

Peter Blume

Retlig regulering af internationale persondataoverførsler

– med særligt henblik på den private sektor



Jurist- og Økonomforbundets Forlag
2006

Retlig regulering af internationale persondataoverførsler

1. udgave, 1. oplag

© 2006 by Jurist- og Økonomforbundets Forlag

Alle rettigheder forbeholdes.

Mekanisk, elektronisk, fotografisk eller anden gengivelse af
eller kopiering fra denne bog eller dele heraf er ifølge
gældende dansk lov om ophavsret ikke tilladt uden
forlagets skriftlige samtykke eller aftale med Copy-Dan

Omslaget: Morten Højmark

Tryk: Narayana Press, Gylling

Indbinding: Jysk Bogbind, Holstebro

Printed in Denmark 2006

ISBN 87-574-1363-0

Lyngbyvej 17

Postboks 2702

2100 København Ø

Telefon: 39 13 55 00

Telefax: 39 13 55 55

e-mail: forlag@djoef.dk

www.djoef-forlag.dk

Forord

Emnet for denne bog er en klassiker i databeskyttelsesretten. Spørgsmålet om, hvorvidt og under hvilke betingelser personoplysninger kan overføres til andre lande, har givet anledning til mange hovedbrud. En del retlige løsningsmuligheder foreligger i dag med udgangspunkt i den EU-retlige regulering, men en globalt dækkende løsning savnes fortsat.

Spørgsmålet om, hvorledes dataoverførsler reguleres og bør reguleres, er udfordrende såvel praktisk som teoretisk. Det er en spændende problemstilling, fordi den omfatter mange forskellige aspekter og fører så vidt omkring. Ydermere gør den det nødvendigt endnu engang at overveje den rationalitet og de værdier, der ligger bag databeskyttelsesretten.

Dette er baggrunden for, at jeg har skrevet denne bog med det håb, at den vil interessere både de virksomheder, der har et behov for at eksportere eller importere persondata, og dem, der i almindelighed er tiltrukket af databeskyttelsesrettens emneverden.

Dataoverførselsproblemet er aktuelt i både den offentlige og private sektor. Denne bog vedrører som udgangspunkt kun sidstnævnte. Selvom der er en række fælles træk, er der ligeledes mange forskelle, hvorfor en mest sammenhængende fremstilling bedst opnås ved at koncentrere sig om en af sektorerne. Den private er valgt, fordi den må betragtes som den mest juridisk udfordrende i denne sammenhæng.

Bogen er skrevet i perioden juli-december 2005, med inddragelse af lidt nyt fra januar 2006 i kapitel 6, afsnit 15.

Jeg takker Datatilsynets sekretariat ved direktør Janni Christoffersen og kontorchef Lena Andersen for adgang til materiale vedrørende tilsynets praksis.

Stud.jur. Nadia Saeed har udarbejdet stikordsregistret.

De synspunkter vedrørende gældende ret og om mulige retspolitiske forandringer, der fremgår af bogen, står alene for min regning.

Frederiksberg januar 2006.

Peter Blume

Indholdsfortegnelse

Forord	5
Kapitel 1 Overførselsproblemet	
1. Optakt	11
2. Offentlig og privat sektor	13
3. Persondata	15
4. Beskyttelseshensyn	18
5. Behandling	20
6. Hvad er en overførsel?	21
7. Overførselsproblemet	22
8. Transmission	24
9. Intention om overførsel	24
10. Kun eksport	25
11. Overførselsmetoden	26
12. Eksportøren	28
13. Formål	28
Kapitel 2 Dansk ret	
1. National rets relevans	31
2. Behandlingsformer	32
3. Den dataansvarlige	35
4. Principper	36
5. Sikkerhed	39
6. Hjemmel	41
7. Samtykke	41
8. Almindelige oplysninger	42
9. Følsomme oplysninger	43
10. Markedsføring	44
11. Samme betingelser?	45
12. Rettigheder	46
13. Tilsyn	46
14. Artikel 29-gruppen	47

Indholdsfortegnelse

Kapitel 3 De tre dimensioner

1. Forskellige dimensioner	51
2. Første dimension: Eksportlandets ret	52
3. Anden dimension: Overførselsregler	53
4. Tredje dimension: Importlandets ret	53
5. Flere lande	56
6. Udfordring	57

Kapitel 4 Inden for EU

1. Fri overførsel	59
2. Begrundelsen for fri overførsel	61
3. Harmonisering?	62
4. Direktivets reguleringsform	65
5. Andre hensyn end privatliv	67
6. Inden for direktivets område	68
7. Fri overførsel	70
8. Oplysningspligt	70
9. Indsigt	72
9.1. Register over overførsler	74
10. Korrektion	75
11. Indsigelsesret	75
12. Sammenfatning	76

Kapitel 5 Overførsel til tredjelande

1. Forhistorie	79
2. Udgangspunkt	80
3. Forskellige tredjelande	82
4. Generelt anerkendte lande	83
5. Tilstrækkelighed	84
6. Udfyldning af tilstrækkelighedsnormen	86
7. Forholdet til konvention 108	90
8. Forskellige sektorer	91
9. Føderale lande	92
10. Tillid	93
11. Undtagelser	94
12. De specifikke undtagelser	97
13. Tilladelse	104
14. Behovet for alternativer	110

Kapitel 6 Særlige overførselsgrundlag

1. Det økonomiske overførselsbehov	111
2. Særlige ordninger	112
3. Direktivets globale virkning	114
4. Virksomhedstyper	115
5. Formål	117
6. Oplysningstypen	117
7. Særordninger kan tillades	118
8. Adfærdskodekser	119
9. Kontrakt	121
10. Standardkontrakt	123
11. 2001-kontrakt for dataansvarlige	125
12. 2004-kontrakt for dataansvarlige	130
13. 2001-kontrakt for databehandlere	133
14. Er kontrakt egnet?	136
15. Bindende virksomhedsregler	136
16. Safe Harbor	143
17. Kombination	147
18. Vurdering	148

Kapitel 7 Håndhævelse

1. Betyggende overførsler?	151
2. Datatilsynets rolle	153
3. Selvkontrol	157
4. Tilsynssamarbejde	158
5. Er de lovlige overførsler lovlige?	159
6. Ulovlige overførsler	159
7. Straf	160
8. Erstatning	161
9. Offentlighed	162
10. Datapoliti	162
11. I importlandet	163
12. Vær beredt!	163

Kapitel 8 En ny løsning?

1. Det globale problem	165
2. Virksomhedsinteresse	166
3. Den registreredes interesse	168
4. Problemets kerne	169
5. Tilsvarende niveau	170
6. En ny start	171
7. Forholdet til national ret	173

Indholdsfortegnelse

8. Folkeretligt instrument	175
8.1. Valg af forum	176
8.2. Betænkeligheder	177
9. Inden for EU	178
10. Tredjelande	179
11. Fantasi	179
 Litteratur	 181
 Bilag	
Europa-Parlamentet og Rådets direktiv 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (uddrag)	183
 Lov nr. 429 af 31.05. 2000 om behandling af personoplysninger	 187
Stikordsregister	209

KAPITEL 1

Overførselsproblemet

1. Optakt

Europæisering, Internationalisering og Globalisering er alle nogle af tidens ord. De henviser mindre eller mindre ambitiøst til en samfundsudvikling, som indebærer en reduktion af landegrænsernes betydning, og til en ændret rolle for den nationale ret. De peger ikke så meget på en status, men snarere på en udviklingstendens, som på forskellige områder har varierende styrke, og som kan være udtryk for forskellige behov. Der er tale om en tendens, som har betydning inden for efterhånden de fleste samfunds- og retsområder. Information er blevet en central ressource, og det kan konstateres, at økonomien i betydelig udstrækning er blevet informatiseret. For produktivitet og indtjeningsevne er adgang til information, herunder personoplysninger, ofte af afgørende betydning. Moderne informationsteknologi og i særlig grad Internettet, betyder, at det er blevet både let og værdiskabende at overføre og anvende information på tværs af traditionelle fysiske grænser.¹ Denne fremgangsmåde er blevet stadig mere naturlig.

På databeskyttelsesrettens område er behovet for en retlig regulering, der overskrider grænser, og som kan danne baggrund for en betryggende udveksling og deling af personoplysninger, ikke noget nyt fænomen, men udformningen af denne retlige regulering udgør fortsat en udfordring, som ikke er blevet mødt på en fuldt ud tilfredsstillende måde. Grænser er fortsat omdrejningspunktet i de gældende regler, og et kernespørgsmål er dermed, hvorledes regler, der er baseret på grænser, kan fungere i en verden, hvor der i stigende udstrækning ikke er nogen grænser. Mødet med denne udfordring og de problemer, som denne giver anledning til, er denne bogs tema.

1. Peter Carey: Data Protection (2nd ed. Oxford 2004) p.100: »The globalization of electronic communications and the rapid growth of the Internet has made the transfer of personal data abroad both extremely easy and of great potential value.«

Kapitel 1 Overførselsproblemet

Den retlige beskyttelse af personoplysninger er af forholdsvis ny dato. Den første nationale regulering gennemføres i Hessen i 1970 og den første nationale lovgivning i Sverige i 1973. De første internationale instrumenter fra OECD og Europarådet, der omtales nærmere i kapitel 5, ser dagens lys i 1980. Selvom beskyttelsen af privatlivets fred i den europæiske menneskerettighedskonvention 1950 artikel 8 og sædvanligvis i nationale straffelove er af ældre dato, og selvom diskussionen af problemstillingen i litteraturen kan spores længere tilbage i tid, er det dækkende at betegne databeskyttelsesretten som et nyt retsområde. Den er ny som et barn af den moderne informationsteknologi, som både aktualiserer og tydeliggør, at der foreligger et beskyttelsesbehov,² og reguleringen er ligeledes ny, fordi beskyttelsen rækker videre end den, som følger af det klassiske værn af privatlivets fred, idet databeskyttelsen omfatter enhver personoplysning, herunder bl.a. persondata, som er blevet offentliggjort. Selvom privatlivets fred er det centrale inspirationsgrundlag, aspirerer databeskyttelsen dermed til at repræsentere en selvstændig grundrettighed.³

Selv nye retsområder kan have deres klassiske spørgsmål og blandt disse er nok intet mere fremtrædende end spørgsmålet om overførsel af personoplysninger til andre lande. Det har været en konstant aspiration at udforme en retlig regulering, der kan muliggøre overførsler på en forsvarlig måde; dvs. en måde, som ikke indebærer, at overførslen medfører en risiko for integritetskrænkelser. Denne aspiration, som endnu ikke er fuldt ud tilfredsstillende, er blevet væsentligt mere presserende i takt med den øgede internationalisering og globalisering, der kombineres med den praktiske lettelse af dataoverførsler, som den moderne informationsteknologi indebærer. Overførsler kan i dag ske hurtigere og billigere, end det tidligere var tilfældet. Behovet er vokset, og de praktiske muligheder er forbedrede. Det kan dog fortsat i dag konstateres, at der foreligger mange retlige vanskeligheder, og at der ikke er frit løb med hensyn til dataoverførsler.

