og overføre persondata og på den anden side beskyttelsen af grundlæggende menneskerettigheder og den personlige integritet.

1.1. Præsentation af specialets problemformulering og fremgangsmåde

Dette speciale er baseret på et ønske om at få belyst nogle af de forskellige databeskyttelsesretlige problemstillinger, der er forbundet med grænseoverskridende behandling af persondata. Specialet vil inddrage de relevante aspekter af behandlingsspørgsmålet herunder databeskyttelsesrettens kilder, de persondataretlige grundbegreber og det persondataretlige overførselsproblem. Derudover vil specialet omhandle overførsel af persondata til tredjelande og fokusere på særlige reguleringsformer beregnet til den private sektor, herunder Kommissionens standardkontrakter og Safe Harbor-ordningen, men med særlig fokus på udvalgte retlige spørgsmål af relevans for multinationale koncerner, der anvender reguleringsformen Binding Corporate Rules[13].

> BCR er en særlig juridisk reguleringsform, der kan vedtages for en koncern, som har virksomheder i flere lande. BCR sikrer et tilstrækkeligt databeskyttelsesniveau i forbindelse med overførsel af persondata fra en enhed eller virksomhed i koncernen, der er beliggende i

[13] Peter Blume anvender betegnelsen bindende virksomhedsregler, men jeg har af begrebshensyn valgt den engelske betegnelse Binding Corporate Rules (BCR). BCR må anses for en mere rammende betegnelse, da den understreger, at kerneområdet for BCR er virksomheder i en koncernkonstellation jf. den engelske oversættelse af corporate, der anvendes som betegnelse for en koncern jf. Svensson, A. L. (2006): Engelsk-dansk økonomisk ordbog. Derudover anvender mange af de europæiske datatilsynsmyndigheder også betegnelsen BCR blandt andet det danske Datatilsyn, det franske CNIL og det hollandske CBP.

EU/EØS[14] til en anden enhed eller virksomhed i koncernen, der er beliggende i tredjelande uden for EU/EØS.

BCR er under stadig forandring, idet den globale udvikling stiller større og større krav til reguleringsformens tilpasningsevne, og det må forventes, at denne reguleringsform kan få stor betydning for multinationale koncerner, idet BCR gør koncerner i stand til at regulere interne forhold med en betydelig effektivitet inden for lovgivningens rammer.

Specialets problemformulering er som følger: *Beskrivelse af den grænseoverskridende behandling af persondata med inddragelse af relevante aspekter af behandlingsspørgsmålet og belysning af overførsel af persondata til tredjelande med fokus på særlige reguleringsformer beregnet til den private sektor, herunder særlig fokus på reguleringsformen BCR og en kort juridisk analyse af udvalgte retlige spørgsmål af relevans for multinationale koncerner, der anvender denne reguleringsform. Analysen vil hovedsageligt bygge på en gennemgang af den såkaldte Artikel 29-gruppes udtalelser vedrørende BCR.*

Specialet vil i afsnit 2 behandle databeskyttelsesrettens kilder og spørgsmålet om den juridiske retskildeværdi af Artikel 29-gruppens udtalelser.
Afsnit 3 vil behandle de persondataretlige grundbegreber, idet disse er grundlæggende for den generelle forståelse af databeskyttelsesretten, og vil beskæftige sig med det persondataretlige overførselsproblem, eftersom dette danner grundlag for den efterfølgende beskrivelse af den grænseoverskridende behandling af persondata.
Afsnit 4 vil belyse mulighederne for overførsel af persondata til tredjelande og herunder inddrage de særlige reguleringsformer beregnet til den private sektor samt foretage en kort juridisk analyse af udvalgte retlige spørgsmål af relevans for multinationale koncerner, der anvender reguleringsformen BCR.
Slutteligt vil afsnit 5 indeholde den konklusion, der kan udledes på baggrund af gennemgangen af behandlingsspørgsmålet, overførsel af persondata til tredjelande og de særlige reguleringsformer.

[14] EØS (Det Europæiske Økonomiske Samarbejdsområde) er en samlebetegnelse for det fælles økonomiske område dannet ved EØS-aftalen mellem EU og Norge, Island og Liechtenstein. Databeskyttelsesdirektivet er tiltrådt af EØS-Komiteén ved beslutning 83/1999 af 25. juni 1999 og efterfølgende implementeret i de tre nævnte lande.

2. Databeskyttelsesrettens kilder

Databeskyttelsesretten er at betragte som et nyt retsområde. Et udsagn med modifikationer vil nogen nok hævde, idet mange af de retsprincipper, der er kendetegnende for databeskyttelsesretten, går langt tilbage. Dette er i et vist omfang også korrekt, da databeskyttelsesretten blandt andet kodificerer grundlæggende menneskeretlige principper om privatlivets fred og integritetsbeskyttelse. Det er dog også åbenbart, at behovet for persondatabeskyttelse og regulering af persondataoverførsler hovedsageligt er opstået som følge af den digitale informationsteknologis, herunder Internettets, udbredelse i de sidste to årtier i det tyvende århundrede, idet den digitale teknologi har muliggjort opbevaring og formidling af persondata i et uoverskueligt omfang. Peter Blume nævner meget rammende, at databeskyttelsesretten er ny, idet den som følge af den moderne informationsteknologi aktualiserer og tydeliggør et beskyttelsesbehov, og fordi beskyttelsen rækker videre end den beskyttelse, som klassiske folkeretlige værn af privatlivets fred tilsigter, da databeskyttelsesretten omfatter enhver type persondata, som er blevet offentliggjort[15].

2.1. Databeskyttelsesrettens folkeretlige baggrund

Databeskyttelsesretten er som juridisk disciplin tæt forbundet med grundlæggende menneskerettigheder, herunder retten til privatlivets fred. Hovedformålet med databeskyttelsesreguleringen er netop at sikre den enkelte borgers privatliv og integritet mod unødige krænkelser, og de folkeretlige tekster er derfor en vigtig del af de retskilder, der danner grundlag for databeskyttelsesretten, eftersom flere af de disse tekster indeholder bestemmelser, der omhandler retten til privatlivets fred.

2.1.1. De menneskeretlige retskilder

På internationalt folkeretligt plan findes Forenede Nationers (FN) Verdenserklæring om Menneskerettighederne af 10. december 1948 (Verdenserklæringen), i hvilken der gives en nærmere præcisering af de økonomiske, sociale, kulturelle, borgerlige og politiske rettigheder. Retten til respekt for privatlivets fred er fastsat i artikel 12:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[15] Blume, P. (2006): Retlig regulering af internationale persondataoverførsler, s. 12. Peter Blumes udsagn uddybes i afsnit 2.1.1.1.

Verdenserklæringen har ikke karakter af en traktat eller konvention og må derfor betragtes som en politisk og moralsk hensigtserklæring, der opfordrer de deltagende medlemsstater til at stræbe efter at fremme respekten for og overholdelsen af de rettigheder, som er nærmere defineret i Verdenserklæringen, uden at staterne herved bliver folkeretlige pligtsubjekter. På trods af, at Verdenserklæringen ikke er juridisk bindende, har den dog dannet grundlag for udvikling af menneskerettigheder både i FN-regi og i regionale institutioner som eksempelvis Europarådet[16]. En retlig udmøntning af principperne i Verdenserklæringen resulterede blandt andet i FN's internationale konvention om civile og politiske rettigheder af 1966 (Konvention 1966), der er folkeretligt bindende for de deltagende stater[17]. Artikel 17 i Konvention 1966, der vedrører privatlivets fred, lyder således:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

En lignende bestemmelse om privatlivets fred findes i artikel 8, stk. 1 i Konventionen til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder af 4. november 1950 – Den Europæiske Menneske-rettighedskonvention (EMRK):

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.

EMRK er i henhold til ordlyden i dens præambel i vidt omfang baseret på principperne og idealerne i Verdenserklæringen, men til forskel fra Verdenserklæringen indeholder EMRK stort set kun artikler, der vedrører civile og politiske rettigheder[18]. Det fremgår af EMRK artikel 1, at de kontraherende parter skal garantere enhver person under deres jurisdiktion de i konventionen sikrede rettigheder og friheder. Det betyder således, at det er staterne, der er pligtsubjekter i forhold til EMRK. Modsætningsvis kan private som eksempelvis enkeltpersoner og virksomheder ikke gøres menneskeretligt ansvarlige på overstatsligt niveau. Der er dermed tale om en pligt uden folkeretligt ansvar for private[19]. Det fremgår endvidere af EMRK artikel 59, at konventionen kun kan tiltrædes af Europarådets medlemsstater. Den folkeretlige rækkevidde af EMRK begrænses dermed set i forhold til det område, som eksempelvis Konvention 1966 dækker, eftersom 152 ud af 192 FN-

[16] Europarådet blev oprettet i 1949 og danner rammen om et samarbejde mellem 47 stater. Rådet omfatter således hele Europa med undtagelse af Hviderusland.
[17] Danmark ratificerede Konvention 1966 ved bekendtgørelse nr. 30 af 29. marts 1976.
[18] I henhold til Den Europæiske Menneskeretskonvention med kommentarer (2003), s. 2 omfatter civile og politiske rettigheder blandt andet beskyttelse af borgernes fysiske integritet og privatsfære.
[19] En diskussion vedrørende den såkaldte Drittwirkung der Grundrechte, der henviser til spørgsmålet om, hvorvidt der under visse omstændigheder kan siges at være en pligt for og mellem private til at overholde konventionens rettigheder, falder uden for dette speciales emneområde.

medlemsstater har tiltrådt Konvention 1966[20]. Det skal dog bemærkes, at EMRK i modsætning til andre menneskerettighedskonventioner såsom Konvention 1966 har etableret et effektivt håndhævelsessystem i form af organer, herunder Den Europæiske Menneskerettighedsdomstol (EMD), som kan træffe bindende afgørelser for medlemsstaterne på grundlag af klager fra enkeltpersoner, der mener, at deres konventionsmæssige rettigheder er krænket. EMRK er inkorporeret i dansk ret ved Lov nr. 285 af 29. april 1992 jf. nu Lovbekendtgørelse nr. 750 af 19. oktober 1998.

En tredje interessant retskilde, der bør nævnes i denne sammenhæng, er Den Europæiske Unions Charter om Grundlæggende Rettigheder (EU-charteret), der blev vedtaget som en politisk erklæring på Nice-topmødet i 2000, og som med Lissabon-traktaten vil få bindende juridisk status. Lissabon-traktaten er i skrivende stund endnu ikke ratificeret af Irland, hvorfor EU-charterets endelige juridiske status er uafklaret, men uagtet denne usikkerhed er charteret meget interessant, da det for første gang i én tekst inkorporerer de europæiske unionsborgeres samlede politiske, økonomiske, borgerlige og sociale rettigheder samt fastlægger rettigheder for alle personer, der opholder sig inden for EU's grænser. I forhold til databeskyttelsesretten er artikel 8 i EU-charteret særlig interessant, idet denne artikel anerkender databeskyttelse som en grundlæggende, uafhængig rettighed løsrevet fra den almindelige grundrettighed om privatlivets fred, der er nævnt i EU-charterets artikel 7. Artikel 8 lyder som følger:

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

Stefano Rodotà betragter processen fra grundfæstningen af privatlivets fred i EMRK artikel 8 til anerkendelsen af databeskyttelsesretten som en uafhængig rettighed i EU-charterets artikel 8 som en endelig afslutning på et langt evolutionært forløb. Dette forløb har ifølge Rodotà adskilt privatlivets fred og databeskyttelsen i to enkeltstående, uafhængige grundrettigheder[21]. Denne udtalelse er meget interessant, idet den rammer kernen i diskussionen vedrørende det indbyrdes forhold mellem den menneskeretlige og den databe-

[20] Jf. Office of the United Nations High Commissioner for Human Rights: Status of Ratifications of the principal International Human Rights Treaties.
[21] Se Stefano Rodotá i Gutwirth, S. [et al.], [Eds.] (2009): Reinventing Data Protection?, s. 77 f.

skyttelsesretlige regulering. En dybdegående gennemgang af denne diskussion falder uden for dette speciales emneområde, men jeg har valgt kort at skitsere og behandle diskussionen i det efterfølgende afsnit, idet jeg ikke mener, at den helt kan udelades, da diskussionen er meget relevant i forhold til databeskyttelsesrettens kilder.

2.1.1.1. Det indbyrdes forhold mellem den menneskeretlige og den databeskyttelsesretlige regulering

Indledningsvis i afsnit 2.1.1. nævnte jeg, at Peter Blume mener, at databeskyttelsen rækker videre end den beskyttelse, som klassiske folkeretlige værn af privatlivets fred tilsigter[22]. Blume henviser i bogen Databeskyttelsesret til, at det er en almindelig antagelse, at EMRK artikel 8 alene omfatter de oplysninger om persondata, der relaterer sig til privatlivets fred, som denne opfattes fra et menneskeretligt synspunkt. Konsekvensen af denne opfattelse er, at beskyttelsen i EMRK artikel 8 kun vil omfatte de persondata, der karakteriseres som følsomme[23], og at de menneskeretlige regler dermed har et mindre bredt anvendelsesområde end de databeskyttelsesretlige regler, der omfatter alle typer persondataoplysninger, som kan henføres til en fysisk person[24].

Spørgsmålet er således, om denne afgrænsning af EMRK artikel 8 er korrekt, hvilket leder hen til diskussionen omkring det indbyrdes forhold mellem den menneskeretlige og den databeskyttelsesretlige regulering.

EMRK artikel 8 er blevet anvendt af både EMD og af EF-Domstolen i sager, der vedrørte persondata, som set ud fra en databeskyttelsesretlig betragtning ikke er følsomme[25]. På baggrund af denne praksis kan det udledes, at det i forhold til anvendeligheden af EMRK artikel 8 er afgørende, i hvilken situation persondataoplysningerne bliver anvendt, snarere end hvilke oplysningstyper, følsomme eller ikke-følsomme, der er tale om. Status af den enkelte persondataoplysning afhænger således af, hvordan den bliver anvendt. Dette betyder dermed, at den menneskeretlige og den databeskyttelsesretlige regulering anlægger en forskelligartet indfaldsvinkel, hvilket medfører, at de to reguleringer ikke i alle tilfælde begge er anvendelige. Hvis der tages udgangspunkt i persondata som beskyttelsesobjekt, betyder det, at databeskyttelsesreguleringen er den bredest virkende. På den anden side har

[22] Blume, P. (2006): Retlig regulering af internationale persondataoverførsler, s. 12.
[23] Følsomme oplysninger er udtømmende defineret i Databeskyttelsesdirektivets artikel 8, stk. 1 jf. Lov nr. 429 af 31. maj 2000 om behandlinger af personoplysninger § 7. Der er tale om oplysninger vedrørende racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold.
[24] Blume, P. (2008): Databeskyttelsesret, s. 81.
[25] For praksis fra EMD se eksempelvis Copland vs. Storbritannien eller Perry vs. Storbritannien. For praksis fra EF-Domstolen se eksempelvis C-465/00.

EMD med den meget vidstrakte fortolkning af EMRK artikel 8 statueret, at begrebet privatlivets fred omfatter mere end blot det private hjem og intimsfæren[26], og at en opdeling af de forskellige persondataoplysninger ikke har betydning set i forhold til et menneskeretligt perspektiv.

Peter Blume påpeger, at forholdet mellem de to reguleringer endnu ikke er fuldt ud afklaret, idet der foreligger et behov for mere retspraksis, før der kan drages en endelig konklusion[27]. Der er dog ikke tvivl om, at der er en nær sammenhæng mellem den menneskeretlige og den databeskyttelsesretlige regulering.