2. Allerede brugen af telegrafen medførte nye muligheder for dataoverførsler, men den digitale informationsteknologi må anses for noget kvalitativt nyt.
3. I en erklæring vedtaget september 2005 af verdens datatilsyn, Montreux Declaration: The protection of personal data and privacy in a globalised world: a universal right respecting diversities, fremhæves i nr. 11 databeskyttelse som en fundamental menneskeret. – Dette er i god overensstemmelse med, at databeskyttelse nævnes som en selvstændig rettighed i artikel 8 i EU's charter om grundlæggende rettigheder 1999 (EFT 2000 C 364/01). Bestemmelsen var i øvrigt medtaget som artikel 68 i den ikke for tiden gennemførte forfatningstraktat.

2. Offentlig og privat sektor

Disse vanskeligheder beror på de betydelige retskulturelle forskelle, der er virksomme på globalt plan. Forskelle, der har deres grobund i, hvorledes forholdet mellem stat og samfund, anskues. Bag en databeskyttelsesretlig regulering ligger en opfattelse af, hvorledes forholdet mellem stat og borger samt forholdet mellem virksomheder og individer skal betragtes. Der er varierende opfattelser med hensyn til, i hvilken udstrækning disse relationer retligt bør reguleres, og ligeledes uenighed om, hvilke reguleringsmekanismer som i givet fald bør tages i anvendelse. Disse retskulturelle forskelle indebærer specielt for den private sektors vedkommende, at en retlig beskyttelse af personoplysninger ikke er en selvfølge, og som konsekvens heraf foreligger der en betydelig retlig ujævnhed. En fuldstændig og dermed ureguleret frihed til at foretage overførsler betragtes derfor under især et europæisk perspektiv som hverken forsvarligt eller realistisk, når beskyttelseshensynets styrke som udtryk for grundlæggende rettigheder for borgerne tages i betragtning, men dette udelukker ikke, at der etableres en retlig ramme, som på en smidig måde kan gøre det muligt at foretage persondataoverførsler.

En retlig regulering er etableret, og en række forskellige retlige instrumenter er blevet udviklet, men desuagtet repræsenterer dataoverførsler en retlig problemstilling, som omfatter et væld af aspekter, og som rejser komplicerede spørgsmål, der ikke tilstrækkeligt er blevet besvaret. Klassikeren er stadig levende, og det er indtrykket, at en løsning af overførselsproblemet opfattes som meget væsentligt af mange dataansvarlige virksomheder mm. Der er et stort ønske om en praktisabel og gennemskuelig regulering. Det er denne bogs formål at udrede de forskellige spørgsmål i denne forbindelse og dermed dels at skabe et grundlag for, at de gældende regler kan anvendes på en hensigtsmæssig måde, dels herved at bidrage med et udgangspunkt for de fortsatte retspolitiske overvejelser.

2. Offentlig og privat sektor

Behovet for at overføre persondata foreligger både i den private og den offentlige sektor, men årsagerne til behovet er sædvanligvis meget forskellige. I den private sektor er det først og fremmest økonomiske hensyn, der medfører et behov for at kunne gennemføre dataoverførsler. De er nødvendige for, at virksomheder med en international profil kan fungere optimalt. Hovedparten af de i denne sektor faktisk foretagne overførsler vedrører oplysninger om ansatte (human resources), finansielle data og kundedata. Personlige og ideelle hensyn kan ligeledes begrunde et behov for dataoverførsler, men de kommercielle hensyn, der er knyttet til virksomhedernes drift, er de mest frem-

Kapitel 1 Overførselsproblemet

trædende og er ligeledes dem, der giver anledning til de største retlige vanskeligheder. Gode muligheder for persondataoverførsler kan betragtes som en af forudsætningerne for at det private erhvervsliv kan fungere optimalt i den moderne internationaliserede økonomi indfanget i informationssamfundets rammer.

Udgangspunktet for en stillingtagen til en konkret dataoverførsel er direktiv 95/46 EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger – i det følgende benævnt direktivet. Et yderligere udgangspunkt er lov nr. 429 af 31.5.2000 om behandling af personoplysninger. Loven betegnes ofte persondataloven, men i denne bog kaldes den personoplysningsloven med forkortelsen POL. Som det fremgår af den følgende fremstilling, er direktivet og loven udfyldt af forskellige former for supplerende regulering samt administrativ og i mindre omfang judiciel praksis.⁴

Direktivet og POL udgør ligeledes udgangspunktet i den offentlige sektor, hvor der i forbindelse med myndighedsudøvelse i en del tilfælde kan være et overførselsbehov, eksempelvis mellem nationale skattemyndigheder eller sociale myndigheder. Det er først og fremmest i relation til forskellige former for retshåndhævelse, at overførselsbehovet er aktualiseret og i dag påkalder sig betydelig interesse, bl.a. fordi modstridende retlige grundhensyn i en del tilfælde konfronteres. Dataoverførsler tillægges betydning i bestræbelserne på at forebygge og bekæmpe forskellige former for kriminalitet, herunder terror, der er en af de store og svært gennemskuelige udfordringer, som databeskyttelsesretten i disse år konfronteres med. Betydningen af sådanne overførsler understreges ofte med stor styrke,⁵ idet der i forbindelse med vurderingen af disse overførslers omfang og betingelserne for deres gennemførelse foreligger en betydelig retspolitisk uenighed om, hvorvidt grundlæggende rettigheder for borgerne herved krænkes. Disse overførsler er kontroversielle og hører til de mere »hotte« emner i den aktuelle retspolitiske debat. I forhold til overførsler med henblik på retshåndhævelse finder direktivet ikke altid an-

4. I bogens bilag er medtaget POL samt et uddrag af direktivet. Adgang til de forskellige retskilder fås lettest via Datatilsynets hjemmeside, www.datatilsynet.dk. I forhold til denne bogs tema må særligt fremhæves, at der under rubrikken internationalt er links til Europa-Kommissionens hjemmeside og til de udenlandske datatilsyn, der har oprettet en hjemmeside.

5. Jfr. eksempelvis Europa Kommissionens beslutning K (2004) 1914 af 14.5.2005 om overførsel af passagerdata (såkaldte PNR data). I dette som i en del andre tilfælde indebærer de offentligretlige hensyn, at private virksomheder, in casu luftfartsselskaber, pålægges en overførselsforpligtelse. Overførsler af denne karakter adskiller sig dermed fra de tilfælde, som er betinget af kommercielle hensyn.

3. Persondata

vendelse, jfr. artikel 13, og personoplysningslovens rolle er ligeledes tit forholdsvis sekundær. Den retlige regulering er i nogle tilfælde baseret på specielle retlige instrumenter, herunder Schengen- og Europol-aftalerne.⁶

Selvom der er visse fælles træk er overførselsproblemet og de retlige overvejelser dette giver anledning til i betydeligt omfang forskellige i den private og den offentlige sektor, og det vil derfor, også af hensyn til læsekredsen, være noget anspændt at samle dem i den samme fremstilling, som let vil kunne fremtræde som uhomogen. På denne baggrund tager denne bog udelukkende sigte på dataoverførsler i den private sektor med hovedvægten lagt på overførsler foranlediget af et kommercielt behov. Dette valg beror dels på, at det er i denne sektor, at det største antal dataansvarlige har en interesse i spørgsmålet, dels at de løsningsmodeller, der er udviklet her, har den største almene interesse, idet de belyser mange af de afvejninger, som i almindelighed har betydning for udformningen af databeskyttelsesretten.

Under et retssikkerhedsperspektiv kan det hævdes, at overførsler i den offentlige sektor eller som er baseret på offentlige hensyn, må påkalde sig størst interesse, men som det vil fremgå senere, spiller en hensyntagen til retssikkerhed også en betydelig rolle i den private sektor. Det er i en vis forstand dette hensyn, som udgør grobunden for de komplikationer, der foreligger, idet beskyttelsen af den personlige integritet og den kommercielle interesse i at have adgang til personoplysninger ikke altid er let at forene. Det er denne manglende forenelighed, som udgør en af hovedårsagerne til, at overførselsproblemet foreligger.

Det er i en vis forstand lidt af en smags sag, hvor man vælger at lægge vægten, men under alle omstændigheder giver det en mere overskuelig og sammenhængende fremstilling at koncentrere den om en af sektorerne, og min smag har altså været til den private sektor.⁷

3. Persondata

Indledningsvis er det hensigtsmæssigt at afklare en række af de fundamentale begreber, der har betydning for overførselsproblemet. Genstanden for en overførsel er personoplysninger eller persondata. Det er alene overførsel af

6. Se lov 415 (Europol) og 418 (Schengen) af 10.6.1997.

7. I visse situationer vil en overførsel fra en offentlig myndighed til en myndighed i et andet land kunne have interesse for den private sektor. Dette kan være tilfældet, når den modtagende myndighed videregiver de overførte oplysninger til virksomheder i den private sektor.

Kapitel 1 Overførselsproblemet

sådanne data, der er omfattet af den retlige regulering, som behandles i denne bog. Persondata er legaldefineret i direktivets artikel 2a og POL § 3 nr.1. Det fremgår heraf, at der er tale om oplysninger, som kan henføres til en identificeret eller identificerbar fysisk person, der i reguleringens terminologi betegnes den registrerede. Negativt indebærer denne definition, at anonyme oplysninger samt fuldt ud anonymiserede oplysninger ikke er omfattet, idet der ikke i forhold til sådanne oplysninger er nogen risiko for integritetskrænkelser. Sådanne oplysninger karakteriseres ved, at det ikke er muligt ved hjælp af adgang til koder o.lign. at henføre oplysningen til en bestemt person. Er oplysningen eksempelvis krypteret, vil den være identificerbar, såfremt den kan dekrypteres ved hjælp af krypteringsnøglen.⁸ Det er alene, såfremt en sådan afkodning ikke er mulig, eller den kun kan ske ved en uforholdsmæssigt stor ressourceanvendelse, at der er tale om en anonymiseret oplysning.