2.1.1.2. Sammenfatning

Sammenfattende kan det fastslås, at Verdenserklæringen og Konvention 1966 understreger, at retten til privatliv er en anerkendt menneskerettighed og en grundlæggende individuel rettighed. EU-charteret har med bestemmelsen i dets artikel 8 stadfæstet databeskyttelsesretten som en grundlæggende, uafhængig rettighed. Charteret har, uanset tvivlen vedrørende dets fremtidige juridiske status, en yderst positiv betydning for databeskyttelsesrettens status som grundlæggende rettighed, og bestemmelsen i artikel 8 illustrerer med al tydelighed databeskyttelsesrettens øgede principielle betydning. Det kan dermed fastslås, at de menneskeretlige bestemmelser om privatlivets fred udgør en meget væsentlig retskilde i forhold til databeskyttelsesretten.

2.1.2. Andre folkeretlige retskilder

De menneskeretlige retskilder udgør som nævnt en vigtig del af fundamentet for databeskyttelsesretten. Disse retskilder er dog også karakteriseret ved, at deres anvendelsesområde er meget bredt. I relation til specialets emne er det derfor interessant at se på andre folkeretlige retskilder, som mere specifikt omhandler den internationale databeskyttelsesret.

Det første epokegørende internationale reguleringsinstrument, der direkte vedrørte databeskyttelse, blev udfærdiget i 1980. Der er tale om Guidelines on the Protection of Privacy and Transborder Flows of Personal Data udarbejdet af Organisation for Economic Cooperation and Development (OECD). Retningslinjerne, der har status som en rekommandation og således ikke er retligt bindende, fastslår en række fundamentale hovedprincipper

[26] Se eksempelvis Peck vs. Storbritannien eller Société Colas Est og andre vs. Frankrig.
[27] Blume, P. (2008): Databeskyttelsesret, s. 82.

for internationale persondataoverførsler[28]. I punkt 17 fastslås et vigtigt princip om fri persondataoverførsel mellem stater, der har tilsluttet sig retningslinjerne. Der er dog mulighed for at fravige dette udgangspunkt, såfremt særlige grunde taler for det. Retningslinjerne giver dermed ikke definitivt mulighed for fri overførsel af persondata mellem de tilsluttede stater.

På trods at, at retningslinjerne ikke er retligt bindende, betragtes de stadig som værende en af de vigtigste standarder inden for international databeskyttelsesret. Peter Blume anfører, at OECD's retningslinjer udgør de basale minimumskrav, som databeskyttelsesreguleringen i et tredjeland under alle omstændigheder skal opfylde for, at en dataoverførsel fra et EU-medlemsland og til et tredjeland kan accepteres og henviser i den forbindelse til en udtalelse fra Artikel 29-gruppen, Working Paper nr. 19 af 3. maj 1999, hvoraf samme synspunkt fremgår[29].

OECD's retningslinjer blev efterfulgt af Europarådets Konvention nr. 108 af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (Konvention 108). Danmark har ratificeret Konvention 108 i 1989, og konventionen udgør således en bindende folkeretlig forpligtelse for Danmark. Ligeledes udgør Konvention 108 en bindende folkeretlig forpligtelse for alle øvrige medlemsstater og EU som institution[30]. Konvention 108 angiver en række grundlæggende principper om databeskyttelse, der er de samme som dem, der er formuleret i OECD's retningslinjer. Konvention 108 fastslår i artikel 12, stk. 2 et princip om fri dataoverførsel mellem de kontraherende stater. Den frie dataoverførsel begrænses dog af artikel 12, stk. 3, der fastsætter en række undtagelser til princippet om fri dataoverførsel. Det kan dermed udledes, at der heller ikke under Konvention 108 eksisterer en ubetinget forpligtelse til at acceptere frie dataoverførsler mellem konventionsstaterne.

OECD's retningslinjer og Konvention 108 har fortsat en vis praktisk betydning for den internationale databeskyttelsesret[31]. OECD's retningslinjer benyttes dog hovedsageligt i lande, der ikke har en fuldt udbygget national databeskyttelsesregulering, og retningslinjerne

[28] De 8 principper er: Collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, accountability. Retningslinjerne suppleres endvidere af OECD's Recommendation on Cross-border Co-operation in the Enforcement of Laws protecting Privacy af 12. juni 2007.

[29] Jf. Blume, P. (2006): Retlig regulering af internationale persondataoverførsler, s. 79 samt Cécile de Terwangne i Gutwirth, S. [et al.], [Eds.] (2009): Reinventing Data Protection?, s. 176 midt. For en gennemgang af begrebet tredjeland henvises til afsnit 3.1.5.

[30] Det er normalt kun muligt for stater at tiltræde konventioner, men ved en justering af Konvention 108 af 15. juni 1999 blev der åbnet for EU's tilslutning.

[31] Foruden de to nævnte internationale reguleringsinstrumenter har FN 14. december 1990 udarbejdet et sæt retningslinjer kaldet Guidelines Concerning Computerized Personal Data Files.

er som nævnt ikke folkeretligt bindende. Konvention 108 er derfor ud fra en retskildemæssig betragtning i denne sammenhæng mere interessant. Konvention 108's fundamentale betydning for Databeskyttelsesdirektivet understreges af, at det i Databeskyttelsesdirektivets præambel, betragtning 11, direkte nævnes, at direktivet er en præcisering og udvidelse af principperne i Konvention 108. Der er imidlertid ingen tvivl om, at den bestemmende dataregulering i EU er Databeskyttelsesdirektivet, idet hverken OECD's retningslinjer eller Konvention 108 har formået at skabe en tilstrækkelig velfungerende retlig ramme for internationale dataoverførsler. Retningslinjerne og Konvention 108 er for det første for åbent udformet, for det andet tillades for mange nationale fravigelser, og for det tredje mangler der konkrete håndhævelsesinstitutioner, som kan sanktionere overtrædelser. Der er dog heller ikke tvivl om, at de forpligtelser og rettigheder, der følger af Databeskyttelsesdirektivet, bygger på det databeskyttelsesretlige grundlag, der er fastsat i Konvention 108 jf. præamblen i Databeskyttelsesdirektivet, betragtning 11, og Konvention 108 er ikke væsensforskellig fra OECD's retningslinjer. Disse reguleringsinstrumenters retskildeværdi i forhold til det eksisterende Databeskyttelsesdirektiv er dermed meget betydelig.

2.2. Databeskyttelsesretten på det fællesskabsretlige plan

2.2.1. Databeskyttelsesdirektivet - Fri overførsel af persondata inden for EU?

Databeskyttelsesdirektivet trådte i kraft den 24. oktober 1998 og fastsatte i artikel 32 et krav om implementering i national lovgivning senest den 24. oktober 1998. For Danmarks vedkommende skete implementeringen noget senere, idet direktivet først blev implementeret ved Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger[32], der trådte i kraft 1. juli 2000.

Reguleringen i Databeskyttelsesdirektivet er baseret på en distinktion mellem dataoverførsler til tre typer af lande: Lande, der er medlem af EU/EØS, tredjelande, der har et såkaldt tilstrækkeligt beskyttelsesniveau samt tredjelande, der ikke antages at have et tilstrækkeligt beskyttelsesniveau. Databeskyttelsesdirektivet fastlægger den almindelig fællesskabsretlige databeskyttelsesregulering og er således udgangspunktet og begrebsafklaringsgrundlaget for enhver grænseoverskridende behandling af persondata fra et EU-/EØS-medlemsland og

[32] Herefter benævnt Persondataloven og forkortet PSL.

til et andet EU-/EØS-medlemsland eller fra et EU-/EØS-medlemsland og til et tredjeland, uanset om der er tale om et tredjeland, der har et tilstrækkeligt beskyttelsesniveau eller ej[33].

Databeskyttelsesdirektivet har to hovedformål, der nævnes i artikel 1, stk. 1 og 2: For det første at sikre et højt fælles databeskyttelsesniveau i EU-/EØS-medlemslandene, og for det andet at sikre den frie overførsel af persondata mellem medlemslandene uden at knytte betingelser eller begrænsninger hertil med henvisning til databeskyttelsesretlige hensyn. Bestemmelsen i artikel 1, stk. 2 om den frie dataoverførsel anses formelt for direktivets hovedformål[34], og i princippet betyder det, at det ikke tillægges betydning, hvordan importlandets[35] regler er udformet, idet disse regler uden videre er acceptable, såfremt der er tale om et EU-/EØS-medlemsland. Det betyder således, at det som udgangspunkt må formodes, at persondata i praksis kan flyde frit inden for EU, og at der er etableret et indre marked for persondataoverførsler. Problemstillingen er dog ikke helt så enkel jf. det nedenstående.

I forbindelse med implementeringen af Databeskyttelsesdirektivet blev det overvejet, om direktivet forudsætter fuld harmonisering, eller om der er tale om et minimumsdirektiv. Peter Blume anfører med rette, at direktivet i sin helhed hverken er et harmoniserings- eller minimumsdirektiv, da det indeholder begge typer af bestemmelser[36]. Dette udgangspunkt er også antaget af EF-Domstolen, der i den såkaldte Lindqvist-sag[37] i sin betragtning, punkt nr. 96 fastslår, at Databeskyttelsesdirektivet principielt set er harmoniserende, for derefter i betragtningen, punkt nr. 97 at påpege, at direktivet samtidig indeholder en række modifikationer til det nævnte udgangspunkt.
Direktivet bygger i vid udstrækning på retlige standarder, og det er vanskeligt at realisere en harmonisering med udgangspunkt i dette præskriptive grundlag. Endvidere er direktivet også præget af subsidiaritetsprincippet, hvilket betyder, at der er overladt medlemslandene visse frihedsgrader i forbindelse med nationale tiltag, retlig udfyldning af reglerne og i forhold til den intensitet, som databeskyttelsen kan reguleres med.
Databeskyttelsesdirektivet har således ikke tilsigtet eller medført en fuldt ud harmoniseret databeskyttelsesregulering, eftersom der fortsat er betydelige nationale forskelle på databe-

[33] Se afsnit 4.1. for en nærmere gennemgang af begrebet tilstrækkeligt beskyttelsesniveau.
[34] Jf. Blume, P. (2008): Databeskyttelsesret, s. 85 samt Rowland, D. & Macdonald, E. (2005).: Information Technology Law, 3. udgave, 2005, s. 323 f.
[35] Importlandet er betegnelsen for modtagerlandet, når persondata, der behandles i medfør af et lands – eksportlandets – lovgivning, flyttes, således at behandlingen nu er omfattet af et andets lands – importlandets – lovgivning.
[36] Blume, P. (2006): Retlig regulering af internationale persondataoverførsler, s. 63 f.
[37] Jf. C-101/01.

skyttelsesreguleringen inden for EU. Disse forskelle beror ikke på de formelle databeskyttelsesretlige bestemmelser i de enkelte medlemslandes lovgivning, idet disse bestemmelser ofte afskriver direktivets regler. Derimod beror de nationale forskelle på medlemslandenes individuelle fortolkning af de formelle bestemmelser. På grund af den abstrakte måde, hvorpå den databeskyttelsesretlige regulering, herunder Databeskyttelsesdirektivet, er udformet og i kombination med rækkevidden og bredden af disse regler, er der opstået en tradition for, at reglerne får deres egentlige juridiske substans via den måde, hvorpå de anvendes og fortolkes i praksis[38]. Det betyder, at selvom en databeskyttelsesretlig regel fremtræder ens i to medlemslande, er der ikke nødvendigvis i praksis tale om et sammenfald med ens anvendelse og fortolkning[39]. Endvidere kan det påpeges, at datatilsynsmyndighederne i medlemslandene er meget forskellige. Direktivet foreskriver i artikel 28, at der skal nedsættes et eller flere tilsyn, men disses kompetence og organisering er varierende[40]. Derudover kan det også nævnes, at der benyttes forskellige typer anmeldelsesformularer i forbindelse med behandling af persondata afhængig af hvilket medlemsland, der er tale om. Dette kan udgøre en stor administrativ belastning for de virksomheder, der har aktiviteter i flere lande inden for EU.

Det kan dermed konstateres, at det første problem i relation til den frie dataoverførsel inden for EU ligger i den databeskyttelsesretlige divergens mellem EU-medlemslandene. Det betyder, at den anførte forudsætning i Databeskyttelsesdirektivet for den frie dataoverførsel – tilsvarende beskyttelsesniveauer i alle medlemslande – forsvinder og rejser spørgsmålet om, hvorvidt formålet med artikel 1, stk. 2 kan opfyldes. Direktivet angiver således i dets præambel, betragtning 9:

> ” …; inden for rammerne af denne manøvremargen og i overensstemmelsen med fællesskabsretten kan der forekomme forskelle i gennemførelsen af direktivet, og dette kan få konsekvenser for udvekslingen af oplysninger såvel inden for den enkelte medlemsstat som på fællesskabsplan;”

Med denne erklæring fastslås det, at formålet i artikel 1, stk. 2 formodentlig ikke vil kunne realiseres fuldt ud.

[38] Blume, P. (2006): Retlig regulering af internationale persondataoverførsler, s. 65.
[39] Som eksempel kan nævnes, at engelsk retspraksis har anlagt en meget snæver definition af begrebet persondata. Den ledende dom er afsagt af Court of Appeal i sagen Michael John Durant vs. Financial Services Authority, hvori appelretten fastslog, at den blotte omtale af en persons navn i et dokument ikke nødvendigvis var at betragte som vedkommendes persondata, men at der skulle knyttes flere oplysninger til personens navn som eksempelvis adresse og telefonnummer. Denne opfattelse strider mod Databeskyttelsesdirektivets brede definition af begrebet persondata. Sagen udløste en formel advarsel fra Kommissionen, der ikke mente, at direktivet var blevet implementeret korrekt.
[40] Eksempelvis har nogle datatilsynsmyndigheder som det engelsk Office of the Information Commissioner mulighed for selvstændige sanktionsbeføjelser i form af eksempelvis bødeudskrivninger, mens det danske Datatilsyn må benytte politiet hertil.

Et andet problem i relation til spørgsmålet om fri overførsel af persondata inden for EU vedrører direktivets anvendelsesområde. Databeskyttelsesdirektivet finder kun anvendelse inden for retsområder, der dækkes af det fællesskabsretlige samarbejde under søjle 1 jf. direktivets artikel 3, 2. punkt[41]. På det undtagne område gælder princippet om fri overførsel af persondata således ikke[42]. Det er objektivt vurderet et problem, eftersom det er mest hensigtsmæssigt, at der gælder den samme databeskyttelsesregulering inden for alle retsområder.

2.2.1.1. Sammenfatning

På baggrund af det ovenstående kan det sammenfattende anføres, at udgangspunktet i Databeskyttelsesdirektivet om fri overførsel af persondata inden for EU ikke er helt definitivt. Den frie dataoverførsel er dog stadig forudsætningen og målet, men en endelig dybdegående harmonisering må anses for illusorisk, idet der formodentlig vil gå mange år, før der foreligger en egentlig harmoniseret europæisk databeskyttelsesret. Det skyldes blandt andet, at de nationale forskelle og de forskellige retskulturer fortsat har en væsentlig indflydelse på databeskyttelsesretten i EU. Det må dog på trods af ovennævnte problemstillinger konkluderes, at der inden for EU gælder et princip om fri overførsel. Der skal således ikke opfyldes særlige betingelser for at foretage en persondataoverførsel til et land inden for EU, og det er følgelig heller ikke nødvendigt at indgive anmeldelse eller opnå tilladelse hertil. Der er imidlertid tale om en frihed med visse begrænsninger og forpligtelser, idet persondata ikke i alle tilfælde kan overføres, da importlandets nationale fortolkning og udfyldning af direktivet kan begrænse denne overførsel. Endvidere kan der i de enkelte medlemslande være tale om forskellige håndhævelsesniveauer af de databeskyttelsesretlige regler. I relation til dataoverførsler til tredjelande uden for EU må det dog fastholdes, at der er inden for EU er tale om overførselsfrihed.

2.3. Artikel 29-gruppen og dets Working Papers som retskilde

Artikel 29 i Databeskyttelsesdirektivet etablerede en "Gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger" – den såkaldte Artikel 29-gruppe. Gruppen er en uafhængig, centralplaceret rådgivningsenhed, der består af en repræsentant for den eller de datatilsynsmyndigheder, som hver medlemsland har udpeget,

[41] Søjle 1 omfatter det klassiske EU-samarbejde (blandt andet Det Indre Marked), søjle 2 indeholder EU's fælles udenrigs- og sikkerhedspolitik, mens søjle 3 omhandler politi- og retssamarbejdet.
[42] Der findes enkelte andre undtagelser herunder behandling af persondata til familiemæssige og personlige formål. Disse undtagelser er ikke relevante for dette speciale og vil ikke blive omtalt yderligere.

og af en repræsentant for den eller de myndigheder, der er oprettet for fællesskabsinstitutionerne og -organerne, samt af en repræsentant for Kommissionen[43].

Artikel 29-gruppen udfylder en vigtig rolle i relation til den europæiske databeskyttelsesret, idet gruppen fremkommer med forskellige udtalelser og henstillinger, der udmønter sig i de ud fra et databeskyttelsesretligt synspunkt meget vigtige fortolkningsdokumenter kaldet Working Papers (WP). Det interessante i forbindelse med Artikel 29-gruppens WP er, at disse fortolkningsdokumenter alene er af vejledende og ikke juridisk bindende karakter. Spørgsmålet er dermed, om retskildeværdien af disse WP kan tillægges nogen signifikant betydning?

For det første bør der ses på Artikel 29-gruppens generelle kompetencer. I henhold til det ovenstående har Artikel 29-gruppen kun mulighed for at komme med henstillinger og udtalelser. Henstillinger og udtalelser er EU-retsinstrumenter inden for søjle 1, som ikke er bindende jf. EF-Traktatens artikel 249, 5. punkt, og disse retsakter kan således ikke prøves ved EF-Domstolen jf. EF-Traktatens artikel 230, stk. 1. Enhver retshåndhævelse af de henstillinger og udtalelser, der fremkommer i gruppens WP, og som er rettet mod personer og virksomheder, må således gå gennem nationale ret og anlægges ved de nationale domstole eller indbringes for de stedlige datatilsynsmyndigheder[44]. På trods af de manglende juridisk bindende beføjelser bør Artikel 29-gruppens kompetencer ses i et bredere perspektiv. I relation hertil kan nævnes, at Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor i artikel 15 tillægger Artikel 29-gruppen kompetence til at beskytte grundlæggende rettigheder og frihedsrettigheder samt legitime interesser i den elektroniske kommunikationssektor. Derudover bør Artikel 29-gruppens kompetencer også ses i lyset af, at EF-Domstolen i henholdsvis Lindqvist-sagen og Rechnunghof/-Österreichischer Rundfunk-sagen[45] har fastslået, at Databeskyttelsesdirektivet har et meget bredt anvendelsesområde, der strækker sig ud over grænserne for Det Indre Marked. I sammenhæng med EF-Domstolens udtalelser i de nævnte sager og med EU-charterets anerkendelse af databeskyttelsesretten som en grundlæggende, uafhængig rettighed, kan det hævdes, at tendensen går i retning af en udvidelse af Artikel 29-gruppens kompetencer ud

[43] Henset til, at Artikel 29-gruppen både rådgiver Kommissionen og udtaler sig om dennes initiativer, forekommer det problematisk, at Kommissionen ligeledes er medlem af Artikel 29-gruppen og fungerer som sekretariat for denne jf. Databeskyttelsesdirektivets artikel 29, stk. 5 uagtet, at Kommissionen ikke har nogen stemmeret.
[44] Jf. Kuner, C. (2007): European Data Protection Law, s. 50.
[45] Jf. C-465/00.

over dem, gruppen på nuværende tidspunkt er tillagt i henhold til Databeskyttelsesdirektivet. Det bør ligeledes bemærkes, at Artikel 29-gruppen i Databeskyttelsesdirektivets artikel 30, stk. 3 er tillagt en særlig kompetence til på eget initiativ at fremsætte henstillinger om ethvert spørgsmål vedrørende beskyttelsen af personer i forbindelse med behandling af persondata inden for Fællesskabet. Denne kompetence rækker ud over Artikel 29-gruppens rolle som rådgivningsenhed for Kommissionen, og gruppen fungerer således både som rådgivningsenhed for Kommissionen og for andre EU-institutioner, herunder Europa-Parlamentet, der er involveret i beslutningsprocesser vedrørende databeskyttelse, samt for forskellige kategorier af dataansvarlige. I kraft af denne kompetence i Databeskyttelsesdirektivet artikel 30, stk. 3 kan Artikel 29-gruppen således beskæftige sig med mere generelle og i nogle tilfælde endda søjleuafhængige problemstillinger, der vedrører persondatabeskyttelse.

For det andet kan det næppe betvivles, at Artikel 29-gruppen har opnået en betydelig indflydelse i kraft af, at gruppen er sammensat af repræsentanter fra de europæiske datatilsynsmyndigheder. Det enkelte datatilsyn vil i sin nationale praksis med overvejende sandsynlighed, om end ikke med nødvendighed, lægge de synspunkter til grund og følge de WP, som tilsynet i Artikel 29-gruppen selv har været med til at formulere.

For det tredje er det i forbindelse med retskildediskussionen af Artikel 29-gruppens WP meget relevant at nævne Europa-Parlamentets beslutning af 4. september 2007 om institutionelle og retlige virkninger af anvendelse af soft law-instrumenter. I denne beslutning henvises der i litra C til, at de såkaldte soft law-instrumenter som for eksempel henstillinger og udtalelser ikke har nogen retlig værdi eller bindende virkning. Europa-Parlamentet anfører dog i litra R, at EF-Domstolen ikke desto mindre i den såkaldte Grimaldi-dom har fastslået, at sådanne retsakter ikke kan anses for at være ganske uden retsvirkninger:

> ”Da henstillinger ikke kan anses for at være ganske uden retsvirkninger, skal de nationale retsinstanser dog ved afgørelsen af tvister, der indbringes for dem, tage hensyn til henstillinger, navnlig når disse kan bidrage til fortolkningen af nationale bestemmelser udstedt til gennemførelse heraf, eller når der er tale om henstillinger, som har til formål at udfylde bindende fællesskabsretlige bestemmelser”.[46]

På baggrund af EF-Domstolens erklæring i Grimaldi-dommen kan det dermed ikke udelukkes, at henstillinger – uanset at de ikke er juridisk bindende – kan tjene som retskilde. Dette betyder således, at der skal tages hensyn til henstillinger ved fortolkning og udfyld-

[46] Jf. C-322/88, sammendragets 3. punkt samt præmis 16 og 18.

ning. Ifølge Morten Wegener kan der ved ikke-bindende retsakter dog højst være tale om en fakultativ hensyntagen og ikke en obligatorisk[47].

2.3.1. Sammenfatning

Sammenfattende kan det konkluderes, at Artikel 29-gruppens kompetencer i form af udtalelser og henstillinger, der udmønter sig i gruppens WP, er en vigtig og betydningsfuld retskilde i forbindelse med grænseoverskridende behandling af persondata. Uagtet, at Artikel 29-gruppens WP ikke er juridisk bindende, og der således kun kan være tale om en fakultativ hensynstagen, vil der på baggrund af det ovennævnte næppe være tvivl om, at de nationale datatilsynsmyndigheder og andre adressater vil tage hensyn til og føle sig forpligtet til at følge Artikel 29-gruppens henstillinger – dette også henset til EF-Domstolens erklæring i Grimaldi-dommen.

3. De persondataretlige grundbegreber og overførselsproblemet

3.1. De persondataretlige grundbegreber

I relation til den senere fremstilling vil det være hensigtsmæssigt at introducere de persondataretlige grundbegreber, idet disse ligger til grund for forståelsen og vurderingen af de databeskyttelsesretlige problemstillinger, herunder den grænseoverskridende behandling af persondata og overførsler til tredjelande. Grundbegreberne udledes af de retskilder, som ligger til grund for databeskyttelsesretten; i særdeleshed Databeskyttelsesdirektivet og i et vist omfang også den supplerende regulering samt administrativ og judiciel praksis. Databeskyttelsesdirektivet indeholder legaldefinitioner af en række af de persondataretlige grundbegreber jf. direktivets artikel 2, litra a-h, der i vidt omfang er videreført i PSL. Af størst interesse i forhold til dette speciales emne er grundbegreberne *persondata, behandling, den registeransvarlige* og *registerfører*. Begrebet *tredjeland* må også anses for et yderst væsentligt persondataretligt grundbegreb i denne sammenhæng. Dette begreb er ikke på samme måde som de andre nævnte grundbegreber legaldefineret i Databeskyttelsesdirektivet, men betegnelsen *tredjeland* er dog udtrykkelig nævnt og anvendt i direktivet – både i præamblen og i de enkelte artikler, herunder de for den senere fremstilling meget væsentlige artikler 25 og 26 jf. PSL § 27, der vedrører overførsel af persondata til tredjelande.

[47] Jf. Wegener, M. (2000): Juridisk Metode, s. 238 f.

3.1.1. Persondata

Genstanden for en grænseoverskridende behandling er persondata, der er legaldefineret i Databeskyttelsesdirektivets artikel 2, litra a jf. PSL § 3, nr. 1. Det fremgår af artikel 2, litra a, at persondata er enhver form for information, der kan henføres til en identificeret eller identificerbar person. Ved udtrykket identificerbar person skal forstås en person, der direkte eller indirekte kan identificeres. Det kan eksempelvis være ved et identifikationsnummer eller ved et eller flere elementer, der er særlige for en given persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet. Omfattet af begrebet persondata er herefter oplysninger, som kan henføres til en fysisk person, selv om dette forudsætter kendskab til personnummer, registreringsnummer eller lignende særlige identifikationer som eksempelvis et løbenummer. Omfattet vil også være oplysninger, der foreligger i form af eksempelvis et billede, et fingeraftryk, en persons stemme eller genetiske kendetegn. Der er således tale om en meget bred definition[48]. Omvendt indebærer definitionen i Databeskyttelsesdirektivet og PSL, at oplysninger, der er gjort anonyme på en sådan måde, at den fysiske person ikke længere kan identificeres, ikke er omfattet af begrebet persondata, idet der for sådanne oplysninger ikke er nogen risiko for integritetskrænkelser. Eksempelvis vil en virksomheds overførsel af en generel karakteristik af de ansatte ikke udgøre en overførsel af persondata, medmindre der er tale om så få ansatte, at det på trods af den generelle karakteristik vil være muligt at identificere personerne[49].

3.1.2. Behandling

Behandlingsbegrebet er et andet af databeskyttelsesreguleringens absolutte kernebegreber. Behandling er defineret i Databeskyttelsesdirektivets artikel 2, litra b jf. PSL § 3, nr. 2, der fastslår, at en behandling er enhver operation eller række af operationer – med eller uden brug af elektronisk databehandling – som persondata gøres til genstand for. Det gælder eksempelvis indsamling, registrering, systematisering, brug, opbevaring, søgning, sammenstilling, udvælgelse, videregivelse og tilintetgørelse[50]. Direktivets eksemplifikationer af behandlingsbegrebet kan ikke anses for udtømmende på grund af artiklens formulering, og det må fastslås, at behandlingsbegrebet omfatter enhver form for håndtering af oplysninger. Der vil således være tale om en behandling af persondata, hvis blot en af de nævnte former for håndtering af oplysninger finder sted. I relation til dansk ret betyder det, at be-

[48] Jf. Betænkning om behandling af personoplysninger nr. 1345/1997, s. 210 f. samt Artikel 29-gruppens WP 136 af 20. juni 2007.
[49] Blume, P. (2006): Retlig regulering af internationale persondataoverførsler, s. 17.
[50] I artikel 2, litra b opremses yderligere en række eksempler på behandling, som ikke nævnes her.

handlingsbegrebet er udvidet i forhold til de oprindelige registerlove[51], der kun omfattede registre og videregivelse af de registrerede oplysninger. Behandlingsbegrebet skal dermed forstås og fortolkes i ekstensiv forstand, hvilket betyder, at begrebet favner bredt og omfatter alt, der kan forekomme, fra der sker indsamling af persondata, til disse bliver slettet eller arkiveret.

Behandlingsbegrebets kompleksitet og mange facetter er genstand for adskillige teoretiske overvejelser, og en kort gennemgang af behandlingsbegrebet yder ikke dette fuld retfærdighed. I dette speciale har jeg dog – især af hensyn til læseren – valgt at medtage og fokusere på de dele af behandlingsbegrebet, som direkte relaterer sig til problemstillingen med den grænseoverskridende behandling af persondata. Det er i sagens natur overførselsspørgsmålet, der er af størst interesse her, og som det vil fremgå af senere afsnit, har overførselsspørgsmålet en tæt sammenhæng med behandlingsbegrebet. Når jeg i dette afsnit om behandlingsbegrebet har valgt ikke at medtage overførselsspørgsmålet, skyldes det, at en sådan gennemgang forudsætter et kendskab til andre persondataretlige grundbegreber – den dataansvarlige, databehandleren og tredjeland – og derfor har jeg valgt at lade gennemgangen af overførselsspørgsmålet være et selvstændigt afsnit.

3.1.3. Den registeransvarlige – den dataansvarlige

Mange af de forpligtelser, der følger af Databeskyttelsesdirektivet, påhviler den registeransvarlige, og begrebet er defineret i direktivets artikel 2, litra d jf. PSL § 3, nr. 4, der i stedet anvender betegnelsen den dataansvarlige[52]. En dataansvarlig er den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler, der må foretages behandling af persondata. Status som dataansvarlig tillægges så snart, eksempelvis en juridisk person vælger at foretage en persondatabehandling og udøver bestemmelsesretten over denne databehandling. Den dataansvarlige, pligtsubjektet, er således den fysiske eller juridiske person med flere, som over for de registrerede[53], rettighedssubjekterne, har det umiddelbare ansvar for behandlingen, og som har dispositionsretten over de oplysninger, der indgår i behandlingen.

[51] Forinden PSL trådte i kraft den 1. juli 2000 var gældende lovgivning inden for området Lov nr. 293 af. 8. juni 1978 om private registre samt Lov nr. 294 af 8. juni 1978 om offentlige myndigheders registre med senere ændringer.
[52] Det vil ligeledes være den betegnelse, som dette speciale anvender.
[53] I Databeskyttelsesdirektivet og i PSL anvendes betegnelsen den registrerede, hvorfor dette speciale også benytter denne terminologi på trods af, at databeskyttelsesreguleringen dækker over mere end blot registrering af persondata. Den engelske betegnelse data subject ville i så henseende være mere korrekt.

En effektiv persondatabeskyttelse afhænger dermed af en korrekt identifikation af den dataansvarlige. I en globaliseret verden med komplekse koncernstrukturer er det ikke altid let at fastlægge, hvem der er dataansvarlig, og det kan forekomme, at der må foretages en mere dybdegående analyse. Et spørgsmål i relation hertil kan være, hvem der anses for dataansvarlig, hvis persondata sendes rundt mellem de enkelte selskaber i koncernen. I den forbindelse er det vigtigt at fastholde, at ethvert selskab – uanset om der er tale om moderselskabet eller datterselskaber – er en selvstændig juridisk person med deraf følgende databeskyttelsesretlige forpligtelser. Hvert enkelt selskab inden for koncernen kan derfor være dataansvarlig i forhold til de persondata, som selskabet behandler. Der kan dog også være tale om, at det enkelte selskab er databehandler jf. nedenstående afsnit.

3.1.4. Registerfører – databehandleren

Begrebet registerfører er defineret i Databeskyttelsesdirektivets artikel 2, litra e jf. PSL § 3, nr. 5, der i stedet anvender betegnelsen databehandleren[54]. En databehandler er den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne. En afdeling som for eksempel en human ressource-afdeling, der generelt behandler persondata på vegne af det selskab, hvori afdelingen er hjemmehørende, vil ikke i direktivets forstand være databehandler, idet der ikke er tale om en selvstændig juridisk person. Derimod vil et selskab, der har til formål at behandle persondata på vegne af moderselskabet[55], være en selvstændig juridisk person og skal i et sådan tilfælde anses for databehandler. Det skal endvidere påpeges, at det er den dataansvarlige, der er direkte ansvarlig over for de registrerede for enhver ulovlig behandling af persondata, og ikke databehandleren, idet denne blot behandler persondata på den dataansvarliges vegne.