I en overførselssituation optræder en eksportør og en importør, idet det er forholdet mellem disse, som er reguleret i de regler, der omtales i kapitel 4-6. Det kan overvejes, om det er nødvendigt, at der er tale om persondata for begge parter, for at overførselsreglerne aktualiseres. Det kan være nærliggende, at dette ikke er tilfældet i den situation, hvor eksportøren har foretaget en fuldstændig anonymisering med den konsekvens, at importøren ikke er i stand til at identificere de overførte oplysninger under den forudsætning, at eksportøren ikke senere skaber mulighed herfor. Foreligger der tilstrækkelig sikkerhed herfor, modtager importøren ikke persondata, idet oplysningerne ikke er identificerbare for denne. Det er muligvis denne opfattelse, der er baggrunden for, at det i Østrigs Datenschutzgesetz 2000 § 12(3 nr.2) gøres muligt at overføre data, der kun indirekte er persondata for modtageren. Eksportøren må nationalt overholde personoplysningsloven i forhold til andre former for behandling, men det er nærliggende at lægge til grund, at overførslen ikke har karakter af en persondatabehandling. Lovgivningens regler er formentlig ikke anvendelige i denne situation, idet der ikke udløses nogen risiko for, at de overførte data kan misbruges med integritetskrænkelser til følge. Problemstillingen er vist nok ikke afklaret i dansk ret.

Det er som fremhævet en forudsætning for, at der foreligger en personoplysning, at oplysningen kan henføres til en bestemt person. Dette indebærer, at oplysninger om en bestemt gruppe af fysiske personer, som ikke er individuelt identificerede, ikke er omfattet af reglerne. Overførsel af en generel

8. I Estlands personoplysningslov af 12.2.2003 (RT I 2003,26,158) fastsættes i § 28(6 nr.3), at overførsel i krypteret form frit kan ske, såfremt krypteringsnøglen ikke overføres, jfr. yderligere hertil nedenfor.

3. Persondata

karakteristik af de ansatte i en virksomhed vil således ikke udgøre en overførsel af personoplysninger, idet der muligvis må tages forbehold i forhold til virksomheder med meget få ansatte. Det bør herved tilføjes, at en generel karakteristik kan være krænkende, men bedømmelsen heraf beror på andre dele af retssystemet end databeskyttelsesretten.

Det er som udgangspunkt uden betydning, hvorfra personoplysningerne stammer og hvilken nationalitet personerne har, herunder om de statsborgere i et EU-land. Konsekvensen heraf er bl.a., at regler, som begrænser overførsel af oplysninger til et bestemt land, også omfatter oplysninger om dette lands borgere, når disse oplysninger befinder sig i eksportlandet, f.eks. Danmark.

Bestemmelserne gælder således for alle personoplysninger, som er i overførerens besiddelse. Selvom der vist nok ikke er eksempler herpå i dansk praksis, kan der muligvis ved vurderingen af konkrete overførsler tages hensyn til, om udlændinge grundet deres nationale retskultur har særlige forventninger i relation til beskyttelsen af deres personoplysninger. En sådan opfattelse er lagt til grund i engelsk ret,⁹ idet det herefter kan tillægges betydning, at der i en bestemt situation foreligger en lavere forventning til databeskyttelse end sædvanligt i eksportlandet. Selvom der kan være en vis ræson i denne tankegang, specielt hvis personoplysningerne kun kortvarigt befinder sig i eksportlandet, er der tale om et moment, der kun kan tillægges en marginal betydning ved bedømmelsen af, om en overførsel kan finde sted. Udgangspunktet er således i dansk ret, at nationalitet og oplysningernes oprindelse ikke har betydning ved vurderingen af dataoverførsler.

Oplysninger om juridiske personer, virksomheder, foreninger og myndigheder er ikke persondata og er dermed ikke er omfattet. Beskyttelse af omdømme eller image har ikke samme karakter som beskyttelse af personlig integritet. Direktivet udelukker dog ikke, jfr. præambelens Betragtning 24, at det i national ret kan bestemmes, at også sådanne oplysninger beskyttes efter de nationale regler. I dansk ret er dette tilfældet på enkelte områder, jfr. POL § 1(3). En undtagelse fra dette almindelige udgangspunkt er, at oplysninger om enkeltpersondrevne virksomheder, f.eks. et I/S, betragtes som personoplysninger, hvilket er baseret på den opfattelse, at det personlige og det erhvervsmæssige ikke kan adskilles. Er der tale om en sådan oplysning, gælder de almindelige regler fuldt ud. Sådanne oplysninger er persondata.

9. Data Protection Act 1998 fremhæver i Schedule 1 som et moment ved vurderingen af overførsler (uden for EU) »the country of origin of the information contained in the data«.

Kapitel 1 Overførselsproblemet

Den her foretagne fastlæggelse af persondatabegrebet er sket på grundlag af dansk ret. Som det fremgår især i kapitel 4, forstås dette fundamentale begreb ikke på fuldt ud samme måde i alle EU-medlemsstater, uanset at de alle er underlagt direktivet. Sådanne fortolkningsforskelle har betydning for de praktiske muligheder for persondataoverførsler, jfr. hertil senere.

4. Beskyttelseshensyn

Denne afgrænsning af overførselens genstand har nær sammenhæng med de beskyttelseshensyn, som reguleringen søger at varetage. Den er således baseret på den grundantagelse, at oplysninger om personer giver en viden om den enkelte persons personlighed og private forhold med den konsekvens, at sådanne oplysninger vil kunne misbruges på en sådan måde, at der i forhold til personen opstår en integritetskrænkelse. Denne krænkelse kan være følelig og eksempelvis medføre et tab eller udsætte personen for noget, denne anser som uønskeligt, f.eks. markedsføring. Krænkelsen kan dog også være mere ubestemmelig og være relateret til almene opfattelser af personers autonomi og værdighed, der i samfundet anses for at udgøre et grundlag for grundlæggende rettigheder. Den retlige regulering er i en vis udstrækning baseret på forholdsvis vage begreber, og det er ikke muligt i en kort præcis formel at angive, hvad der i denne sammenhæng skal forstås ved privathed.¹⁰ Der kan derfor også være forskellige opfattelser af, hvor tungtvejende beskyttelseshensynet er, og hvorledes dette bedst lader sig udmønte i specifikke retlige regler, der samtidig tager hensyn til legitime behov for at kunne anvende personoplysninger. Disse behov kan ofte for en umiddelbar betragtning fremtræde mere tungtvejende end den noget ubestemmelige privathed. De modsatte hensyn er svært sammenlignelige, og det er undertiden blevet anført, at det savner mening at søge at afbalancere dem. Der skal på denne baggrund ofte tages stilling til vanskelige afvejningsspørgsmål, idet det herved har betydning, at den fastsatte regulering tillige tjener det generelle formål at fastlægge, hvorledes virksomheder m.fl. kan behandle persondata.

10. Se i denne sammenhæng Peter Blume: Databeskyttelsesret (2.udg. København 2003) p.20-42. – Raymond Wacks: Law, Morality and the Private Domain (Hong Kong 2000) fremhæver p.214, at »the long search for a »definition« of »privacy« has produced a continuing debate that is often sterile and, ultimately, futile«. Dette er nok at stille sagen lige lovligt på spidsen, men det er ikke påkrævet her at gå nærmere ind i dette spørgsmål.

4. Beskyttelseshensyn

I denne relation er en væsentlig problemstilling, om der er behov for en beskyttelse af alle former for personoplysninger eller kun af sådanne, hvis misbrug med en rimelig grad af sandsynlighed vil kunne medføre en krænkelse af privatheden. Med andre ord om beskyttelsen alene bør omfatte de oplysningstyper, som befinder sig i kerneområdet af beskyttelsen af privatlivets fred i EMRK artikel 8, eller om den skal være videregående. Det klare udgangspunkt i gældende databeskyttelsesret er, at alle personoplysninger er beskyttelsesværdige, hvilket som nævnt ovenfor indebærer, at beskyttelsen er betydeligt bredere end den menneskeretlige. Databeskyttelsen strækker sig fra de mest trivielle til de mest følsomme personoplysninger. Der er ikke nogen undtagelser, hvilket undertiden har ført til kritik af, at reguleringen er for bred og savner tilstrækkelig rationalitet og realisme. Under alle omstændigheder medfører denne bredde, at overførselsproblemet er aktuelt i forhold til alle personoplysninger,¹¹ hvilket i betydelig udstrækning er medvirkende til komplicere dette og ligeledes gør det yderligere vanskeligt at tage stilling til de ovenfor nævnte afvejningsspørgsmål.

Denne afgrænsning af reguleringsgenstanden er dog ikke ensbetydende med, at det er de samme regler, som gælder i forhold til behandlingen af alle former for personoplysninger. I gældende ret er det lagt til grund, at visse oplysninger er mere integritetsrisikable end andre. Der er således i direktivet (artikler 7 og 8) gennemført en sondring mellem almindelige og følsomme oplysninger, idet der gælder strengere regler for sidstnævnte. Her i landet er denne opdeling forfinet yderligere (§§ 6-8) med en opdeling mellem almindelige, almindelige fortrolige, følsomme, og semifølsomme oplysninger, idet det kan fremhæves, at alle oplysningstyper, der ikke specifikt er nævnt i §§ 7 og 8 eller § 11 (personnummer), er almindelige og omfattet af § 6.¹²

Denne opdeling er generel, idet det dog også lægges til grund, at den faktuelle kontekst kan indebære, at en almindelig oplysning kan blive følsom. En fortegnelse med navne på personer, der deltager i et forsøg med et nyt medicinalprodukt, vil derfor kunne blive betragtet som følsom, selvom et navn er

11. Det er interessant at bemærke, at § 12(3 nr.1) i Østrigs Datenschutzgesetz 2000 fastsætter en særregel, der gør det muligt at overføre persondata, der er offentliggjort i Østrig.

12. Det kan bemærkes, at de enkelte oplysningskategorier er ganske brede, hvilket bedst illustreres af § 7 (= artikel 8), der omfatter de mest følsomme oplysninger. En af disse er oplysninger om helbredsmæssige forhold, der kan omfatte alt fra cancer til en brækket lillefinger. Kategorierne er ligeledes kulturafhængige. Der kan således i forskellige lande være reel forskel på følsomhedsgraden af en oplysning om, hvorvidt en person er medlem af den danske folkekirke, men den er desuagtet altid følsom. Et hensyn til kulturen kan dog have en vis betydning ved vurderingen af en konkret dataoverførsels betimelighed.