3.1.5. Tredjeland

Grundbegrebet tredjeland er jf. afsnit 3.1. ikke udtrykkeligt defineret i Databeskyttelsesdirektivet. I overensstemmelse med den bagvedliggende hensigt med direktivets artikel 25 samt den definition, der er indsat i PSL § 3, nr. 9, må tredjeland forstås som en samlebetegnelse for alle de lande, direktivet ikke er adresseret til. Det vil sige lande, som ikke er medlem af EU[56], eller som ikke har gennemført en lovgivning, der svarer til Databeskyttel-

[54] Det vil ligeledes være den betegnelse, som dette speciale anvender.
[55] Det kan være et selskab i koncernen, der har fået overladt alle lønrelaterede opgaver.
[56] Jf. også Betænkning om behandling af personoplysninger nr. 1345/1997, s. 223 f. samt Waaben, H. & Nielsen, K. K. (2008): Lov om behandling af personoplysninger med kommentarer, s. 130.

sesdirektivets regler. Idet EØS-landene jf. note 14 har gennemført en sådan lovgivning, betragtes disse lande derfor ikke længere som tredjelande i forhold til direktivet, men sidestilles med et EU-land. Alle andre lande vil således skulle betragtes som tredjelande, hvilket medfører, at der som udgangspunkt kun kan ske overførsel af persondata til disse lande, såfremt der foreligger et tilstrækkeligt beskyttelsesniveau jf. direktivets artikel 25 og 26 jf. PSL § 27, eller der anvendes en af de særlige reguleringsformer, som i kraft af deres natur kan yde tilstrækkelig garanti for beskyttelse af de registreredes persondatarettigheder.

3.2. Overførselsbegrebet

Behandlingsbegrebet er som tidligere nævnt meget bredtfavnende og dækker over mange forskellige underkategorier af begreber. I relation til den grænseoverskridende behandling af persondata påkalder især overførselsbegrebet sig interesse.

Der er i teorien enighed om, at en overførsel er en behandling[57], men hvad der skal forstås ved en overførsel, kan give anledning til tvivl, eftersom der i Databeskyttelsesdirektivet ikke findes en legaldefinition af begrebet. En definition af overførselsbegrebet er dog ofte indeholdt i EU-medlemslandenes nationale databeskyttelsesreguleringer, hvilket eksempelvis er tilfældet for den tyske Bundesdatenschutzgesetz:

> Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
>
> a) die Daten an den Dritten weitergegeben werden oder
>
> b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft.[58]

og den hollandske Wet bescherming persoonsgegevens:

> "Processing of personal data" shall mean: any operation or any set of operations concerning personal data, including in any case the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as blocking, erasure or destruction of data.[59]

PSL anvender begrebet overførsel i § 27, men der er ikke i selve lovteksten indeholdt en definition heraf. Forarbejderne til PSL viser imidlertid betænkningsudvalgets overvejelser omkring overførselsbegrebet. Udvalget bemærkede i sin betænkning, at Databeskyttelsesdirektivet anvender betegnelsen videregivelse i artikel 25 og 26. I den på det tidspunkt

[57] Jf. blandt andet Blume, P. (2006): Retlig regulering af internationale persondataoverførsler, s. 21 samt Kuner, C. (2007): European Data Protection Law, s. 159.
[58] Jf. Bundesdatenschutzgesetz § 3, nr. 4, 3. punkt.
[59] Jf. Wet bescherming persoonsgegevens, artikel 1, litra b. Af hensyn til den sproglige forståelse af bestemmelsen er der i stedet for den originale formulering på hollandsk medtaget den uofficielle engelske oversættelse fra det hollandske datatilsyn CBP.

gældende registerlovgivning[60] blev udtrykket videregivelse benyttet om en overførsel af oplysninger til enhver anden end den registrerede, den dataansvarlige, databehandleren og personer under den dataansvarlige eller databehandlerens direkte myndighed. En overførsel af oplysninger til en dataansvarlig eller personer under den dataansvarliges direkte myndighed blev betegnet som en overladelse af oplysningerne og ikke som en videregivelse. Når personer under den dataansvarliges direkte myndighed anvendte oplysningerne, blev det betegnet som intern anvendelse af oplysningerne og heller ikke som en videregivelse. Udvalget fastslog derfor, at hensigten med betegnelsen videregivelse i artikel 25 og 26 i Databeskyttelsesdirektivet havde et bredere sigte. Udvalget lagde i denne forbindelse vægt på blandt andet den engelske og franske implementering af Databeskyttelsesdirektivet, hvori betegnelsen videregivelse er benævnt henholdsvis transfer og transfert samt den tyske implementering af direktivet, hvori der er anvendt udtrykket Übermittlung[61], hvilket betyder fremsendelse, transmission eller lignende. Endvidere tillagde udvalget det vægt, at en overførsel af oplysninger til personer, juridiske som fysiske, der under den dataansvarliges direkte myndighed var beføjet til at behandle oplysningerne – det vil sige en intern anvendelse – ligesom enhver anden form for overførsel kunne indebære en risiko for krænkelse af den registreredes integritet. Også en sådan overførsel af oplysninger fandt udvalget var omfattet af reguleringen i Databeskyttelsesdirektivets artikel 25 og 26. Tilsvarende måtte antages at gælde for en databehandler i et tredjeland. På den anførte baggrund fandt udvalget, at bestemmelserne i direktivets artikel 25 og 26 måtte antages at omfatte enhver form for overførsel af oplysninger til tredjelande, uanset om der var tale om en videregivelse i den betydning, de dagældende registerlove benyttede, intern anvendelse eller en overladelse[62].

Overførselsbegrebet i PSL § 27 skal således anvendes som en samlebetegnelse, der omfatter tre former for behandling:
For det første omfatter overførselsbegrebet videregivelse, der indebærer, at persondata flyttes til en anden enhed med selvstændig retlig eksistens. Eksempelvis er der tale om videregivelse, når persondata flyttes mellem selskaber, der er koncernforbundne.

[60] I 1997, hvor udvalget afgav sin betænkning, var gældende registerlovgivning de i note 51 nævnte love.
[61] Jf. ovenstående citering af Bundesdatenschutzgesetz § 3, nr. 4, 3. punkt.
[62] Jf. Betænkning om behandling af personoplysninger nr. 1345/1997, s. 282 f.

For det andet omfatter overførselsbegrebet den dataansvarliges interne anvendelse af persondata eksempelvis ved flytning af persondata fra en afdeling til en anden inden for samme selskab.
For det tredje omfatter overførselsbegrebet overladelse, hvorved forstås flytning af persondata til en databehandler eller personer under databehandlerens direkte myndighed, der udfører en opgave på vegne af den dataansvarlige og i overensstemmelse med dennes instruks.

3.2.1. Den nationale lovgivnings betydning for overførselsbegrebet

På baggrund af gennemgangen i ovenstående afsnit kan det således fastslås, at en overførsel er en behandling, og at overførselsbegrebet vedrører spørgsmålet om, hvorvidt det retligt set er muligt at flytte persondata fra et lands jurisdiktion til et andet lands jurisdiktion. Overførselsbegrebet vedrører dermed alene eksportlandets regulering i forhold til muligheden for at flytte persondata ud af landet. Med dette udgangspunkt er det dermed også af stor betydning at få fastlagt, hvorledes den databeskyttelsesretlige regulering fastlægger det civile lovvalg, og hvorledes den nationale lovgivning har indvirkning på og betydning for overførselsbegrebet.

I henhold til Databeskyttelsesdirektivets artikel 4 jf. PSL § 4 er hovedreglen, at det er etableringslandet, der er bestemmende for lovvalget. Det betyder, at PSL gælder for behandlinger af persondata, der udføres for en dataansvarlig, der er etableret i Danmark, og hvis aktiviteter foregår inden for EU[63]. Det er således en forudsætning for, at en overførsel kan finde sted, at de pågældende persondata af dataeksportøren[64] bliver behandlet i overensstemmelse med eksportlandets databeskyttelsesretlige regler. Dataeksportøren skal dermed lovligt være i besiddelse af og foretage lovlig behandling af de pågældende persondataoplysninger. Dette princip er klart udtrykt i Databeskyttelsesdirektivets artikel 25, stk. 1 jf. præamblens betragtning, punkt nr. 60 og PSL § 27, stk. 5, hvoraf det fremgår, at en dataoverførsel skal være baseret på en nationalt lovlig behandling. Hvis disse betingelser ikke er opfyldt, kan der som udgangspunkt ikke ske en persondataoverførsel. De førnævnte regler er møntet på eksport af persondata til tredjelande, men princippet om, at der skal foreligge en national lovlig behandling er tillige gældende inden for Databeskyttelsesdirekti-

[63] Etablering skal jf. Databeskyttelsesdirektivets præambel, betragtning 19 forstås som faktisk udøvelse af aktiviteter gennem en mere permanent struktur. Den retlige struktur er uden betydning, og aktiviteter, der udøves af såvel filialer som datterselskaber, er omfattet.
[64] En dataeksportør kan eksempelvis være en virksomhed.

vets område. Forskellen er blot, at tredjelande i henhold til direktivets bestemmelser i artikel 25 og 26 skal opfylde yderligere betingelser ud over betingelsen om, at behandlingen efter de nationale regler skal være lovlig, før en dataoverførsel kan finde sted.

3.3. Sammenfatning

På baggrund af ovenstående gennemgang af de persondataretlige grundbegreber, overførselsbegrebet og de problemer, der er forbundet hermed, kan det således sammenfattes, at der foreligger et persondataretligt overførselsproblem. Dette problem opstår som følge af, at de persondata, der før var beskyttet af den nationale lovgivning, efter overførslen befinder sig i et andet jurisdiktionsområde, hvor de førgældende nationale regler ikke finder anvendelse. Såfremt der er tale om et jurisdiktionsområde, der har de samme regler eller mere beskyttende regler i forhold til de registrerede, er det ikke umiddelbart et problem[65], men det bliver problematisk, når reglerne i importlandet stiller de registrerede dårligere eller slet ikke yder dem nogen persondatabeskyttelse overhovedet. Persondatabeskyttelsen undermineres dermed, hvis det – set i forhold til den førgældende nationale lovgivning – uden retlige restriktioner er muligt at flytte persondata til en jurisdiktion, der anvender persondata mere frit og øger risikoen for integritetskrænkelser. På den anden side er det heller ikke ønskeligt for globaliseringen og internationaliseringen, hvis den retlige regulering i forbindelse med grænseoverskridende behandling af persondata satte så snævre retlige rammer for dataoverførslerne, at sådanne overførsler ikke ville være mulige. Den retlige regulering, herunder de særlige reguleringsformer, er således udtryk for et forsøg på at finde en løsning på det persondataretlige overførselsproblem.

4. Overførsel af persondata til tredjelande

4.1. Det tilstrækkelige beskyttelsesniveau – tilstrækkelighedsnormen

Databeskyttelsesdirektivet sikrer, at der i de enkelte EU-medlemslande er etableret og gennemført en databeskyttelsesretlig regulering med et beskyttelsesniveau som fastsat i direktivet. Det beskyttelsesniveau og den sikkerhed, som Databeskyttelsesdirektivet yder, foreligger set ud fra en fællesskabsretlig betragtning ikke i tredjelande. Det betyder således, at det hverken er forsvarligt eller hensigtsmæssigt af hensyn til integritetsbeskyttelsen at have fri dataoverførsel til tredjelande. Selvom udgangspunkt for den grænseoverskridende behandling af persondata er, at der nationalt set skal være tale om en lovlig behandling, vil

[65] Jf. også den tidligere diskussion vedrørende overførsler inden for EU i afsnit 2.2.

denne forudsætning – blandt andet på grund af de retlige problemer, der foreligger i de enkelte medlemslande – ikke i sig selv kunne sikre imod overførsler til tredjeland, hvor persondata vil kunne behandles uden begrænsninger og med risiko for integritetskrænkelser. På denne baggrund tager Databeskyttelsesdirektivet i artikel 25, stk. 1 jf. PSL § 27, stk. 1 udgangspunkt i en norm om, at importlandets retlige regulering skal sikre et tilstrækkeligt beskyttelsesniveau – den såkaldte tilstrækkelighedsnorm. Ud fra denne norm, der ikke er særlig præcis formuleret eller uddybet i Databeskyttelsesdirektivet, kan det udledes, at direktivets grundlæggende regler og principper skal være accepteret i importlandets retlige regulering, således at en overførsel af persondata ikke medfører en væsentlig forringelse af den beskyttelse af den registrerede, som er tilsigtet efter Databeskyttelsesdirektivet og PSL. Behandlingen af persondata i det pågældende tredjeland skal derfor i det væsentligste være undergivet en regulering som den, der følger af direktivet og PSL.

En vurdering af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, sker på grundlag af samtlige de forhold, der har indflydelse på en overførsel, herunder navnlig hvilke type persondata, der er tale om, behandlingens formål og varighed, eksportlandet og det endelige importland, samt de retsregler, regler for god forretningsskik og sikkerhedsforanstaltninger, som gælder i tredjelandet jf. Databeskyttelsesdirektivets artikel 25, stk. 2 jf. PSL § 27, stk. 2. Udfyldningen af tilstrækkelighedsnormen er i høj grad baseret på Artikel 29-gruppens udtalelser[66], og i gruppens mest centrale udtalelse vedrørende tilstrækkelighedsnormen[67] er der formuleret en række vejledende synspunkter, som kan bidrage til udfyldningen og fortolkningen af tilstrækkelighedsnormen.

Såfremt det vurderes, at der som grundlag for overførsler foreligger et tilstrækkeligt beskyttelsesniveau i et tredjeland, kan dette indebære, at det fastslås, at et bestemt tredjelands databeskyttelsesretlige regulering opfylder tilstrækkelighedsnormen, således at der frit kan overføres persondata til dette tredjeland. Databeskyttelsesdirektivets artikel 25, stk. 6 fastslår, at Kommissionen med bindende virkning for medlemslandene kan træffe beslutning om, at et bestemt tredjeland sikrer et tilstrækkeligt beskyttelsesniveau. I skrivende stund er de sikre tredjelande: Schweiz, Canada[68], Argentina, Guernsey, Jersey, Isle of Man og

[66] Jf. blandt andet Artikel 29-gruppens WP 3 af 25. juni 1997 og WP 4 af 26. juni 1997.
[67] Artikel 29-gruppens WP 12 af 24. juli 1998 sammenfattede det hidtidige arbejde til en samlet stillingtagen til alle de centrale spørgsmål i forbindelse med dataoverførsler til tredjelande.
[68] Begrænset anvendelsesområde. Yderligere oplysninger herom kan findes på Kommissionens hjemmeside vedrørende sikre tredjelande.

USA[69]. Til disse lande kan der frit ske persondataoverførsler uden, at der stilles yderligere krav end de almindelige krav, der fremgår af den nationale lovgivning i relation til behandling. Overførsler af persondata, som er omfattet af PSL § 7, stk. 1, de følsomme persondataoplysninger, kan dog heller ikke ske til sikre tredjelande, medmindre Datatilsynet forinden har afgivet en udtalelse herom.