Kapitel 1 Overførselsproblemet

en almindelig oplysning. Herved imødekommes den kritik af opdelingen, som er baseret på, at enhver oplysning kan være følsom. Derimod er det modsatte, at en følsom oplysning grundet konteksten bliver betragtet som almindelig, ikke ifølge praksis muligt. Opgradering, men derimod ikke nedgradering, kan grundet konteksten finde sted.¹³

Opdelingen mellem forskellige oplysningstyper har først og fremmest betydning for en vurdering af, om en persondatabehandling nationalt er lovlig, men den kan dog tillige have en vis betydning ved bedømmelsen af en konkret overførselssituation. Jo mere følsomme de pågældende persondata er, desto mere sikkert skal det være at overførslen er i overensstemmelse med de fastsatte regler, som dermed underkastes en særlig streng fortolkning. Opdelingen mellem forskellige oplysningstyper spiller en rolle såvel for vurderingen af overførselens tilladelighed som i forhold til de procedurer, som skal følges i denne forbindelse, jfr. kapitel 5 og 6.

5. Behandling

Reguleringen vedrører behandling af personoplysninger. Behandling er således reguleringens andet kodeord. Herved forstås som udgangspunkt enhver aktivitet i forbindelse med en personoplysning, jfr. direktivets artikel 2b og POL § 3 nr.2. Reguleringen er dermed vidtfavnende og omfatter alt, der kan forekomme fra oplysninger indsamles, til de blive slettet eller arkiveret. Hermed er reguleringen betydeligt mere vidtgående end de oprindelige registerlove,¹⁴ der hovedsageligt alene omfattede registrering og videregivelse af registrerede oplysninger. Der kan dog fortsat spores enkelte »tilbagefald« til denne form for regulering, jfr. hertil i kapitel 5.

For en umiddelbar betragtning er der ikke nogen undtagelser fra behandlingsbegrebet, men i dansk praksis er enkelte særegne undtagelser, som dog kun sjældent har nogen direkte betydning for dataoverførsler, blevet anerkendt.¹⁵ Der findes endnu ikke afgørelser fra EF Domstolen, som giver grundlag for antagelser om, hvorvidt sådanne undtagelser er acceptable, idet det kan tilføjes, at der ikke i denne henseende følges den samme praksis i alle EU-lande, jfr. videre om denne problemstilling i kapitel 4.

13. Dette gælder principielt, selvom oplysningen er offentliggjort af den registrerede, jfr. dog § 7(2 nr.3), hvorefter sådanne oplysninger kan behandles.

14. Lovbkg. nr.622 af 2.10.1987 om private registre mv., lovbkg. nr.654 af 20.9.1991 om offentlige myndigheders registre.

15. Se herom Peter Blume: *Behandling af persondata* (2003) p.67-69.

6. Hvad er en overførsel?

Der er ikke nogen tvivl om, at overførsel er en behandling, men hvad der skal forstås ved en overførsel, kan give anledning til nogen tvivl. Det kan indledningsvis konstateres, at der ikke findes nogen legaldefinition af begrebet. Umiddelbart forekommer det let at definere, hvad en overførsel er. Denne betegner således den situation, at oplysning, der behandles i medfør af et lands lovgivning, flyttes, således at behandlingen nu er omfattet af et andet lands lovgivning. Konsekvensen af en sådan flytning af personoplysninger er, at de ikke længere er omfattet af dansk ret, men den ret, der gælder i den jurisdiktion, de er blevet flyttet til. Dette indebærer bl.a., at videregivelse m.v. til udenlandske ambassader og repræsentationer må vurderes som en dataoverførsel.¹⁶

Med dette udgangspunkt bliver det således af stor betydning, hvorledes det civile lovvalg er fastlagt i databeskyttelsesretten. Reglerne om lovvalg fremgår af direktivets og lovens artikel 4/§ 4. Udgangspunktet er her det sædvanlige EU-retlige, idet det er etableringslandet, der er bestemmende for lovvalget. Persondatabasebehandling foretaget af virksomheder (dataansvarlige), der er etablerede i Danmark, og hvis aktivitet foregår inden for EU, er omfattet af dansk ret. Ved etablering forstås, at aktiviteterne har en vis permanent struktur, jfr. direktivets præambel betragtning 19. Det afhænger af en konkret vurdering, hvorvidt en sådan struktur foreligger, idet der herved kan tages hensyn til, hvorledes etableringsbegrebet sædvanligvis forstås inden for EU-retten.

For så vidt angår forholdet mellem EU-landene, jfr. i kapitel 4, er reguleringens overordnede formål at sikre, dels at der altid er et lands lovgivning, som finder anvendelse, således at retstomme rum undgås, dels så vidt muligt at undgå, at flere landes lovgivning finder anvendelse på samme tid.¹⁷ Reglerne varetager dermed en ordensmæssig funktion. Behandles oplysninger her

16. I Registertilsynets Årsberetning 1986 p.41 blev det fastslået, at ambassader falder uden for begge registerlove og dermed hverken skal betragtes som offentlige eller private. – Det er ikke sikkert, at denne opfattelse fortsat fuldt ud lægges til grund. I Datatilsynets udtalelse af 22.6.2005 i en sag vedrørende databasen CPR Søg lægges således til grund, at ambassader skal bedømmes som private, idet det kan anmærkes, at spørgsmålet om hvorvidt der foreligger en overførsel, når ambassader indhenter oplysninger fra databasen, ikke er nævnt.

17. Det kan fremhæves, at en filial af en dataansvarlig i et EU-land, som er etableret her i landet, er omfattet af dansk ret, uanset hvor behandlingen finder sted, jfr. Kristian Korfits Nielsen, Henrik Waaben: Lov om behandling af personoplysninger (København 2001) p.119. § 4 har således en vis ekstraterritorial virkning.

Kapitel 1 Overførselsproblemet

i landet af en virksomhed, der er etableret i andet EU-land finder dette lands ret anvendelse. Datatilsynet, der har jurisdiktion, jfr. direktivets artikel 28(6), skal dermed i sådanne tilfælde anvende det pågældende lands personoplysningslov, jfr. POL § 64(1). Tilsynet vil kunne konsultere det pågældende lands datatilsyn, således at retsanvendelsen bliver korrekt.

I forhold til lande uden for EU, de såkaldte tredjelande, er det i § 4(3) fastsat, at dansk ret gælder, såfremt virksomheden anvender hjælpemidler, f.eks. edb-udstyr som centrale servere eller terminaler, der indebærer, at behandlingen faktisk sker i Danmark. Det følger endvidere af denne regel, at indsamles der f.eks. via en hjemmeside aktivt oplysninger fra Danmark, er denne indsamling omfattet af dansk ret. Dette kan eksempelvis være indiceret af, at der på hjemmesiden bliver anvendt dansk sprog. Foretages der i sådanne tilfælde en ulovlig persondatabehandling, er det dermed forudsat, at eksempelvis en udenlandsk domstol skal anvende dansk databeskyttelsesret, idet der dog vist nok ikke findes eksempler herpå.

Alt i alt må det konstateres, at bestemmelserne om lovvalg, der ikke omfatter strafferetten, som reguleres af reglerne i straffelovens kapitel 2, er ganske komplicerede.¹⁸ Disse regler, der juridisk fastlægger rammerne for, hvornår overførselsspørgsmålet opstår, giver dog vistnok kun sjældent anledning til tvivl i praksis.

7. Overførselsproblemet

En overførsel foreligger, når persondatabehandling er omfattet af et andet lands ret. Overførselsproblemet opstår som følge af, at de personoplysninger, der har været beskyttet af den nationale ret, efter overførslen befinder sig et sted, hvor disse regler ikke finder anvendelse. Er den nye jurisdiktions regler bedre eller blot de samme, foreligger der ikke noget væsentligt problem, men er reglerne dårligere, eller er der slet ikke nogen regler, foreligger der et problem set under den enkelte persons perspektiv. Det kan således opfattes som en underminering af databeskyttelsen, såfremt det uden videre er muligt at flytte persondata til et sted, hvor de kan anvendes mere frit og dermed også med større risici for integritetskrænkelser, end tilfældet er nationalt. En tradi-

18. Jfr. Betænkning 1345/1997 p.218 om direktivets artikel 4. Se endvidere drøftelsen i Christopher Kuner: *European Data Privacy Law and Online Business* (Oxford 2003) p.90-108.

Se i øvrigt Artikel 29-gruppens WP 56 af 30.5.2002 p.5-10 med en god oversigt over artikel 4. – Om Artikel 29-gruppen se i kapitel 2.

7. Overførselsproblemet

tionel frygt har været, at oplysninger bliver flyttet til de såkaldte data havens, hvor der ikke er nogen regulering, og hvor alt er muligt. I takt med den moderne kommunikationsteknologis udvikling er dette en frygt, der er blevet forstærket i betragtning af, at der findes et stort antal data havens.

Forfølges indtil videre dette spor, kan der ydermere anføres argumenter, som kan understøtte den opfattelse, at der i og for sig kun bør kunne ske overførsler til områder, hvor beskyttelsen er bedre. Problemstillingen ansues her under den registreredes perspektiv, og denne vil ofte opleve sig i en svag position i forhold til handlinger, der finder sted i en fremmed jurisdiktion. Her er den almindelige kultur anderledes, sproget er fremmed og måske endda ulæseligt, og yderligere er det ukendte myndigheder, der har ansvar for databeskyttelsen. Den registrerede har derfor ringere muligheder for at sikre, at personoplysninger ikke bliver misbrugt. Under alle omstændigheder kan der være en betydelig usikkerhed i denne henseende.

Der er dog også stærke argumenter imod en alt for bastant afskæring af dataoverførsler. Det kan anføres, at det også nationalt, herunder i Danmark, tit er vanskeligt for den registrerede at varetage sine interesser i forhold til sine data og at der derfor ikke er nogen grund til at romantisere de hjemlige forhold. En fremmed retskultur medfører ikke nødvendigvis en reelt ringere databeskyttelse. Mere tungtvejende er den omstændighed, at overførsel af personoplysninger er et af de centrale fundamenter for internationalisering og globalisering. Der er tale om en af drivkræfterne i denne udvikling, og det vil føre til en uoverskuelig situation såfremt sådanne overførsler ikke var mulige. En sådan regulering vil blive konfronteret med økonomiske behov, som ikke i længden vil kunne modstås. Den vil ikke være realistisk. Det er ikke databeskyttelsesrettens formål at stille sig hindrende i vejen for almindelig erhvervsudøvelse, og i dag er megen af denne udøvelse af international karakter. Under dette perspektiv er det nødvendigt, at der kan ske overførsler, og det er ligeledes ønskeligt, at dette kan ske uden for snærende retlige barrierer og uden, at det er nødvendigt at aktivere et alt for tungt bureaukrati.