4.2. Singulære undtagelser til tilstrækkelighedsnormen

Tilstrækkelighedsnormen repræsenterer det klare udgangspunkt ved persondataoverførsler til tredjelande, hvilket teoretisk set betyder, at det ikke burde være muligt at overføre persondata til lande, der ikke har et tilstrækkeligt beskyttelsesniveau. Det er dog databeskyttelsesretligt set blevet betragtet som for vidtgående at fastsætte et absolut forbud imod disse overførsler; dels på grund af, at udbygningen af den internationale samhandel og de reelle forhold inden for globale telekommunikationsnetværk i forskellige situationer kræver en vis fleksibilitet i de internationale dataoverførsler[70]; dels fordi der kan være tilfælde, hvor det er i de registreredes interesse, at der kan ske dataoverførsler. Dertil kommer, at det i praksis vil være umuligt at håndhæve et absolut forbud. Som følge heraf er der i Databeskyttelsesdirektivets artikel 26, stk. 1 jf. PSL § 27, stk. 3 fastsat en række undtagelser, hvor der vil kunne ske overførsel af persondata til et tredjeland, som ikke sikrer et tilstrækkeligt beskyttelsesniveau[71].

Undtagelserne har for en dels vedkommende væsentlig betydning for persondataoverførsler inden for den private sektor, men som det fremgår af Databeskyttelsesdirektivets artikel 26, stk. 1, er medlemslandene ikke forpligtede til at gennemføre alle de i direktivet nævnte undtagelser. Der kan således forekomme nationale afvigelser, og der kan foreligge forskelligartede betingelser for de virksomheder, som ønsker at foretage persondataoverførsler på baggrund af de nævnte undtagelsesbestemmelser. For en koncern med selskabsrepræsentation i flere medlemslande kan dette anspore til forumshopping mellem medlemslandene for at finde frem til den mest gunstige fortolkning af undtagelsesbestemmelserne[72]. Dette synspunkt er også antaget af Artikel 29-gruppen, der ligeledes har fastslået, at undtagelsesbestemmelserne skal fortolkes og anvendes restriktivt, så de registreredes grundlæggende

[69] Kun angående Safe Harbor-ordningen. Denne ordning har dog så specielle og særegne træk, at den bedst kategoriseres under særordninger, selvom der er tale om en særlig anvendelse af Databeskyttelsesdirektivets artikel 25, stk. 1. Se afsnit 4.3.2. om Safe Harbor-ordningen.
[70] Jf. Databeskyttelsesdirektivets præambel, betragtning 56 samt Beretning fra Kommissionen - Første beretning om gennemførelsen af databeskyttelsesdirektivet (95/46/EF), s. 19.
[71] Undtagelserne vil ikke blive gennemgået yderligere, idet der i stedet henvises til PSL § 27, stk. 3, nr. 1-8, der medtager alle de undtagelser, som er oplistet i Databeskyttelsesdirektivet.
[72] Jf. Beretning fra Kommissionen - Første beretning om gennemførelsen af databeskyttelsesdirektivet (95/46/EF), s. 19.

rettigheder og integritet ikke krænkes[73]. Artikel 29-gruppen er generelt set skeptisk i forhold til Databeskyttelsesdirektivets artikel 26, stk. 1 og påpeger som et af de væsentligste problemer, at dataeksportøren ved anvendelse af undtagelsesbestemmelserne ikke har nogen pligt til at sikre, at de overførte persondata beskyttes i importlandet. Der er således en risiko for integritetskrænkelse forbundet med anvendelse af undtagelsesbestemmelserne. Artikel 29-gruppen påpeger endvidere, at den bedste praksis for en dataansvarlig, der ønsker at foretage en international dataoverførsel, vil være først at undersøge, om det pågældende tredjeland yder en tilstrækkelig databeskyttelse og herefter selv sørge for, at overført persondata beskyttes i dette land. Hvis databeskyttelsesniveauet i tredjelandet på grundlag af samtlige de forhold, der har indflydelse på overførslen, ikke vurderes at være tilstrækkeligt, bør den dataansvarlige tage Databeskyttelsesdirektivets artikel 26, stk. 2 i betragtning for at opnå en tilstrækkelig beskyttelse ved eksempelvis at anvende Kommissionens standardkontraktbestemmelser eller vedtage en BCR[74].

Af de ovennævnte årsager kan undtagelsesbestemmelserne ikke undværes, men i videst muligt omfang bør de generelle ordninger – det vil sige de særlige reguleringsformer og særordninger – anvendes, idet disse ordninger forudsætter, at der er en databeskyttelsesretlig regulering i importlandet, og de giver mulighed for at stille krav til udformningen af importlandets ret.

4.3. De særlige reguleringsformer og særordninger

Som nævnt indledningsvis har EU i et vist omfang efterkommet det internationale erhvervsbetonede pres og medvirket til udviklingen af forskellige reguleringsformer og særordninger, der øger mulighederne for grænseoverskridende behandling af persondata, herunder overførsler til tredjelande. Hjemlen for disse generelle ordninger er fastsat i Databeskyttelsesdirektivets artikel 26, stk. 2, der giver et medlemsland tilladelse til overførsel af persondata til et tredjeland, der ikke sikrer et tilstrækkeligt beskyttelsesniveau, hvis den dataansvarlige yder tilstrækkelige garantier for beskyttelse af privatlivets fred, personers grundlæggende rettigheder og frihedsrettigheder samt for udøvelsen af de dertil knyttede rettigheder. Bestemmelsen fastsætter endvidere, at sådanne garantier især kan fremgå af passende kontraktbestemmelser. Artikel 26, stk. 3 fastslår en forpligtelse for de nationale datatilsynsmyndigheder til at underrette Kommissionen og de øvrige medlemslande om til-

[73] Jf. Artikel 29-gruppens WP 114 af 25. november 2005, s. 3 f. samt s. 10.
[74] Jf. i det hele diskussionen i WP 114 af 25. november 2005.

ladelser, som gives efter bestemmelsen. Derudover har Kommissionen beføjelse til i overensstemmelse med proceduren i direktivets artikel 31, stk. 2 at træffe afgørelse om, at visse standardkontraktbestemmelser frembyder tilstrækkelige garantier i henhold til artikel 26, stk. 2.

I dansk ret er det formelle udgangspunkt PSL § 27, stk. 4, der implementerer Databeskyttelsesdirektivets artikel 26, stk. 2 og 3. Ifølge bestemmelsen kan Datatilsynet give tilladelse til, at der overføres persondata til tredjelande, som ikke opfylder kravene i PSL § 27, stk. 1, såfremt den dataansvarlige yder tilstrækkelige garantier for beskyttelse af de registreredes rettigheder. PSL § 27, stk. 4 angiver ikke, hvilke ordninger, der kan danne grundlag for en tilladelse, hvilket betyder, at Datatilsynet udøver et frit skøn og kan fastsætte nærmere vilkår for overførslen. I almindelighed er det ikke overførslens retlige form, men dens grad af overensstemmelse i forhold til PSL og Databeskyttelsesdirektivet og dens pålidelighed angående efterlevelse og håndhævelse, der er afgørende for, om der gives tilladelse[75]. Endvidere kan det ud fra bestemmelsens ordlyd fastslås, at det er den dataansvarlige, der skal kunne dokumentere, at det set i forhold til de registreredes rettigheder og personlige integritet er betryggende, at der gives tilladelse til overførsel. Den dataansvarlige skal således kunne dokumentere, at der ved overførslen ikke er risiko for integritetskrænkelser. Denne dokumentationsbryde kan være tung og krævende for den dataansvarlige, og på baggrund heraf kan det derfor være meget hensigtsmæssigt at anvende en af de særlige reguleringsformer eller særordninger, som eksisterer, idet disse kan lette dokumentationsbyrden. Ud fra en objektiv betragtning af de eksisterende gennemførte generelle ordninger synes der at foreligge to typer:

Den første type er karakteriseret ved, at der for den enkelte specifikke persondataoverførsel etableres en særlig retlig ramme – en særlig reguleringsform – hvorved en tilpasset udgave af Databeskyttelsesdirektivet trænger ind i et tredjeland, som ikke har et tilstrækkeligt beskyttelsesniveau. Der etableres herved en databeskyttelsesretlig regulering hos den konkrete dataimportør, eksempelvis et datterselskab i en stor koncern, som skaber en retstilstand, der set ud fra et EU-retligt perspektiv er acceptabel[76]. Under denne første type af generelle ordninger henhører Kommissionens standardkontraktbestemmelser og BCR.

Den anden type af generelle ordninger, som på nuværende tidspunkt kun repræsenteres af Safe Harbor-ordningen, er karakteriseret ved, at der nærmere er tale om en modifikation af

[75] Jf. Blume, P. (2006): Retlig regulering af internationale persondataoverførsler, s. 118.
[76] Jf. Blume, P. (2006): Retlig regulering af internationale persondataoverførsler, s. 113.

Databeskyttelsesdirektivets tilstrækkelighedsnorm i artikel 25, stk. 1 end om en egentlig reguleringsform. En sådan reguleringsform er ikke direkte relateret til specifikke overførsler men angiver derimod, at virksomheder, der er omfattet af denne ordning, kan foretage persondataoverførsler på grundlag af særlige regler, som ikke fuldt ud modsvarer Databeskyttelsesdirektivets regler. Eftersom denne type af ordninger kan medføre en udvanding af direktivet, vil det næppe være sandsynligt, at der opstår andre ordninger end den ene, som er gennemført[77].

Kommissionens standardkontraktbestemmelser og Safe Harbor-ordningen vil kort blive omtalt i de to efterfølgende afsnit, men specialet tilsigter ikke en dybdegående behandling af disse to ordninger, idet de begge frembyder komplicerede databeskyttelsesretlige problemstillinger, som det ikke vil være muligt at behandle inden for rammerne af dette speciale.

4.3.1. Standardkontraktbestemmelser herunder de af Kommissionen vedtagne standardkontrakter

Kommissionen har i henhold til Databeskyttelsesdirektivets artikel 26, stk. 4 fastslået, at visse standardkontraktbestemmelser frembyder tilstrækkelige garantier for beskyttelse af privatlivets fred, grundlæggende rettigheder og frihedsrettigheder samt for udøvelsen af de dertil knyttede rettigheder. Anvendelsen af disse standardkontraktbestemmelser sker efter dansk ret i henhold til PSL § 27, stk. 4, der omfatter såvel anvendelse af Kommissionens standardkontraktbestemmelser som andre kontraktbestemmelser udarbejdet af den dataansvarlige, og der skal i begge tilfælde indhentes tilladelse fra Datatilsynet. Datatilsynets beføjelse i PSL § 27, stk. 4 danner således grundlag for, at det kan sikres, at kontrakten indholdsmæssigt er acceptabel. Dette betyder, at enhver kontrakt, der indholdsmæssigt kan sikre de føromtalte garantier, kan opnå godkendelse, og der er ikke fastsat yderligere begrænsninger i valg af kontraktstype. Virksomheder, der ønsker at benytte sig af standardkontrakter, kan derfor vælge at udforme en sådan kontrakt selv. Det er dog set ud fra en pragmatisk synsvinkel både en tids- og ressourcekrævende opgave at udforme sådanne kontrakter, idet de indholdsmæssigt ikke ligner de kontrakter, der normalt benyttes i virksomheder. Det vil derfor formodentlig alene være de helt store multinationale koncerner, som kan løfte den opgave, det er at udforme disse kontrakter med den konsekvens, at kontraktmodellen kun vil blive benyttet i begrænset omfang.

[77] Jf. Blume, P. (2006): Retlig regulering af internationale persondataoverførsler, s. 113 f.

For at fremme brugen af kontraktbestemmelser i små og mellemstore virksomheder, og fordi EU generelt set har en har en økonomisk interesse i, at der sker forsvarlige persondataoverførsler, har Kommissionen derfor vedtaget tre beslutninger om standardkontraktbestemmelser:

Den første standardkontrakt blev godkendt i 2001 af Kommissionen[78] og regulerer overførsler fra en dataansvarlig i et medlemsland til en dataansvarlig i et tredjeland, der ikke har et tilstrækkeligt beskyttelsesniveau jf. 2001-kontrakten, artikel 2. Det fremgår endvidere af 2001-kontraktens præambel, betragtning 1, at det er en forudsætning, at den nationale databeskyttelsesregulering i eksportlandet er overholdt. Denne undtagelsesfrie forudsætning er også fastholdt i forhold til de andre standardkontrakter.

Den anden standardkontrakt, som regulerer overførsler fra en dataansvarlig i et medlemsland til en dataansvarlig i et tredjeland, der ikke har et tilstrækkeligt beskyttelsesniveau, blev godkendt af Kommissionen i 2004 med ikrafttræden i 2005[79]. Denne standardkontrakt minder i stort omfang om 2001-kontrakten, idet 2004-kontrakten dog er mere virksomhedsorienteret som følge af den kritik, erhvervskredse, herunder ICC, rettede mod 2001-kontrakten[80]. Der er således gennemført en række mindre ændringer og tilpasninger, der passer bedre til det traditionelle erhvervslivs dataoverførselsbehov. 2001- og 2004-standardkontrakterne kan ikke kombineres jf. 2004-kontraktens præambel, betragtning 3 jf. artikel 1, stk. 1, men eftersom de to nævnte standardkontrakter ikke udtømmende angiver de kontrakter, som de nationale datatilsynsmyndigheder kan godkende, må formuleringen i 2004-kontrakten forstås således, at en kombination af de to standardkontrakter ikke skaber en kontrakt, som de nationale datatilsynsmyndigheder er forpligtede til at godkende, men som de kan godkende. Udgangspunktet er jo ellers i henhold til såvel Databeskyttelsesdirektivets artikel 26, stk. 4 som betænkningsudvalgets bemærkninger til PSL § 27, stk. 4[81], at en anvendelse af Kommissionens standardkontraktbestemmelser altid vil opfylde kravet om de fornødne garantier og vil forpligte de nationale datatilsynsmyndigheder til at godkende kontrakten.

Den tredje standardkontrakt blev godkendt af Kommissionen i 2001[82] og regulerer modsat de to tidligere nævnte standardkontrakter overførsler fra dataansvarlige til databehandlere i

[78] Jf. Kommissionens beslutning af 15. juni 2001. Herefter benævnt 2001-kontrakten.
[79] Jf. Kommissionens beslutning af 27. december 2004. Herefter benævnt 2004-kontrakten.
[80] Jf. Kommissionens beslutning af 27. december 2004, præamblen, betragtning 2. Se også ICC - Kommentarer og FAQs (Frequently Asked Questions) til Kommissionens beslutning.
[81] Jf. Betænkning om behandling af personoplysninger nr. 1345/1997, s. 289 f.
[82] Jf. Kommissionens beslutning af 27. december 2001.

tredjelande. Den dataansvarlige har i praksis ikke kun behov for at overføre persondata til andre dataansvarlige men også til databehandlere. Overladelse af persondata til en databehandler i et tredjeland er i henhold til tidligere afsnit også at betragte som en overførsel, og det kan i en sådan situation være hensigtsmæssigt at anvende standardkontrakter, idet databehandleren dermed kan behandle alle de overførte persondata på grundlag af de samme regler.

Alle de ovenfornævnte standardkontrakter er konstrueret som en form for tredjemandsløfte til de registrerede. De registrerede er ikke egentlige parter i relation til kontrakten men får tildelt status som begunstigede tredjemænd. Der fastsættes et fælles ansvar for dataeksportøren og dataimportøren, og der er mulighed for håndhævelsessanktioner i tilfælde af misligholdelse. Ligeledes kan de registrerede vælge, om krænkelser skal bedømmes af domstolene eller ved mægling. Derudover garanterer de kontraherende parter, at persondataoplysningerne vil blive behandlet i overensstemmelse med de databeskyttelsesretlige regler, der fremgår af den pågældende standardkontrakt.

Standardkontrakterne medfører på baggrund af det ovenfor nævnte fordele, fordi de giver mulighed for en afgrænset og kontrolleret regulering af den grænseoverskridende databehandling, som den dataansvarlige påtager sig forpligtelser i forhold til. Selvom der ikke er fuld aftalefrihed, så tilbyder standardkontrakter den dataansvarlige en vis indflydelse på udformningen af det grundlag, der sker dataoverførsler på baggrund af. Standardkontrakter er dog ikke umiddelbart den bedste overførselsløsning for multinationale koncerner eller egentlige enhedsselskaber[83]. Dette kan blandt andet begrundes i kontrakters retlige natur. Har et internationalt enhedsselskab behov for at overføre persondata inden for selskabets rammer, kan det som enhedsselskab ikke kontrahere med sig selv, og en standardkontrakt vil i dette tilfælde ikke være løsningen. For store multinationale koncerner med mange selskaber i koncernkonstellationen og mange forskellige persondataoverførsler er standardkontrakter ofte heller ikke løsningen, da det kan forekomme uoverskueligt og være økonomisk og juridisk meget byrdefuldt at benytte standardkontrakter i denne sammenhæng, idet der til hver enkelt overførsel eller gruppe af overførsler skal udarbejdes en standardkontrakt.

[83] Herved forstås et selskab, som er enkeltstående og én samlet selvstændig juridisk enhed. Forskellen i relation til koncerner ligger i, at et enhedsselskab ikke indgår i en selskabskonstruktion med datterselskaber, men et enhedsselskab kan godt have filialer, da disse ikke er selvstændige juridiske personer. Enhedsselskaber kan opnå betydelig størrelse og være internationalt repræsenteret som eksempelvis Visa.

4.3.2. Safe Harbor-ordningen

Safe Harbor-ordningen er som nævnt baseret på Databeskyttelsesdirektivets artikel 25, stk. 1 og ikke artikel 26, stk. 2, men den fungerer egentlig som en selvstændig særordning og kan dermed i realiteten ikke sammenlignes med den situation, hvor et tredjeland godkendes med et tilstrækkeligt beskyttelsesniveau efter tilstrækkelighedsnormen.

Safe Harbor-ordningen er udviklet af U.S. Department of Commerce i samarbejde med Kommissionen og omfatter alene virksomheder i den private sektor under amerikansk jurisdiktion og under myndighedskompetence af enten Federal Trade Commission eller U.S. Department of Transportation. Dette betyder også, at det langt fra er alle amerikanske virksomheder, der kan tilslutte sig Safe Harbor-ordningen. Tilslutning er eksempelvis ikke mulig for finansielle virksomheder eller telekommunikationsvirksomheder[84].

Ordningen indebærer en form for styret selvregulering, idet en amerikansk virksomhed frivilligt kan vælge at tilslutte sig ved at tegne sig på en liste, som siden 1. november 2000 har været ført af U.S. Department of Commerce. Ved at tilslutte sig denne liste tilkendegiver den pågældende virksomhed, at den accepterer en række fastsatte principper om persondatabeskyttelse[85]. Herefter kan virksomheden registrere sig som en Safe Harbor, hvilket betyder, at der frit kan overføres persondata fra en virksomhed beliggende i EU til den pågældende amerikanske virksomhed, idet den amerikanske virksomhed i kraft af prædikatet Safe Harbor og dens tilkendegivelse om at leve op til ordningens principper antages at have et tilstrækkeligt beskyttelsesniveau[86].

Safe Harbor vedrører alene dataimportører i den private sektor og adskiller sig herved fra Kommissionens standardkontraktbestemmelser og BCR, idet disse reguleringsformer tilliger inddrager dataeksportøren. Det betyder, at såfremt eksempelvis en dansk virksomhed kan konstatere, at en amerikansk virksomhed er omfattet af Safe Harbor-ordningen, kan der ske en persondataoverførsel, idet den amerikanske virksomhed opfylder tilstrækkelighedsnormen i kraft af Safe Harbor og således er omfattet af PSL § 27, stk. 1. Selvom der

[84] Jf. Kuner, C. (2007): European Data Protection Law, s. 181.
[85] Disse principper er: Notice, choice, onward transfer, security, data integrity, access, enforcement. Desuden suppleres principperne af 15 FAQs, hvori principperne uddybes og forklares. Disse FAQs er en integreret del af Safe Harbor-ordningen. Mere information omkring principperne med videre kan hentes på U.S. Department of Commerce – Safe Harbor.
[86] Kommissionen fastslog i sin beslutning af 26. juli 2000, at Safe Harbor-ordningen sikrer et tilstrækkeligt beskyttelsesniveau for persondata, der overføres fra EU til virksomheder etableret i USA.

sker overførsel af persondata til en amerikansk virksomhed under Safe Harbor-ordningen, skal der dog alligevel foreligge en tilladelse fra Datatilsynet efter PSL § 50, stk. 2, da ordningen som nævnt er omfattet af PSL § 27, stk. 1.

Safe Harbor-ordningen er på grund af sit begrænsede anvendelsesområde ikke den mest optimale løsning for multinationale koncerner eller enhedsselskaber, der ønsker at foretage internationale persondataoverførsler. Der er fortsat mange amerikanske virksomheder, som ikke har tilsluttet sig Safe Harbor-ordningen, og som følge af den særlige konstruktion af ordningen har mange amerikanske virksomheder svært ved at anvende og gennemskue Safe Harbor-reglerne.

4.3.3. Sammenfatning

Sammenfattende kan det fastslås, at standardkontrakter herunder Kommissionens standardkontraktbestemmelser og i mindre omfang Safe Harbor-ordningen kan være gode, brugbare reguleringsformer og særordninger i forhold til grænseoverskridende behandling af persondata. I relation til internationale enhedsselskaber og multinationale koncerner er disse ordninger umiddelbart vurderet ikke de mest egnede eller hensigtsmæssige løsninger, og der kan opstå forskellige anvendelsesproblemer med disse ordninger i praksis. For enhedsselskabers vedkommende kan det ikke lade sig gøre at anvende standardkontrakter, idet et selskab ikke kan kontrahere med sig selv, og for multinationale koncerner kan det være en uoverskuelig opgave at udfærdige et utal af standardkontrakter i forbindelse med mange forskellige overførsler af persondata. Safe Harbor-ordningens anvendelsesområde er snævert, så hverken i forhold til enhedsselskaber eller multinationale koncerner er denne særordning anvendelig, hvis der skal foretages overførsel til andre end amerikanske virksomheder.

4.4. En kort juridisk analyse af udvalgte retlige spørgsmål vedrørende reguleringsformen BCR

Begrænsningen i de juridiske reguleringsformer, der hidtil har været nævnt i forbindelse med gennemgangen af dataoverførsler til tredjelande er, at der er tale om ad hoc løsninger, hvor anvendeligheden og hensigtsmæssigheden skal vurderes i forhold til hver enkel persondataoverførsel eller en afgrænset gruppe af overførsler. I praksis har store multinationale koncerner behov for en reguleringsform, der kan benyttes som et alternativ til standardkontrakter, således at koncernen ikke er tvunget til at holde styr på adskillige kontrakter

mellem de enkelte koncernselskaber. Set i forhold til enhedsselskaber er behovet for en alternativ reguleringsform formodentlig også størst og mest aktuelt for koncerner. Dette skyldes, at såfremt der etableres et enhedsselskab frem for en koncernkonstellation, så er den dataansvarlige antageligvis bedre stillet i relation til behandling af persondata, idet der sker en intern anvendelse, og idet der ikke er tale om en egentlig spredning af persondata. Intern anvendelse er som tidligere nævnt en persondatabehandling, eftersom overførselsbegrebet ikke forudsætter, at der er sket overdragelse til en anden dataansvarlig, men intern anvendelse vil formodentlig af de nationale datatilsynsmyndigheder blive betragtet mere lempeligt end videregivelse, idet der er mindre risiko for integritetskrænkelse, fordi oplysningerne forbliver inden for den samme juridiske enhed og ikke flyttes rundt mellem forskellige selvstændige selskaber. Analysen i afsnit 4.4. vil derfor på baggrund heraf udelukkende koncentrere sig om multinationale koncerners anvendelse af BCR.

På baggrund af multinationale koncerners behov for en alternativ reguleringsform til standardkontrakter udsendte Artikel 29-gruppen i 2003 WP 74, hvori gruppen foreslog, at der kunne vedtages et sæt bindende koncernregler. Gruppen fastslog endvidere, at den anså disse regler for hensigtsmæssige, anvendelige og sikrende et tilstrækkeligt beskyttelsesniveau i henhold til Databeskyttelsesdirektivets artikel 26, stk. 2[87]. Reguleringsformen BCR var dermed en realitet, om end selve konceptet ikke var nyt, idet mange koncerner allerede anvendte forskellige codes of conduct[88] eller rettede sig efter andre særlige adfærdskodekser som eksempelvis dem, der kan udarbejdes i medfør af Databeskyttelsesdirektivets artikel 27 jf. PSL § 74. Til forskel fra disse adfærdskodekser, der er rettet mod en hel branche eller mod brancherepræsentationsorganer, dækker BCR kun den bestemte koncern, som den er skabt til[89]. I relation til databeskyttelsesretten må BCR dermed anses for en ny, innovativ reguleringsform.

En definition af BCR er nævnt indledningsvist men for at opridse essensen heraf, så dækker betegnelsen BCR over et sæt regler, der vedtages for en koncern med selskaber i flere lande. For at en BCR kan udgøre fornøden hjemmel til overførsel af persondata i henhold

[87] Jf. Artikel 29-gruppens WP 74 af 3. juni 2003, s. 5 f.
[88] Codes of conduct er typisk dokumenter, hvor virksomheden har nedskrevet sine etiske retningslinjer, og hvor virksomheden over for omverden erklærer, hvordan den vil handle og forholde sig i forskellige situationer. Der kan være tale om generelt formulerede forretningsprincipper eller detaljerede retningslinjer. Artikel 29-gruppen fastslår i WP 74 af 3. juni 2003, s. 5, note 4 at brug af codes of conduct er meget udbredt i koncernforhold og nævner i den forbindelse forskellige eksempler.
[89] Jf. Büllesbach, A., Poullet, Y. & Prins C. [Eds.] (2006): Concise European IT Law, s. 116 samt Artikel 29-gruppens WP 74 af 3. juni 2003, s. 8 og s. 14.

til databeskyttelseslovgivningen, skal den være bindende og forpligtende for samtlige enheder og selskaber i koncernen og kan således ikke anvendes som hjemmel til overførsel af persondata til selskaber, der ikke er en del af koncernen[90]. Når reglerne er godkendt af datatilsynsmyndighederne i de EU-medlemslande, hvorfra koncernen ønsker at overføre persondata – for dansk rets vedkommende vil en BCR skulle godkendes af Datatilsynet efter bestemmelsen i PSL § 27, stk. 4 – kan der i princippet frit overføres persondata mellem koncernens selskaber, såfremt disse selskaber lever op til kravene i den pågældende BCR samt reglerne i databeskyttelseslovgivningen i øvrigt. Det skal dog påpeges, at selvom en BCR skaber hjemmel til at overføre persondata, skal der stadig være særskilt national hjemmel til at behandle de pågældende persondata jf. Databeskyttelsesdirektivets artikel 25, stk. 1 jf. PSL § 27, stk. 5[91].

Der er således tale om en reguleringsform, som er skræddersyet til den pågældende koncern med de individuelle, særegne behov og den erhvervsprofil, som koncernen måtte have. Koncernen skal dermed blot efterleve den pågældende BCR, og såfremt koncernen gør dette, vil alle selskaber i koncernen blive betragtet som en sikker havn – en safe haven – inden for hvilken persondata frit kan flyttes fra et koncernselskab til et andet og stadig opretholde det samme beskyttelsesniveau, uanset hvor de pågældende persondata måtte befinde sig.

4.4.1. Artikel 29-gruppens WP vedrørende BCR

Artikel 29-gruppen har vedtaget flere WP, som i høj grad danner grundlag for de krav, der stilles til udformning og indhold af en BCR. Rent retskildemæssigt betragtet foreligger der ikke meget andet relevant og brugbart materiale, som kan benyttes i forbindelse med en analyse af BCR, end det Artikel 29-gruppen har udarbejdet[92]. Analysen vil derfor i vidt omfang være baseret på gruppens overvejelser. Den retskildemæssige værdi af Artikel 29-gruppens WP er behandlet i afsnit 2.2.2., og på den baggrund lægges Artikel 29-gruppens WP i denne analyse til grund som juridisk fortolkningsgrundlag.

Kravene til udformning og indhold af en BCR findes i Artikel 29-gruppens nøgledokument WP 74, der i praksis er styrende for de nationale datatilsynsmyndigheders vurdering af en

[90] Jf. Artikel 29-gruppens WP 74 af 3. juni 2003, s. 9.
[91] Jf. også Artikel 29-gruppens WP 74 af 3. juni 2003, s. 7 f.
[92] ICC dog har i 2004 udarbejdet en rapport vedrørende BCR, som i det omfang, det anses for nødvendigt, vil blive inddraget.

BCR[93], samt WP 107 og WP 108. Gruppen har tillige udformet en skabelon, der kan anvendes, når en koncern anmoder om tilladelse til overførsel af persondata til tredjelande på baggrund af en BCR og en skabelon, der kan bruges i forbindelse med strukturering af en BCR. Disse skabeloner findes i udtalelserne WP 133 og WP 154. Endvidere har Artikel 29-gruppen i WP 153 udarbejdet en tjekliste over, hvilke elementer og principper en BCR skal indeholde samt en FAQ vedrørende BCR i WP 155, som jævnligt vil blive opdateret i takt med, at reguleringsformen udvikler sig. De fire sidstnævnte WP vil ikke blive gennemgået yderligere i dette speciale, idet de alle er en opsamling og en konkretisering af de betragtninger, som Artikel 29-gruppen har fremsat i WP 74, WP 107 og WP 108, og således giver bedst mening som støttedokumenter eller modelforslag i forbindelse med den praktiske udformning af en BCR, men ikke har megen relevans i forbindelse med en juridisk analyse.

Sammenfattende kan det dermed konstateres, at Artikel 29-gruppen har udstedt i alt 7 WP, der relaterer sig til BCR. De for dette speciale relevante betragtninger, hvilket hovedsagelig vil være betragtningerne i WP 74, vil blive behandlet i de efterfølgende afsnit.

4.4.2. BCRs anvendelsesområde og egnethed

Et af de væsentligste spørgsmål i relation til BCR har været spørgsmålet om, for hvilke typer af koncernkonstellationer reguleringsformen vil være egnet. Der er ingen tvivl om, at anvendelsesområdet for en BCR er multinationale koncerner, hvilket tydeligt fremgår af Artikel 29-gruppens indledningsvise bemærkninger i WP 74[94]. En selskabsretlig præcisering vil i denne sammenhæng være relevant, idet koncernbegrebet anvendes på forskellig måde i de enkelte EU-medlemslande[95].

Som tidligere nævnt er begrebet koncern en betegnelse for en gruppe af formelt set selvstændige selskaber, der har fælles ejerinteresser. I virksomhedsøkonomisk henseende arbejder koncerner ofte som en økonomisk enhed, mens de enkelte koncernselskaber i juridisk henseende udgør selvstændige retssubjekter med hver deres selskabsretlige organisation. Medarbejderne er ansat i ét bestemt koncernselskab og ikke i koncernen som sådan, og kontrakter indgås af og med det enkelte koncernselskab og ikke af og med koncernen som sådan. Konglomerater er en betegnelse, der anvendes om en koncern, når dattervselskaberne drives uafhængigt af hinanden og ikke eller kun i meget begrænset omfang har

[93] Jf. Blume, P. (2006): Retlig regulering af internationale persondataoverførsler, s. 137, note 27.
[94] Jf. Artikel 29-gruppens WP 74 af 3. juni 2003, s. 5 f.
[95] Jf. Krüger Andersen, P. (2008): Aktie- og anpartsselskabsret, s. 485 f.

fælles forretningsmæssige aktiviteter. I konglomeratet skaber hvert selskab egne resultater og egen strategisk position, og datterselskabernes bidrag til koncernen vil ofte primært være af finansiel karakter[96].