Der er alt i alt tunge vægte på begge sider af vægtskålen, og det er derfor som i forhold til så mange andre af databeskyttelsens problemstillinger nødvendigt at finde en afbalanceret løsning, der tager hensyn til begge synsvinkler. En gennemgående problemstilling i denne bog er dermed, om den regulering, der gælder i dag, er udtryk for en sådan balance. Spørgsmålet er, om der tages tilstrækkeligt hensyn både til den enkeltes beskyttelsesbehov og til den kommercielle interesse. Bag fremstillingen af gældende ret lurer således hele tiden denne retspolitiske problemstilling.

8. Transmission

Overførselsbegrebet kan yderligere præciseres i en række henseender. For at der skal foreligge en overførsel, er det forudsat, at oplysninger med en vis grad af permanens er flyttet til en anden jurisdiktion, hvor de bliver genstand for en behandling. Ved at tillægge dette moment betydning tages der især hensyn til de særlige træk ved den moderne teknologi idet denne præcisering indebærer, at den blotte transmission af data via en bestemt jurisdiktion ikke i sig selv indebærer en overførsel.¹⁹ Oplysningerne er kun på rejse. Det er eksempelvis velkendt, at en e-mail, der evt. er ledsaget af diverse filer, routes i opdelte elementer på vej frem til modtageren. Ruten, der ikke er kendt af afsender og modtager, kan gå igennem flere jurisdiktioner, hvilket i øvrigt også kan være tilfældet for en rent indenlandsk mail.

Det siger nærmest sig selv, at en regulering, der indebar, at retlige betingelser relateret til de jurisdiktioner, som passerer, skal opfyldes for at gennemføre en sådan transmission, både ville være upraktisk og have uoverskuelige konsekvenser. Selvom transmitterede data i princippet vil kunne opsnappes og lagres i en »uønskelig« jurisdiktion, må denne risiko forebygges ved hjælp af sikkerhedsforanstaltninger, hvilket især er aktuelt for persondata af en vis følsomhed. Persondata kan blive underlagt krav under rejsen, men denne opgave er ikke egnet til at blive varetaget via overførselsreglerne, der således ikke gælder, når der udelukkende sker transmission, jfr. POL § 4(3 nr.1).

Det bør præciseres, at det kun er den rene transmission, der ikke er omfattet af overførselsreglerne. Mange overførsler er ikke karakteriseret ved at være »point to point«, idet personoplysningerne passerer og gør ophold ved en række mellemstationer, inden de når deres endelige destination. Dette kan eksempelvis være tilfældet ved overførsler inden for international koncern. I sådanne situationer finder reglerne anvendelse også i forhold til mellemstationerne.

9. Intention om overførsel

Det er i et vist omfang forudsat, at den dataansvarlige skal have en intention om at foretage en overførsel. Den omstændighed, at en sådan faktisk finder

19. Jfr. Kristian Korfijs Nielsen, Henrik Waaben: Lov om behandling af personoplysninger (København 2002) p.285, hvor der lægges vægt på, at modtageren befinder sig i et tredjeland.

sted eller i hvert fald bliver muliggjort, er ikke nødvendigvis altid tilstrækkelig til, at der foreligger en overførsel. Det må herved præciseres, at placeres personoplysninger f.eks. grundet en teknisk fejl i en fremmed jurisdiktion, vil der sædvanligvis være tale om overførsel. Den her foretagne afgrænsning tager dermed udelukkende sigte på situationer, hvor en i øvrigt lovlig persondatabehandling ikke omfatter en intention om at foretage en overførsel. Denne negative afgrænsning har i praksis særligt været aktuel i forhold til offentlige myndigheders hjemmesider med personoplysninger, der uden den registreredes samtykke som følge af offentlighedslovgivningen kan formidles, men noget tilsvarende må antages at gælde i den private sektor. Et eksempel kan være en tilgængelig database med navne og arbejdstelefonnumre på ansatte i dansk nationalt orienteret virksomhed. En sådan database vil uanset at den er globalt tilgængelig, ikke implicere en overførsel.

Det er i almindelighed lagt til grund, jfr. herved også EF Domstolens afgørelse i Lindqvist sagen,²⁰ at den blotte omstændighed, at persondata placeres på en hjemmeside og dermed er tilgængelige globalt, ikke indebærer en overførsel.²¹ For at dette skal være tilfældet forudsættes det, at hjemmesiden aktivt er rettet mod modtagere i en eller flere fremmede jurisdiktioner. I vel nok de fleste tilfælde vil der ikke være tvivl om, hvorvidt dette er tilfældet, men foreligger en sådan situation, kan der tages hensyn til forskellige faktorer, herunder det anvendte sprog, f.eks. en dansk hjemmeside på kinesisk, og informationens karakter. Der foreligger endnu ikke yderligere praksis, der kan belyse, om der er andre særlige momenter, der kan tillægges betydning i den private sektor, men der vil kun sjældent være egentlig tvivl om, hvorvidt en overførsel er intenderet.

10. Kun eksport

Den retlige regulering vedrører som udgangspunkt alene eksport af persondata. Overførselsreglerne angår, hvornår persondata kan flyttes ud af en bestemt jurisdiktion, således at eksportlandets ret ikke finder anvendelse, men derimod ikke, hvornår de kan føres ind i denne. En sådan import medfører ikke noget særskilt behov for regulering, eftersom disse data vil være omfattet af

20. C 101-01 (2003), jfr. især nr.61, 68 og 70.

21. Oprindelig var direktivet i Sverige implementeret således, at der var tale om en overførsel, hvilket udløste en betydelig folkelig modstand under sloganet *do not touch my Internet*, hvilket medførte en lovændring, jfr. herom Sören Öman, Hans-Olof Lindblom: *Personuppgiftslagen* (2.udg. Stockholm 2001) p.19-21, 242, 244-45.

Kapitel 1 Overførselsproblemet

den pågældende importlands regler.²² I denne forbindelse kan det på ny præciseres, at POL omfatter alle de personoplysninger, der befinder sig inden for dansk jurisdiktion med undtagelse af tilfælde, hvor den dataansvarlige er etableret i et andet EU-land, idet det i så fald er dette lands ret, der finder anvendelse. Det har således som udgangspunkt ingen betydning, hvorfra de pågældende oplysninger stammer, eller hvilken nationalitet den registrerede har, eller om den registrerede selv befinder sig på dansk territorium.

Overførselsreglerne er kun aktuelle i forbindelse med eksport, men dette er dog ikke ensbetydende med, at den importerende jurisdiktions regulering er uden interesse, jfr. nærmere hertil i kapitel 3, hvor det fremhæves, at importlandets ret må medtænkes i en fuldstændig forståelse af overførselsproblemet. Det kan være denne ret, som skaber de egentlige vanskeligheder i forhold til den konkrete overførselssituation.

11. Overførselsmetoden

Ved vurderingen af om der foreligger en overførsel, har det ingen betydning, hvilket medium der er benyttet til at flytte de pågældende data, og ligeledes i hvilken form de befinder sig. Herved illustreres endnu engang den betydelige bredde, der karakteriserer den databeskyttelsesretlige regulering. Når der bortses fra den ikke systematiske behandling af manuelle data, der ikke er omfattet af loven, jfr. § 1(1-2), gælder de databeskyttelsesretlige regler for overførsler af enhver form for personoplysninger. Da den kommercielle og samfundsmæssige interesse i dag først og fremmest er relateret til overførsler i elektronisk form, er det ikke påkrævet her at gennemføre nogen større øvelse med hensyn til, hvorledes der kan skelnes mellem systematisk og ikke systematisk manuel behandling, jfr. dog i kapitel 3 vedrørende importsituationens betydning.

Det kan dog som et kuriosum nævnes, at en papirliste over forretningsforbindelser eller kunder vil kunne udgøre en systematisk behandling, hvilket gør de danske overførselsregler anvendelige og samtidig kan accentuere et af de mange håndhævelsesproblemer, som foreligger i forbindelse med data-

22. Christopher Kuner: *European Data Privacy Law and Online Business* (Oxford 2003) overvejer p.124 med note 17, om det skulle være forbudt at importere personoplysninger, der er blevet indsamlet i strid med menneskerettighederne. Et sådant forbud kan ikke direkte udledes af direktivet eller loven, men det kan nok antages, at det vil være i strid med princippet om god databehandlingsskik, jfr. § 5(1), at behandle sådanne oplysninger.

11. Overførselsmetoden

overførsler, jfr. nærmere hertil i kapitel 7. Det må i denne forbindelse fremhæves, at dansk ret i forhold til manuelt behandlede oplysninger er mere bred end den regulering, som følger af direktivet, der alene omfatter manuelle registre, jfr. artikel 3(1).

Alle former for overførsel af persondata i digital form er omfattet af den regulering, der omtales i de følgende kapitler. Det er uden betydning, om overførslen sker elektronisk, f.eks. via intranet eller Internet, eller den sker på anden måde, f.eks. data placeret på en harddisk i en bærbar computer, der medtages på et fly. Tilsvarende gælder, såfremt en person, der befinder sig i et andet land, logger sig på en database i hjemlandet og herved får adgang til persondata. I et sådant sikkert i praksis ofte forekommende tilfælde er der tale om en overførsel, også selvom personen er dansk, og databasen befinder sig i Danmark. Der foreligger en overførsel i alle tilfælde, hvor en personoplysning gøres til genstand for behandling et sted, hvor eksportlandets ret ikke finder anvendelse. I alle tilfælde er det de samme regler, der skal overholdes, og med en mulig reservation for intranet er det da også vanskeligt at argumentere for, at den anvendte praktiske metode skulle have nogen indflydelse på den retlige regulering.

Det kan dog i denne forbindelse fremhæves, at der kan opstå et selvstændigt sikkerhedsspørgsmål i forhold til metoder, som indebærer en risiko for, at udenforstående kan få adgang til de pågældende persondata. Hensynet til sikkerhed kan begrunde, at der stilles særlige vilkår for, at en bestemt overførsel kan accepteres. Eksempelvis kan der i forhold til overførsler via Internettet være tale om krav om anvendelse af mere eller mindre stærk kryptering, elektronisk signatur, mm. Sådanne krav er praktisk væsentlige, men de angår den måde, hvorpå overførslen tilrettelægges, snarere end grundspørgsmålet, om en overførsel faktisk kan finde sted, jfr. ovenfor under 8. Undertiden indebærer opfyldelsen af sådanne krav, at en overførsel, der ellers ikke vil kunne accepteres, kan finde sted. De medvirker til at skabe den tilstrækkelige tryghed.

Tilrettelæggelsen af overførslen kan have særlig betydning i forhold til opnåelse af tilstrækkelig sikkerhed for, at der ikke overføres flere oplysninger end intenderet. I denne sammenhæng foreligger spørgsmålet, om det er eksportøren eller importøren, der faktisk foretager overførslen. Denne problemstilling har især været aktuel i forhold til overførsel af oplysninger fra luftfartsselskaber til USA, hvor dette i praksis indtil videre sker ved, at oplysningerne indhentes fra USA, frem for at de overføres fra Danmark. Førstnævnte såkaldte pull-metode indebærer en risiko for, at der indhentes overskydende oplysninger, hvilket er mindre sandsynligt, hvis en push-metode bliver benyttet. Denne problemstilling, som sætter fokus på kontrollerbarhed, kan være

Kapitel 1 Overførselsproblemet

aktuel i andre sammenhænge, og i almindelighed skabes den største sikkerhed for, at overførslen ikke omfatter flere data, end det er acceptabelt, ved at eksportøren forestår denne.

12. Eksportøren

På samme måde som overførselsmetoden principielt er uden selvstændig indflydelse på den retlige bedømmelse er det som udgangspunkt uden betydning, hvem der forestår en overførsel. Det er ikke afgørende for reglernes anvendelse, om der er tale om en virksomhed, en forening eller en privatperson. Dette er udgangspunktet, men ved vurderingen af, om overførslen kan finde sted kan det i nogle tilfælde tillægges betydning, hvem der overfører, og ligeledes hvem der skal modtage de overførte oplysninger. I forhold til privatpersoner vil visse overførsler falde uden for loven, jfr. § 2(3) og yderligere nedenfor. Eksportørens identitet kan specielt have en betydning ved en vurdering af sandsynligheden for, at lovgivningens krav, f.eks. i henseende til sikkerhed, vil blive overholdt. Den store virksomhed med ressourcer og et image at pleje vil i sådan sammenhæng kunne fremstå mere tillidsvækkende end andre eksportører. Dette kan blive tillagt vægt i de tilfælde, hvor en overførsel forudsætter en tilladelse.

13. Formål

Medens de implicerede aktørers identitet således alene har betydning ved vurderingen af visse konkrete overførsler, har det generel interesse, hvilket formål en overførsel tilsigter at opfylde. Forinden dette aspekt omtales, skal dog fremhæves, at formålet også konkret har betydning, idet det kan vise om overførslen er sagligt begrundet. Det kan således blive tillagt vægt, om en overførsel er velbegrundet, og eksempelvis om den har et egentligt kommercielt sigte eller er begrundet i forskningsmæssige formål. Som det vil fremgå af senere kapitler, kan formålet tillægges betydning, i det omfang tilsynsmyndigheden, Datatilsynet, skal inddrages ved en bedømmelse af overførselens tilladelighed.

Formålet har særlig betydning, når det skal vurderes, om en overførsel udgør en behandling, der er omfattet af de databeskyttelsesretlige regler. Dette er en første forudsætning for, at de overførselsregler, der er denne bogs genstand, aktualiseres. I forhold til privatpersoner er en overførsel, der udelukkende tager sigte på at varetage et personligt/privat formål, en behandling,

13. Formål

der er undtaget fra reguleringen, jfr. POL § 2(3), og dermed er der ikke tale om en overførsel, som skal opfylde lovgivningens regler. Mailen til familiedlemmer i udlandet med omtale af og billeder fra onkel Jens' 60 års fødselsdag udgør således ikke en overførsel, der skal opfylde bestemte krav. Dette forudsætter dog, at der ikke samtidig varetages andre formål. Der skal være tale om et rent tilfælde.²³

Et andet eksempel herpå er de persondatabehandlinger, der er omfattet af direktivets artikel 9, hvor der gøres undtagelse fra reglerne under hensyntagen til ytringsfriheden, jfr. herved POL § 2(2) samt § 2(6-10). For sådanne behandlinger gælder overførselsreglerne ikke, idet det tilføjes, at dette afhænger af, hvorledes artikel 9 er implementeret i de enkelte medlemsstater. Dette betyder eksempelvis, at et dansk dagblad med støtte i de formål, der begrundes i artikel 9, vil kunne overføre personoplysninger til et dagblad i et hvilket som helst andet land. En sådan overførsel skal således alene være i overensstemmelse med de sikkerhedsregler, som følger af POL §§ 41 og 42. For en god ordens skyld tilføjes, at det falder uden for denne bogs rammer at vurdere betimeligheden af den måde, den databeskyttelsesretlige regulering er afgrænset på. Det bemærkes yderligere, at i forhold til kommercielle dataoverførsler er de her nævnte undtagelser af mindre praktisk interesse, når der herved bortses fra massemedierne.

23. Se i denne sammenhæng Datatilsynets Årsberetning 2000 p.37 vedrørende slægtsforskning. Det lægges her til grund, at overførsel til personer inden for slægten falder uden for loven, og at overførsel til personer uden for slægten kan ske frit, i det omfang der ikke er tale om fortrolige data, eller når oplysningerne stammer fra offentligt tilgængelige kilder.

KAPITEL 2

Dansk ret

1. National rets relevans

Det kan umiddelbart forekomme lidt mærkeligt at starte udredningen af overførselsproblemet med en omtale af national ret. Dette skyldes, at denne ret danner udgangspunktet for såvel problemets opståen som dets løsning. Det er forekomsten af disharmoniske nationale beskyttelsesniveauer, som medfører, at der overhovedet foreligger et overførselsproblem. Var der harmoni, var der intet problem. I hvert fald inden for det område, hvor direktivet finder anvendelse, er det en første forudsætning for, at en overførsel kan finde sted, at de pågældende personoplysninger af eksportøren bliver behandlet i overensstemmelse med eksportlandets databeskyttelsesretlige regler.

Det fremgår af direktivets artikel 25(1), jfr. præambelens betragtning 60, og POL § 27(5), at en overførsel skal være baseret på en nationalt lovlig behandling. Er denne betingelse ikke opfyldt, kan en overførsel ikke finde sted. Disse regler tager sigte på eksport af persondata til et land, der ikke er omfattet af direktivet, jfr. nærmere i kapitel 5, men princippet om lovlig national behandling gælder tillige for overførsler inden for direktivets område, dvs. mellem medlemsstaterne. Forskellen mellem de to situationer er dermed blot, at der i relation til den førstnævnte er fastsat yderligere betingelser, ud over at behandlingen efter de almindelige nationale regler er lovlig, som skal opfyldes, for at en overførsel kan finde sted, jfr. herom under 11. I denne henseende foreligger retspolitisk to spørgsmål. For det første om det overhovedet er ønskeligt at stille sådanne yderligere betingelser, og for det andet hvad disse i givet fald skal gå ud på. Den gældende ordning, der især behandles i kapitel 5, giver et af de mulige svar på disse spørgsmål.

I almindelighed beror betingelsen om, at en overførsel skal være en lovlig behandling, på det simple forhold, at en overførsel er en behandling. Som fremhævet i kapitel 1 omfatter behandlingsbegrebet enhver aktivitet i forbindelse med en personoplysning. Det er en naturlig konsekvens heraf, at en overførsel forudsætter, at de almindelige betingelser for behandling af per-

Kapitel 2 Dansk ret

sonoplysninger er opfyldt. Om det er hensigtsmæssigt at betragte en overførsel som en behandling, drøftes i kapitel 8.

I dette kapitel sættes fokus på grundbetingelsen om, at behandlingen nationalt skal være lovlig, idet der yderligere henvises til kapitel 3, hvori der redegøres for, på hvilken måde denne betingelse har en videregående betydning for en samlet forståelse af overførselsproblemet. Det vil være en bog i sig selv at redegøre for de gældende danske regler, hvorfor det følgende alene har karakter af en fremhævelse af en række hovedtræk idet der i øvrigt henvises til den almindelige databeskyttelsesretlige litteratur.¹

2. Behandlingsformer

Som fremhævet fastsætter hovedparten af bestemmelserne i POL som udgangspunkt de samme regler for en hvilken som helst form for behandling af personoplysninger. Umiddelbart læst har det dermed ikke nogen betydning, på hvilken måde der behandles. Ved den praktiske udfyldning af bestemmelserne tages der dog et vist hensyn hertil, idet der lægges vægt på, i hvilken udstrækning behandlingen udløser en risiko for integritetskrænkelser.² Det er eksempelvis gennemsnitligt mere risikofyldt for de registrerede, at der indsamles oplysninger, end at disse anvendes internt i en virksomhed. Ved vurderingen af en behandlings lovlighed kan der ud over til behandlingsformen tages hensyn til, hvem der er ansvarlig for behandlingen, og hvilket formål denne tilsigter.

Som fremhævet er det en grundbetingelse for en overførsels lovlighed, at den overførende virksomhed lovligt er i besiddelse af oplysningerne, hvilket i det følgende forudsættes at være tilfældet. Ved en mere præcis fastlæggelse af det nationale grundlag for en bedømmelse af overførsels lovlighed har det på denne baggrund interesse at indkredse, hvilke former for behandling der ligeledes kan udgøre en overførsel. Udgangspunktet er, at der ikke kun er tale om en type behandling, som kan indebære en overførsel.

1. Personoplysningsloven er i detaljer kommenteret i Kristian Korfits Nielsen, Henrik Waaben: *Lov om behandling af personoplysninger* (København 2001). Om loven kan endvidere henvises til Peter Blume: *Personoplysningsloven* (København 2000) og *Behandling af persondata* (København 2003). De grundlæggende hensyn og vurderinger, der har betydning på dette retsområde, er behandlet i Peter Blume: *Databeskyttelsesret* (2.udg. København 2003).
2. Se nærmere om behandlingsbegrebets forskellige facetter Peter Blume, *Ugeskrift for Retsvæsen* 2000 p.425-30.