Hvis den selskabsretlige koncerndefinition skal overføres til en databeskyttelsesretlig kontekst, betyder det – også henset til Artikel 29-gruppens udtalelser i WP 74 – at BCR er en velegnet reguleringsform for tætte koncernkonstellationer, mens en BCR ved konglomerater eller løse samarbejdsrelationer vil være mindre eller slet ikke egnet. Dette skyldes, at den diversitet, der foreligger mellem selskaber i et konglomerat, og rækkevidden af overførselsaktiviteterne, vil gøre det meget svært – hvis ikke umuligt – at opfylde de krav, der opstilles i WP 74, og det er nødvendigt, at der foreligger en vis grad af sikkerhed for, at den vedtagne BCR vil kunne fungere inden for koncernen, for at reguleringsformen kan anvendes[97]. I sidste ende vil det dog bero på en vurdering fra de nationale datatilsynsmyndigheder, hvorvidt der foreligger en tilstrækkelig tæt koncern eller ej. Set ud fra et retligt synspunkt vil det næppe give problemer for Datatilsynet at vurdere, hvorvidt en koncern opfylder ovennævnte krav om en tæt koncernkonstellation, idet den danske selskabslovgivning og det danske koncernbegreb er ret klart formuleret på dette område[98]. Det skal i den forbindelse også bemærkes, at en koncern ikke er en fastforankret, uforanderlig enhed, og der kan således tilføjes nye selskaber til konstellationen. Artikel 29-gruppens opfattelse er her, at såfremt der foreligger en allerede godkendt BCR, kan et nyt selskab i koncernen uden videre deltage, hvis det er forpligtet og bundet af de fastsatte regler, og ansøgningsproceduren skal ikke gentages på ny ved de implicerede nationale datatilsynsmyndigheder. Der stilles dog krav om, at der føres en opdateret liste over koncernens selskaber og enheder, og at der årligt sker en rapportering til datatilsynsmyndighederne, således at disse kan få klarhed over koncernens præcise sammensætning[99].

Det kan således på baggrund af ovenstående fastslås, at en BCR er egnet som reguleringsform i forbindelse med grænseoverskridende behandling af persondata for selskaber, der indgår i en tæt koncernstruktur. Heri ligger dog også den begrænsning, at selvom en BCR skaber en safe haven for overførsler inden for koncernen, så er der ikke umiddelbart skabt en safe haven i relation til overførsler, der foretages til selskaber uden for koncernstrukturen.

[96] Jf. Krüger Andersen, P. (2008): Aktie- og anpartsselskabsret, s. 487.
[97] Jf. Artikel 29-gruppens WP 74 af 3. juni 2003, s. 9.
[98] Jf. Krüger Andersen, P. (2008): Aktie- og anpartsselskabsret, s. 488 f.
[99] Jf. Artikel 29-gruppens WP 74 af 3. juni 2003, s. 15.

Dette bringer mig videre til et andet væsentligt spørgsmål i forbindelse med BCRs anvendelsesområde og egnethed nemlig; hvorvidt en BCR skal gælde for hele koncernen eller kun dele heraf? Dette spørgsmål udspringer af den forskel, der er på koncernselskaber, som er beliggende inden for EU, og dermed er under Databeskyttelsesdirektivets jurisdiktionsområde og på koncernselskaber, som er beliggende uden for EU i tredjelande, hvis databeskyttelsesniveau kan være henholdsvis tilstrækkeligt eller utilstrækkeligt.

Det er opfattelsen, at en BCR skal gælde for hele koncernen uanset etableringssted og beliggenhed, hvilket begrundes i, at reguleringsformen på den måde virker mest effektivt og giver den største sikkerhed og overskuelighed i forhold til de registrerede[100]. En BCR er således både en minimumsstandard og en komplementær standard forstået på den måde, at såfremt den nationale databeskyttelsesregulering stiller strengere krav end den pågældende BCR, kan de registreredes krav baseres på den nationale regulering, idet en BCR kun er en minimumsstandard. Såfremt den pågældende BCR derimod yder en bedre databeskyttelse end den nationale databeskyttelsesregulering, kan de registrerede i stedet støtte ret på den pågældende BCR, da denne i dette tilfælde vil fungere som udfyldende regulering. I forhold til de dele af koncernen, der er beliggende inden for EU, vil den pågældende BCR således blive en præcisering af de regler, der fremgår af Databeskyttelsesdirektivet, mens en BCR for de dele af koncernen, der er beliggende i tredjelande, kan yde en effektiv persondatabeskyttelse for de registrerede.

En BCR kan aldrig blive en fuldstændig erstatning for efterlevelse af den nationale databeskyttelsesregulering, idet databeskyttelsesretten er så kompliceret og omskiftelig, at en BCR, der forsøger at eftergøre den nationale databeskyttelsesregulering, vil blive så kompleks, at det ikke vil være muligt at benytte reglerne i praksis. En BCR vil dog i vidt omfang kunne reducere store multinationale koncerners byrde i relation til overholdelse af national databeskyttelsesregulering, eftersom den nationale regulering i vidt omfang vil afspejles i den pågældende BCR.

4.4.3. BCRs retlige status

Spørgsmålet om BCRs retlige status har siden Artikel 29-gruppens udstedelse af WP 74 været et yderst vigtigt anliggende, idet gruppen allerede her betonede vigtigheden af, at en

[100] Jf. Artikel 29-gruppens WP 74 af 3. juni 2003, s. 8.

BCR skal være bindende både eksternt (binding in law) og internt i koncernen (binding in pratice)[101].

For at en BCR kan accepteres, må det dermed være sikkert, at den eksternt har retlig bindende virkning. Der er næppe tvivl om, at dette i sig selv kan være en meget svær opgave, idet en BCR set ud fra et juridisk synspunkt er en langt mere kompleks reguleringsform end en almindelig kontrakt. En BCR skaber efter sin natur ikke som ved almindelige kontrakter en gensidig forpligtelse. Den koncern, der vælger at udstede en BCR, påtager sig i kraft af dette valg en ensidig forpligtelse, og dette gælder uanset, at det er nødvendigt med en tilladelse fra de nationale datatilsynsmyndigheder for, at reguleringsformen kan anvendes.

Principielt set kan en BCR gøres retligt bindende på to måder: Enten i form af en ensidig påtaget forpligtelse fra det styrende moderselskab i koncernen, eller i kraft af en særlig kontrakt mellem de enkelte koncernselskaber eller mellem det styrende moderselskab og de nationale datatilsynsmyndigheder. Uanset hvilken type retsmiddel, der anvendes, er det forudsat af Artikel 29-gruppen, at en BCR ligesom Kommissionens standardkontrakter skal skabe et tredjemandsløfte i relation til de registrerede, således at de registrerede bliver begunstigede tredjemænd, hvor det i henhold til national ret er mulig[102].

I relation til ovennævnte bliver første spørgsmål, om en ensidig påtaget forpligtelse har retlig bindende virkning, og om koncernen kan fastholdes på denne i forbindelse med bedømmelsen af en efterfølgende databeskyttelseskonflikt? Dette spørgsmål er af afgørende betydning i forhold til de registrerede, men det har også betydning i relation til domstolene og de nationale datatilsynsmyndigheder, der skal have en reel mulighed for at behandle klager fra de registrerede. For at spørgsmålet kan besvares, er det nødvendigt at se på, hvordan den nationale ret stiller sig i forhold til ensidigt påtagne forpligtelser. I dansk ret kan en ensidig påtaget forpligtelse være udtryk for en viljeserklæring, der pålægger sin afgiver en forpligtelse, og derfor skaber et retsgrundlag i overensstemmelse med sit indhold. Det kan dermed antages, at dansk ret giver mulighed for, at ensidigt påtagne forpligtelser kan være retligt bindende. Dette er dog ikke tilfældet i alle EU-medlemslande og tredjelande[103], og der kan derfor opstå den situation, at en BCR, der skal omfatte selskaber i mange EU-medlemslande og tredjelande, ikke uden videre er retlig bindende i alle disse lande.

[101] Jf. Artikel 29-gruppens WP 74 af 3. juni 2003, s. 10 f.

[102] Jf. Artikel 29-gruppens WP 74 af 3. juni 2003, punkt 3.3.2., 5.5.1. og punkt 5.6 samt Artikel 29-gruppens WP 108 af 14. april 2005, punkt 5.12-5.14, 5.16 og punkt 5.20.

[103] Se ICC – Rapport vedrørende BCR, s. 19 f., hvori EU-medlemslandenes og forskellige andre landes anerkendelse af ensidigt påtagne forpligtelser er behandlet. Østrigsk privatret anerkender ensidigt påtagne forpligtelsers eksigibilitet, mens dette ikke er tilfældet i eksempelvis Frankrig og Italien.

Dette problem er dog muligt at løse ved at supplere den pågældende BCR med almindelige kontrakter i forhold til selskaber beliggende i sådanne lande, og selskaberne kan på denne måde forpligtes. Muligheden for at anvende supplerende kontrakter vil i øvrigt ligeledes kunne benyttes i forhold til udenforstående underleverandører, som ønskes inddraget under koncernens BCR.

Et andet spørgsmål i relation til ovennævnte er spørgsmålet om tredjemandsløftet i forhold til de registrerede. I dansk ret er udgangspunktet, at en aftale kun har retsvirkninger for dens parter, og for at aftaleforholdet kan medføre forpligtelser for tredjemand, kræves der særlig hjemmel. Der gælder dermed en grundsætning om aftalers relativitet, som indebærer, at C ikke uden videre kan rejse et krav på grundlag af en aftale mellem A og B, selvom denne aftale er misligholdt. Dette udgangspunkt er dog ikke helt så rigoristisk, når det gælder aftalens mulighed for at skabe og tildele rettigheder for tredjemand, idet A kan skabe en ret for C ved at afgive et tredjemandsløfte, der kan gøres gældende direkte mod A, og fordi der er tale om en begunstigelse af en tredjemand, spiller de begrænsninger, der ligger i princippet om aftalers relativitet, ingen rolle. Det er da også forudsat af Artikel 29-gruppen, at alle EU-medlemslande har juridiske redskaber, der minder om eller svarer til tredjemandsløftet[104].

De her drøftede spørgsmål kan således i sidste ende sammenfattes til, at en BCR ikke altid vil kunne stå alene, og det kan i nogle tilfælde være nødvendigt at supplere reguleringsformen med kontrakter.

Ud over, at en BCR skal være retligt bindende i ekstern forstand, må det herudover forudsættes og garanteres, at en BCR er bindende internt i koncernen. En BCR må derfor styres i forhold til den hierarkiske struktur i koncernen, og der skal være sikkerhed for, at samtlige koncernselskaber, ansatte og underleverandører[105] føler sig tvunget til at efterleve og overholde koncernens BCR[106]. Opnåelse af en sådan sikkerhed kan eksempelvis ske via interne foranstaltninger og instrukser fra ledelsen, uddannelse af de ansatte og ved gennemførelse af disciplinære sanktioner over for personer, der bryder koncernens BCR. Det er ledelsens opgave at sørge for, at de fornødne foranstaltninger er på plads, og ideelt set ville det mest hensigtsmæssige være, at bestyrelsen i det styrende moderselskab enstemmigt vedtog kon-

[104] Jf. Artikel 29-gruppens WP 74 af 3. juni 2003, s. 12 samt fodnote 11 samme side.

[105] I relation til underleverandører opstår problemet reelt set ikke, idet en underleverandør oftest vil være databehandler og dermed ikke er ansvarlig over for de registrerede. Databehandlere skal kun opfylde krav om fornødne sikkerhedsforanstaltninger jf. Databeskyttelsesdirektivets artikel 17 jf. PSL § 41, og normalt vil et selskab sikre sig opfyldelse af disse krav gennem standardkontrakter i stedet for gennem koncernens BCR.

[106] Jf. Artikel 29-gruppens WP 74 af 3. juni 2003, punkt 3.3.1. samt Artikel 29-gruppens WP 108 af 14. april 2005, punkt 5.3-5.9. Se også ICC - Rapport vedrørende BCR, s. 18-23, der gennemgår forskellige landes syn på, hvorledes en BCR kan gøres bindende internt i koncernen.

cernens BCR for at sikre overholdelse i samtlige selskaber inden for koncernstrukturen, og at bestemte personer i koncernen blev gjort ansvarlige for koncernens databeskyttelsespraksis. Artikel 29-gruppen har i WP 74 forudsat, at der er sandsynlighed for, at en BCR i kraft af de forskellige foranstaltninger vil være bindende internt i koncernen.

Et andet interessant spørgsmål i forbindelse med drøftelsen af BCRs retlige status er spørgsmålet om, hvor de registrerede kan gøre deres krav gældende, hvis der er tale om en multinational koncern, som har selskaber spredt ud over et stort antal lande? Ud fra Artikel 29-gruppens betragtninger må de registrerede enten gøre deres krav gældende i eksportlandet, hvis det er beliggende inden for EU; i det EU-medlemsland, hvor koncernens europæiske hovedkvarter er beliggende, eller hvis et sådan ikke findes; i det EU-medlemsland, der er angivet i den pågældende BCR. Det er dermed uacceptabelt, hvis de registrerede er henvist til at gøre deres krav gældende i et tredjeland. På denne måde øges tilliden til reguleringsformen BCR, idet retsusikkerheden omkring, hvor de registrerede skal anlægge deres krav og under hvilken jurisdiktion, elimineres.

4.4.4. BCR i praksis

En BCR vedrører efter sin natur overførsel af persondata mellem flere forskellige selskaber og lande, og derfor skal en BCR typisk godkendes af flere EU-medlemslande, før en overførsel kan finde sted. Artikel 29-gruppen har i den forbindelse vedtaget en procedure, der skal sikre, at en BCR kan godkendes af datatilsynsmyndighederne i samtlige EU-medlemslande, hvorfra koncernen ønsker at overføre persondata. Procedure findes i WP 108, og den fastslår, at den pågældende BCR i første omgang udelukkende skal fremsendes til datatilsynsmyndighederne i det EU-medlemsland, hvor koncernens europæiske hovedkvarter er beliggende. Herefter er det op til den pågældende datatilsynsmyndighed at koordinere og indhente godkendelse fra de øvrige implicerede EU-medlemslandes datatilsynsmyndigheder. Når dette er sket, kan der gives tilladelse til overførslerne. Er der tale om et dansk selskab i en koncernkonstellation, der ønsker at benytte sig af BCR, skal dette selskab kun fremsende den pågældende BCR til Datatilsynet, hvis koncernens europæiske hovedkvarter er beliggende i Danmark. Et selskab, der er en del af en koncern, hvis hovedkvarter er beliggende i et andet EU-medlemsland, vil udelukkende skulle fremsende en anmodning om tilladelse i henhold til PSL § 27, stk. 4, idet Datatilsynet automatisk vil modtage den pågældende BCR fra datatilsynsmyndighederne i det land, hvor koncernens hovedkvarter ligger. Når der er opnået godkendelse, skal den pågældende BCR foreligge

på alle de implicerede landes sprog, men koncernen kan under processen nøjes med at fremsende den pågældende BCR på engelsk og på det sprog, der anvendes i det land, hvor den første datatilsynsmyndighed er beliggende[107].

4.4.5. Sammenfatning

Sammenfattende kan en BCR være en brugbar og hensigtsmæssig men også en krævende og kompleks reguleringsform, der kan danne basis for grænseoverskridende behandling af persondata. Reguleringsformen kan reducere brugen af standardkontrakter, og en BCR har den fordel, at den dækker hele koncernen og nye selskaber, der måtte blive tilføjet i koncernkonstellationen, samt at den kan tilpasses den enkelte koncerns individuelle erhvervsmæssige behov. En BCR minder også til en vis grad om den interne regulering og styring, der i forvejen forekommer i koncerner i form af eksempelvis adfærdskodekser. Med de sidst vedtagne WP fra Artikel 29-gruppen bliver det formodentlig også nemmere for multinationale koncerner at skabe en BCR.