2. Behandlingsformer

For en umiddelbar betragtning er det naturligt at antage, at en overførsel sædvanligvis er udtryk for en videregivelse. Herved forstås den situation, at persondata flyttes fra en dataansvarlig til en anden, der herefter som dataansvarlig skal beskytte oplysningerne i overensstemmelse med lovens krav. Videregivelse betragtes normalt som en af de mere integritetsrisikable former for behandling, og danner dermed grundlag for en forholdsvis streng udfyldning af lovens bestemmelser. Der er ikke nogen tvivl om, at mange overførsler har denne karakter, og at det ved bedømmelsen af om national behandling lovligt kan ske, forudsættes, at videregivelsen klart er velbegrundet.

Det er på denne baggrund hensigtsmæssigt nærmere at indkredse, hvad der skal forstås ved en videregivelse. For en sådan er det som nævnt karakteristisk, at personoplysninger er blevet flyttet til en anden, som har en selvstændig retlig eksistens. En virksomhed giver oplysninger til en anden virksomhed. Dette er ikke nødvendigvis ensbetydende med, at den oprindelige databesidder ikke længere råder over oplysningerne, idet information jo er karakteriseret ved at kunne være flere steder på en gang. Det er således ikke nogen betingelse for, at der foreligger en videregivelse, at den videregivende ikke også fortsat kan anvende de pågældende data. To eller flere dataansvarlige kan hver for sig råde over de samme data, idet det afgørende er, at den, der har modtaget oplysningerne, har en egen selvstændig rådighedsbeføjelse. Ved bedømmelsen, af hvilke integritetsrisici der kan være forbundet med en konkret overførsel, udgør dette træk ved information en komplikation i forhold til mulighederne for at udøve kontrol. Persondata er ikke noget håndgribeligt, hvis bevægelser let kan følges. Der kan således i mange tilfælde ske en uønskelig og uoverskuelig spredning af persondata, men i denne henseende adskiller overførsler sig ikke fra videregivelser på nationalt niveau.

I praksis har det netop særlig betydning, at der foreligger en videregivelse, såfremt den modtagende er en selvstændig retlig enhed. Konsekvensen heraf er, at flytning af persondata mellem selskaber, der er forbundne i en koncern, har karakter af en videregivelse i dansk ret. Den omstændighed, at der foreligger en koncern, medfører langt overvejende ikke nogen mildere vurdering af, om videregivelsesbetingelserne er opfyldt, men kan dog i andre henseender tillægges en vis betydning, idet dette eksempelvis gælder i forhold til sikkerhedskrav. Det er omdiskuteret, om det er rimeligt at betragte koncerner på denne måde,³ idet en valgt selskabsform dermed bliver tillagt en databeskyttelsesmæssig betydning. Dette er dog med visse variationer opfattelsen i

3. Se om problemstillingen Peter Blume, Ugeskrift for Retsvæsen 1993 p.392-98.

alle EU's medlemsstater.⁴ Da mange overførsler netop finder sted i koncernforhold, er det væsentligt at være opmærksom på dette forhold. Det bør tilføjes, at ved overførsler har den valgte selskabsform noget mindre betydning, fordi det ikke alene er videregivelse, der kan udgøre en overførsel, jfr. straks nedenfor. Ved udformningen af de retlige konstruktioner, der kan danne rammen omkring overførsler, har selskabsformen dog en vis betydning, jfr. i kapitel 6.

Det er ikke alle overførsler, som kan sammenlignes med en videregivelse. En række overførsler har karakter af en intern behandling. En virksomhed flytter persondata fra en af sine afdelinger til en anden afdeling. En ny dataansvarlig er ikke trådt ind på banen. En overførsel forudsætter således ikke at oplysninger er overdraget til en anden dataansvarlig.⁵ Intern behandling betragtes sædvanligvis som mindre risikabel for den registrerede eftersom der ikke sker nogen egentlig spredning af personoplysningerne.⁶ Disse bliver vel nok gjort tilgængelige for flere, men de forbliver dog inden for den samme enhed, hvorfor risikoen for misbrug er begrænset. Vurderingen af, om behandlingsbetingelserne er opfyldt, er dermed som udgangspunkt mere lempelig, idet dette dog er mere udtalt nationalt, end når der er tale om en overførsel.

Der kan endelig være tale om, at der sker en overladelse, hvorved forstås at data flyttes til nogen, som udfører en opgave på vegne af den dataansvarlige. I forhold til overførsler vil der typisk være tale om, at personoplysningerne bliver edb-behandlet af en anden instans end virksomheden, jfr. yderligere hertil i kapitel 6. Med lovens terminologi bliver oplysningerne overladt til en databehandler. En sådan behandling karakteriseres ved, at det fortsat er den dataansvarlige, der har forpligtelsen til at overholde lovens regler og dermed har pligt til at sikre sig, at databehandleren ikke misbruger de overladte data. Det er forudsat, at der skal foreligge et kontraktforhold mellem dataansvarlig og databehandler, jfr. § 42(2). Overladelse betragtes i almindelighed som ikke særlig risikabel nationalt med den konsekvens, at behandlingsreglerne tolkes lempeligt, men når der er tale om en overførsel, kan der blive stillet særlige krav, jfr. herved især i kapitel 6.

4. Eksempelvis er det ikke ifølge italiensk ret en videregivelse at overføre data mellem selskaber inden for en koncern.

5. Jfr. Betænkning 1345/1997 p.283-84.

6. Såvel i loven som i direktivet betegnes en person som den registrerede. Dette skyldes sprogfattigdom, idet denne terminologi er misvisende i den forstand, at reguleringen som nævnt tager sigte på meget mere end registrering. I engelsk ret anvendes mere dækkende terminologien data subject.

3. Den dataansvarlige

Dette er de tre hovedformer for national behandling, som korresponderer med en overførsel, idet det for en god ordens skyld anmærkes, at videregivelse også omfatter den situation, hvor der sker offentliggørelse, som kan kategoriseres som en kvalificeret form for videregivelse. Det skal endvidere præciseres, at det ikke herved er udelukket, at andre former for behandling kan udgøre en overførsel. Dette vil dog være atypisk, og der kendes vist nok ikke eksempler herpå i praksis.

3. Den dataansvarlige

Forinden der tages stilling til, om der en overførsel kan finde sted, må det som nævnt vurderes, om de pågældende oplysninger behandles lovligt nationalt. Vurderingen heraf omfatter en række delspørgsmål, der alle vedrører, om den dataansvarlige opfylder de forpligtelser, som følger af loven. På dette sted er det derfor nødvendigt at fastlægge, hvem der er den dataansvarlige, jfr. POL § 3 nr.4. Dette er den person eller virksomhed, der har rådighed over personoplysninger, og i hvis interesse behandlingen sædvanligvis finder sted. Afgørende er således ikke, hvor oplysninger faktisk befinder sig, og af hvem de behandles, men for hvem de bliver behandlet. Det er sædvanligvis ikke vanskeligt at fastslå, hvem der er dataansvarlig.⁷ I det følgende lægges det til grund, at den, som vil foretage en overførsel, er den dataansvarlige.

På samme måde som direktivet omfatter POL en række forskellige emner, der normerer den dataansvarliges forpligtelser. Loven angiver en række generelle principper (§ 5), der skal respekteres i forhold til enhver form for behandling af alle typer personoplysninger. Herefter er der fastlagt forskellige behandlingsbetingelser, som er differentierede efter personoplysningens sensitivitetsgrad (især §§ 6-8 og 11). I det konkrete tilfælde skal en af disse betingelser være opfyldt således, at denne udgør hjemlen for behandlingen. Herudover er der tillagt den registrerede en række rettigheder (§§ 28-40), som den dataansvarlige er forpligtet til at sikre bliver opfyldt. Ved siden af disse bestemmelser er der fastsat regler om anmeldelse/tilladelse samt tilsyn, der har til formål at styrke sandsynligheden for, at loven faktisk bliver overholdt. I relation til de sidstnævnte regler medtages i dette kapitel alene en introducere-

7. Undertiden forekommer i praksis selskabskonstruktioner eller selskabsrelationer, der giver anledning til en vis usikkerhed med henblik på, hvem der i det konkrete tilfælde er dataansvarlig, men det er ikke nødvendigt at lade denne problematik belaste denne bog.

rende beskrivelse af Datatilsynet, idet denne mere bureaukratiske del af loven bedre inddrages i de følgende kapitler, når dette er relevant.

4. Principper

Som nævnt fastlægger § 5 almindelige principper for behandlingen af persondata. Denne bestemmelse, der modsvares af direktivets artikel 6, kan karakteriseres som reguleringens »grundlov«. De fastsatte principper har ikke blot betydning ved en vurdering af, om en behandling nationalt er lovlig, men spiller tillige en rolle ved bedømmelsen af, om en overførsel i øvrigt kan finde sted. Deres opfyldelse skal således vurderes selvstændigt i forhold til overførslen. De er så at sige på spil to gange i denne særlige sammenhæng. Selvom det nok vil være forholdsvist sjældent, kan det forekomme, at et af de i det følgende omtalte principper vil være opfyldt i forhold til en national behandling, men derimod ikke ved en overførsel af de samme oplysninger. Dette skyldes, at principperne skal vurderes selvstændigt i relation til hver enkelt behandlingsform.

§ 5(1) fastslår først, at personoplysninger skal behandles i overensstemmelse med god databehandlingsskik. Dette er en åbent formuleret general-klausul, der tager sigte på at muliggøre en generel bedømmelse baseret på hensynet til integritetsbeskyttelse af om en behandling bør finde sted. I praksis kan bestemmelsen benyttes af Datatilsynet til at stoppe eller begrænse en behandling, der ganske vist ikke er i uoverensstemmelse med lovens regler, men derimod ikke er overensstemmende med lovens ånd. I praksis benyttes reglen sædvanligvis ikke primært til at udelukke en behandling, men derimod til at stille betingelser, herunder, når dette er muligt, egentlige vilkår for en accept af den pågældende behandling. Den anvendes netop til at fremme en god skik. Set under den dataansvarliges perspektiv medfører en bestemmelse af denne karakter en vis usikkerhed og begrænser retsanvendelsens forudberegnelighed,⁸ men når det tages i betragtning, hvor forskelligartede persondata-behandlinger loven omfatter, må det lægges til grund, at en sådan general-klausul er nødvendig. Her i landet er den hidtil blevet benyttet på en forholdsvis forsigtig og afbalanceret måde.