5. Konklusion

Meningen med dette speciale har været at bibringe læseren en viden om og indsigt i den grænseoverskridende behandling af persondata, herunder overførsel af persondata til tredjelande, samt at belyse de databeskyttelsesretlige problemer, der er forbundet med disse behandlinger og overførsler, heriblandt de problemer, som multinationale koncerner og store enhedsselskaber, der har aktiviteter i mange lande, kan støde på i forbindelse med overførsler af persondata. Derudover har det været specialets mål at rette fokus mod de særlige reguleringsformer, herunder især reguleringsformen BCR, og analysere reguleringsformens egnethed, retlige status og praktiske anvendelighed i relation til multinationale koncerner.

Jeg har løbende sammenfattet og konkluderet på de overvejelser og betragtninger, der er fremkommet på baggrund af gennemgangen af den grænseoverskridende behandling af persondata og overførsler til tredjelande samt analyseret udvalgte retlige spørgsmål vedrørende BCR. Ud fra disse sammenfatninger og delkonklusioner kan det således overordnet set konkluderes, at den grænseoverskridende behandling af persondata, herunder overførsler til tredjelande, fortsat er en meget kompleks og uløst del af databeskyttelsesretten. På trods af de forskellige tiltag, der har været fra blandet andet EU og internationale organisationer, er det endnu ikke lykkedes at nå frem til en reguleringsform, der fungerer optimalt i

[107] Jf. i det hele Artikel 29-gruppens WP 108 af 14. april 2005.

praksis. De foreliggende særlige reguleringsformer udgør et fremskridt og et godt og nødvendigt supplement til de almindelige databeskyttelsesretlige regler, men de frembyder hver især egne problemer i forhold til de parter, der skal benytte dem. Set ud fra en erhvervsmæssig betragtning kan det dermed ikke endelig fastslås hvilken reguleringsform, der bør foretrækkes for multinationale koncerner, da det i vidt omfang vil bero på en konkret vurdering af koncernens individuelle forhold og behov for persondataoverførsler.

Under alle omstændigheder er det meget vigtigt at have for øje, at alle typer persondataoverførsler, uanset hvor stor betydning disse måtte have for verdensøkonomien og samhandlen, må være baseret på respekt for borgernes informationelle privatliv og personlige integritet. Værdien heraf er essentiel for individer i et moderne informationssamfund, og databeskyttelsesretten skal som en betydningsfuld del af lex informatica bidrage til at værne om disse værdier og på samme tid tillade multinationale koncerner at udøve deres erhvervsmæssige virksomhed.

Specialets systematik angående anvendte referencer og kildemateriale

Meget af det for dette speciale relevante kildemateriale foreligger som elektroniske pdf-dokumenter eller findes kun i elektronisk web udgave. Derfor er der i referencelisten medtaget hyperlinks til alle disse henvisninger.

Henvisningerne i specialet svarer overens med referencelisten, så når der eksempelvis i en fodnote skrives en henvisning til *ICC - Rapport vedrørende Binding Corporate Rules,* kan denne rapport findes i referencelisten, der er listet alfabetisk, og hentes via det tilhørende hyperlink.

I visse tilfælde kan den direkte URL-adresse ikke hentes. Det gælder eksempelvis domme offentliggjort på EF-Domstolens hjemmeside. I stedet er der indsat dommens nummer og URL-adressen på hjemmesidens front page.

Det anvendte citeringsformat er APA 5th via RefWorks.

Referencer

Andersen, H. & Kaspersen, L. B. [Eds.] (2005). *Klassisk og moderne samfundsteori* (3. reviderede udgave/oversættelse: Tom Havemann ed.). Kbh.: Hans Reitzel.

Artikel 29-gruppens working paper af 25. juni 1997 – WP 3: *First Annual Report*.
Besøgsdato: 01-08-2009
URL:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1997/wp3_en.pdf

Artikel 29-gruppens working paper af 26. juni 1997 – WP 4: *First orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy*.
Besøgsdato: 01-08-2009
URL:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1997/wp4_en.pdf

Artikel 29-gruppens working paper af 24. juli 1998 – WP 12: *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive.*
Besøgsdato: 01-08-2009
URL:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf

Artikel 29-gruppens working paper af 3. juni 2003 – WP 74: *Working document: Transfers of personal data to third countries: Applying article 26 (2) of the EU data protection directive to binding corporate rules for international data transfers.*
Besøgsdato: 04-08-2009
URL:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf

Artikel 29-gruppens working paper af 14. april 2005 – WP 107: *Working document setting forth a co-operation procedure for issuing common opinions on adequate safeguards resulting from binding corporate rules.*
Besøgsdato: 04-08-2009
URL:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp107_en.pdf

Artikel 29-gruppens working paper af 14. april 2005 – WP 108: *Working document establishing a model checklist application for approval of binding corporate rules.*
Besøgsdato: 04-08-2009
URL:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf

Artikel 29-gruppens working paper af 25. november 2005 – WP 114: *Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995.*
Besøgsdato: 04-08-2009
URL:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf

Artikel 29-gruppens working paper af 10. januar 2007 – WP 133: *Recommendation 1/2007 on the standard application for approval of binding corporate rules for the transfer of personal data.*
Besøgsdato: 04-08-2009
URL:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp133_en.doc

Artikel 29-gruppens working paper af 20. juni 2007 – WP 136: *Opinion 4/2007 on the concept of personal data.*
Besøgsdato: 14-07-2009
URL:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

Artikel 29-gruppens working paper af 24. juni 2008 – WP 153: *Working document setting up a table with the elements and principles to be found in binding corporate rules.* Besøgsdato: 04-08-2009
URL:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp153_en.pdf

Artikel 29-gruppens working paper af 24. juni 2008 – WP 154: *Working document setting up a framework for the structure of binding corporate rules.*
Besøgsdato: 04-08-2009
URL:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp154_en.pdf

Artikel 29-gruppens working paper af 24. juni 2008, revideret 8. april 2009 – WP 155: *Working document on frequently asked questions (FAQs) related to binding corporate rules.*
Besøgsdato: 04-08-2009
URL:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp155_rev.04_en.pdf

Bekendtgørelse nr. 30 af 29. marts 1976. Bekendtgørelse af international konvention af 16. december 1966 om borgerlige og politiske rettigheder.
Besøgsdato: 29-06-2009
URL:
https://www.retsinformation.dk/Forms/R0710.aspx?id=60860

Bekendtgørelse nr. 59 af 16. maj 1991. Bekendtgørelse af europæisk konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger.
Besøgsdato: 21-04-2009
URL:
https://www.retsinformation.dk/Forms/R0710.aspx?id=60887

Beretning fra Europa-Kommissionen - Første beretning om gennemførelsen af databeskyttelsesdirektivet (95/46/EF) KOM/2003/0265.
Besøgsdato: 01-08-2009
URL:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:DA:PDF

Betænkning om behandling af personoplysninger nr. 1345/1997.
Besøgsdato: 10-05-2009
URL:
http://www.statensnet.dk/betaenkninger/1201-1400/1345-1997-1/1345-1997-1_pdf/searchable_1345-1997-1.pdf

Blume, P. (2006). *Retlig regulering af internationale persondataoverførsler: Med særligt henblik på den private sektor* (1. udgave ed.). Kbh.: Jurist- og Økonomforbundets Forlag.

Blume, P. (2008). *Databeskyttelsesret* (3. udgave ed.). Kbh.: Jurist- og Økonomforbundets Forlag.

Bundesdatenschutzgesetz - vom 20. Dezember 1990 (BGBl. I S. 2954), neugefasst durch Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), geändert durch § 13 Abs. 1 des Gesetzes vom 5. September 2005 (BGBl. I S.2722) sowie durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970).
Besøgsdato: 27-07-2009
URL:
http://www.bfdi.bund.de/cae/servlet/contentblob/409518/publicationFile/25234/BDSG.pdf

Büllesbach, A., Poullet, Y. & Prins C. [Eds.] (2006). *Concise European IT Law*. The Netherlands: Kluwer Law International.

C-101/01 (EF-Domstolens dom af 6. november 2003).
Besøgsdato: 13-07-2009
URL:
http://curia.europa.eu/jcms/jcms/Jo1_6308/

C-322/88 (EF-Domstolens dom af 13. december 1989).
Besøgsdato: 13-07-2009
URL:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61988J0322:DA:HTML

C-465/00 (EF-Domstolens dom af 20. maj 2003 i de forenede sager C-465/00, C-138/01 og C-139/01).
Besøgsdato: 13-07-2009
URL:
http://curia.europa.eu/jcms/jcms/Jo1_6308/

Copland vs. Storbritannien (Den Europæiske Menneskerettighedsdomstols dom af 3. april 2007, application no. 62617/00).
Besøgsdato: 13-07-2009
URL:
http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=62617/00&sessionid=27739494&skin=hudoc-en

Court of Appeal: Michael John Durant v. Financial Services Authority (case: B2/2002/2636 – 2004).
Besøgsdato: 14-07-2009
URL:
http://www.hmcourts-service.gov.uk/judgmentsfiles/j2136/durant-v-fsa.htm

Den Europæiske Menneskeretskonvention med kommentarer art. 1-10 (2003) (2. udgave ed.). Kbh.: Jurist- og Økonomforbundets Forlag.

Europa-Parlamentets beslutning af 4. september 2007 om institutionelle og retlige virkninger af anvendelse af soft law-instrumenter.
Besøgsdato: 25-07-2009
URL:
http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2007-0366&language=DA&ring=A6-2007-0259

Europa-Parlamentets betænkning om Kommissionens første beretning om gennemførelsen af databeskyttelsesdirektivet (95/46/EF) - (KOM(2003) 265 – C5-0375/2003 – 2003/2153(INI).
Besøgsdato: 23-06-2009
URL:
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2004-0104+0+DOC+PDF+V0//DA

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 - Databeskyttelsesdirektivet.
Besøgsdato: 13-02-2009
URL:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DA:HTML

Forenede Nationer: *International konvention om civile og politiske rettigheder af 16. december 1966.*
Besøgsdato: 13-07-2009
URL:
http://www2.ohchr.org/english/law/pdf/ccpr.pdf

Forenede Nationer: *Guidelines Concerning Computerized Personal Data Files af 14. december 1990.*
Besøgsdato: 13-07-2009

URL:
http://ec.europa.eu/justice_home/fsj/privacy/instruments/un_en.htm

Giddens, A. (1990). *The Consequences of Modernity*. Cambridge: Polity.

Gutwirth, S. [et al.], [Eds.] (2009). *Reinventing Data Protection?* Dordrecht: Springer.

ICC - *Kommentarer og FAQs til Kommissionens beslutning samt en alternative standard-kontrakt - Final approved version of alternative standard contractual clauses for the transfer of personal data from the EU to third countries (controller to controller transfers).*
Besøgsdato: 03-08-2009
URL:
http://www.gov.im/lib/docs/odps/iccmodelclauses1.pdf

ICC – *Standardansøgning BCRs – Standard application for approval of binding corporate rules for the transfer of personal data outside the EU.*
Besøgsdato: 04-08-2009
URL:
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/pages/Standard_Application_for_Approval_of_BCRs.pdf

ICC – *Policy statement: Employee privacy, data protection and human ressources.*
Besøgsdato: 18-06-2009
URL:
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/pages/373-22112Final.pdf
ICC – *Rapport vedrørende Binding Coroprate Rules.*
Besøgsdato: 04-08-2009
URL:
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/pages/FINAL_ICC_BCRs_report_rev.pdf

Kaspersen, L. B. [Ed.]. (2005). *Globalisering på vrangen: Politiske, økonomiske og kulturelle perspektiver*. Kbh.: Frydenlund.

Keohane, R. O., & Milner, H. V. (1996). *Internationalization and domestic politics*. Cambridge: Cambridge University Press.

Kommissionens beslutning af 26. juli 2000 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af Safe Harbor-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra Det Amerikanske Handelsministerium.
Besøgsdato: 02-08-2009
URL:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DA:PDF

Kommissionens beslutning af 15. juni 2001 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til direktiv 95/46/EF. Besøgsdato: 03-08-2009
URL:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:181:0019:0031:DA:PDF

Kommissionens beslutning af 27. december 2001 om standardkontraktbestemmelser for overførsel af personoplysninger til registerførere etableret i tredjelande i henhold til direktiv 95/46/EF.
Besøgsdato: 03-08-2009
URL:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:DA:PDF

Kommissionens beslutning af 27. december 2004 om ændring af beslutning 2001/497/EF for at indføre en alternativ standardkontrakt om overførsel af personoplysninger til tredjelande.
Besøgsdato: 03-08-2009
URL:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:DA:PDF
Kommissionens hjemmeside vedrørende sikre tredjelande.
Besøgsdato: 01-08-2009
URL:
http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

Konventionen til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder af 4. november 1950.
Besøgsdato: 13-07-2009
URL:
http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm

Krüger Andersen, P. (2008). *Aktie- og anpartsselskabsret* (10. reviderede udgave ed.). Kbh.: Jurist- og Økonomforbundets Forlag.

Kuner, C. (2007). *European Data Protection Law: Corporate Compliance and regulation* (2. edition). New York. Oxford University Press.

Lov nr. 293 af. 8. juni 1978 om private registre.
Besøgsdato: 01-06-2009
URL:
https://www.retsinformation.dk/Forms/R0710.aspx?id=59381

Lov nr. 294 af 8. juni 1978 om offentlige myndigheders registre.
Besøgsdato: 01-06-2009
URL:

https://www.retsinformation.dk/Forms/R0710.aspx?id=59382

Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger.
Besøgsdato: 18-03-2009
URL:
https://www.retsinformation.dk/Forms/R0710.aspx?id=828

Nøgletal fra EU vedrørende den globale eksport.
Besøgsdato: 18-06-2009
URL:
http://europa.eu/abc/keyfigures/tradeandeconomy/tradingpower/index_da.htm

Organisation for Economic Co-operation and Development: *Guidelines on the protection of privacy and transborder flows of personal data.*
Besøgsdato: 21-04-2009
URL:
http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

Organisation for Economic Co-operation and Development: *Recommendation on cross-border co-operation in the enforcement of laws protecting privacy.*
Besøgsdato: 05-07-2009
URL:
http://www.oecd.org/dataoecd/43/28/38770483.pdf

Office of the United Nations High Commissioner for Human Rights: *Status of Ratifications of the Principal International Human Rights Treaties.*
Besøgsdato: 15-07-2009
URL:
http://www2.ohchr.org/english/bodies/docs/RatificationStatus.pdf

Perry vs. Storbritannien (Den Europæiske Menneskerettighedsdomstols dom af 17. juli 2003, application no. 63737/00).
Besøgsdato: 13-07-2009
URL:
http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=63737/00&sessionid=27739494&skin=hudoc-en

Rowland, D., & Macdonald, E. (2005). *Information technology law*. London; Portland, Or.: Cavendish Pub.

Société Colas Est og andre vs. Frankrig (Den Europæiske Menneskerettighedsdomstols dom af 16. juli 2002, application no. 37971/97).
Besøgsdato: 13-07-2009
URL:
http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=698308&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649

Svensson, A. L. (2006). *Engelsk-dansk økonomisk ordbog* (5. udgave/Annemette Lyng Svensson ed.). Frederiksberg: Samfundslitteratur.

U.S. Department of Commerce - *Safe Harbor.*
Besøgsdato: 02-08-2009
URL:
http://www.export.gov/safeharbor/index.asp

Verdenserklæring om menneskerettighederne.
Besøgsdato: 05-07-2009
URL:
http://www.un.org/en/documents/udhr/

Wegener, M. (2000). *Juridisk metode* (3. reviderede udgave ed.). [Kbh.]: Jurist- og Økonomforbundets Forlag.

Wet bescherming persoonsgegevens - wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens.
Besøgsdato: 27-07-2009
URL: http://www.dutchdpa.nl/downloads_wetten/wbp.pdf?refer=true&theme=purple

Waaben, H., & Korfits Nielsen, K. (2008). *Lov om behandling af personoplysninger med kommentarer* (2. udgave ed.). Kbh.: Jurist- og Økonomforbundets Forlag.