8. En sådan kritik kan ligeledes rettes mod en række af lovens øvrige regler, der enten har karakter af retlige standarder eller anvender ganske vage udtryk. Denne reguleringsform medfører endvidere vanskeligheder, når databeskyttelsesniveauet i forskellige lande skal sammenlignes. Den skaber ligeledes problemer i forhold til en aspiration om at harmonisere nationale lovgivninger, jfr. i kapitel 4.

Dernæst indeholder § 5(2) et almindeligt saglighedskrav. Behandling af persondata skal være baseret på et sagligt formål. Ved udfyldningen af denne retlige standard vil der eksempelvis blive lagt vægt på, hvilket forretningsområde en virksomhed har. Kravet om saglighed indebærer således, at der må være en vis harmoni mellem virksomhedens formål og behandlingens formål. Det skal i forhold til virksomhedens aktivitetsområde være naturligt, at den pågældende behandling finder sted. Dette gælder tilsvarende, når overførselens formål vurderes. Saglighedskravet udgør på samme måde som generalklausulen en reservation, der giver tilsynsmyndigheden et vist spillerum. Medmindre der foreligger en åbenbar situation danner den i praksis et udgangspunkt for en dialog, hvori en virksomhed må sandsynliggøre, at den pågældende overførsel er saglig velbegrundet.

Forudsætningen om, at behandlingen skal være saglig, gælder i almindelighed, men har en særegen betydning i relation til indsamling af oplysninger. § 5(2) fastslår således endvidere, at oplysninger skal indsamles til et bestemt formål, og at de senere alene må anvendes med henblik på formål, der ikke er uforenelige med indsamlingsformålet. Dette skal have en vis præcision, om end kravene hertil ikke er store i praksis. Med dette såkaldte finalité-princip sker der således en begrænsning af den dataansvarliges manøvremargin. Det er forudsat, at der ved angivelsen af formålet ved indsamlingen er sket en vis afgrænsning af de senere former for dataanvendelse. Rammerne for denne afgrænsning er ganske bred, idet det ikke kræves, at et nyt formål skal være foreneligt med det oprindelige, idet det blot ikke må være uforeneligt med dette. Vurderingen af, om dette er tilfældet, sker konkret, men under alle omstændigheder er der tale om et bånd på den dataansvarlige, der også gælder for dem, der lovligt nationalt har modtaget videregivne oplysninger. Aspirationen er, at dataanvendelsen skal være gennemskuelig eller transparent for den registrerede, som i princippet skal kunne forudse, hvad indsamlede oplysninger kan blive anvendt til.

Der er ingen tvivl om, at dette formålsbestemthedsprincip har stor betydning nationalt, hvorimod det kan overvejes, i hvilken udstrækning det spiller nogen selvstændig rolle i forhold til vurderingen af, om en dataoverførsel kan finde sted. Spørgsmålet er dermed, om indsamlingsformålet kan indebære en afskæring af, at oplysningerne senere overføres, og således om denne mulighed skal være medtænkt allerede ved indsamlingen. Dette spørgsmål ses ikke at være fuldt ud afklaret i praksis, men i almindelighed kan dette ikke antages at være tilfældet. Det er ikke et krav, at det af formålet skal fremgå, hvilke former for behandling, der efterfølgende vil blive benyttet, og medmindre formålet på indsamlingstidspunktet er at foretage en overførsel, behøver dette ikke at fremgå. En mulig undtagelse herfra er den situation, at er den dataan-

svarlige bekendt med, at overførsel er en mulighed, kan det følge af princippet om god skik, at de registrerede skal gøres opmærksom herpå.⁹ Dette skyldes, at en sådan information må antages at have betydning for den registreredes beslutning om, hvorvidt der skal gives oplysninger. På denne baggrund kan det lægges til grund, at skal oplysninger overføres med henblik på et formål, der ikke er uforeneligt med det oprindelige, udgør princippet ikke nogen barriere for overførslen. Det er kun en barriere, når indsamlingsformålet i sig selv ikke kan begrunde en overførsel. Om princippet har betydning for dataimportøren, forbliver her en anden historie, som fortælles senere i denne bog.

§ 5(3) fastslår endvidere, at behandlingen skal være proportional i forhold til formålet, og at der ikke må behandles flere oplysninger, end det er nødvendigt for at opfylde det pågældende formål. Sidstnævnte indebærer bl.a. et forbud imod anvendelse af såkaldt overskudsinformation. Disse to principper tager først og fremmest sigte på at skabe disciplin hos den dataansvarlige, der ikke må lade sig friste til at bruge oplysninger ud over, hvad formålet tilsiger, eller til at opbevare tidligere indsamlede oplysninger, blot fordi de måske engang i fremtiden kan være anvendelige (»just in case«). Disse principper indebærer, at der ikke må overføres flere oplysninger end nødvendigt i forhold til det formål, der begrunder overførslen. Det bør forebygges, at der opstår en situation, hvor importøren kan foretage en ubegrundet dataophobning.

Princippet om datakvalitet fremhæves i § 5(4). En dataansvarlig er forpligtet til at sikre, at der ikke behandles ukorrekte eller vildledende oplysninger. Mange anser dette princip som et af de væsentligste i databeskyttelsesretten. Det kan umiddelbart forekomme selvfølgeligt, men pålægger ofte den dataansvarlige en krævende opgave, hvilket specielt er tilfældet, når oplysningerne ikke er blevet indsamlet direkte, men eksempelvis er videregivet af en anden virksomhed eller blevet indhentet fra et offentligt register. Her kan det tit være svært at vurdere oplysningernes kvalitet i forhold til den modtagende virksomheds dataanvendelse. Kravet om god datakvalitet indebærer dermed en særlig udfordring i relation til overførte data, dvs. i de tilfælde, hvor der sker import til en dansk virksomhed, idet de nærmere omstændigheder omkring oplysningernes oprindelige indsamling kan være ukendte for importøren. Det forekommer i sandsynligt, at der ganske ofte i denne situation vil

9. Herved refereres til bestemmelserne om oplysningspligt i §§ 28 og 29, der omtales i kapitel 4. Det er disse bestemmelser, der medfører at formålet skal formuleres, idet dette ikke er en direkte følge af § 5(2).

kunne foreligge kvalitetsproblemer, som også tilsynsmyndigheden vil have vanskeligt ved at tage stilling til. Der stilles krav til importøren om særlig påpasselighed i forhold til importerede data, hvorimod det i praksis vil være sjældent, at princippet stiller sig hindrende i vejen for dataeksport. Det kan dog være medvirkende hertil i situationer, hvor andre momenter skaber tvivl om, hvorvidt en overførsel bør finde sted, eller der foreligger en nærliggende risiko for, at importøren vil anvende oplysningerne på en vildledende måde. Under alle omstændigheder må hensynet til god datakvalitet inddrages ved tilrettelæggelsen af den konkrete overførsel, idet dette eksempelvis kan være aktuelt i situationer, hvor det er forudsat, at de overførte personoplysninger løbende skal ajourføres.

Endelig fastslår § 5(5) et princip om tidsbegrænsning, hvorefter personoplysninger ikke må opbevares længere end nødvendigt i forhold til indsamlingsformålet eller et efterfølgende ikke uforeneligt formål. Nationalt er dette et væsentligt princip, der er vendt imod dataophobning, som i sig selv betragtes som integritetstruende. I relation til dataoverførsler kan det ikke antages, at tidsbegrænsningsprincippet sædvanligvis spiller nogen selvstændig rolle for eksportøren, men kan dog udgøre grundlaget for, at der fastsættes vilkår i henseende til importørens behandling af de overførte data.¹⁰

5. Sikkerhed

Et yderligere tværgående princip fastslår, at den dataansvarlige skal sørge for at der er sikkerhed omkring persondatabehandlingen, jfr. §§ 41 og 42, der svarer til direktivets artikler 16 og 17. Tre former for sikkerhed skal være opfyldt. Personoplysningerne skal for det første være sikret fysisk, f.eks. mod brand og tyveri. Der skal for det andet være systemmæssig sikkerhed, eksempelvis firewalls, der kan forebygge hacking. De systemmæssige krav varierer på samme måde som de øvrige, afhængig af hvor følsomme data behandlingen angår. Dette viser sig bl.a. i forhold til transmission, hvor der ved følsomme data i dansk ret stilles krav om, at der skal anvendes stærk kryptering baseret på en anerkendt algoritme. Krav af denne karakter har betydning for, hvorledes overførslen gennemføres. For det tredje skal der være organisatorisk sikkerhed, idet det skal sikres, at de personer, der har adgang til person-

10. Jfr. dog Datatilsynets afgørelse af 19.5.2004 om den amerikanske Sarbanes Oxley Act, hvor overførsler foranlediget af de krav denne lov indebærer for revisorer, antoges ikke blot at stride mod § 5(1-3), men ligeledes at være problematisk i forhold til § 5(4-5).

data ikke misbruger disse. Et eksempel kan være et krav om at der skal ske logning af dataanvendelsen. I praksis er det ofte denne form for sikkerhed, den menneskelige faktor, som udgør det svage led i kæden, og hvor det kan forudsættes, at den dataansvarlige instruerer og løbende uddanner sine ansatte. I hvilken udstrækning der i en virksomhed er opbygget en sikkerhedsorganisation, som varetager denne uddannelsesfunktion, har i de tilfælde, hvor en tilladelse er påkrævet, betydning for vurderingen af, om konkrete overførsler kan finde sted. Sammenfattende er kravet til den dataansvarlige, at kun autoriserede personer behandler oplysninger udelukkende til autoriserede formål.

Sikkerhedskravene har en ofte ganske teknisk og ligeledes omfattende karakter, hvorfor de ikke egner sig til medtagelse i en lovtekst, hvilket også skyldes at de løbende må opdateres som følge af den teknologiske udvikling.¹¹ I forhold til den private sektor er der ikke fastsat uddybende regler, men det antages sædvanligvis, at de regler, som gælder for den offentlige forvaltning, Bekendtgørelse nr.528 af 15.6.2000 med senere ændringer samt Vejledning nr.37 af 2.4.2001, i det store hele også skal opfyldes i den private sektor.

Som udgangspunkt er der ikke forskel på de sikkerhedskrav, der stilles nationalt og ved overførsler. Disse krav har stor praktisk betydning, idet de er rettet dels mod selve overførslen dels, når dette er muligt, mod importøren, der sædvanligvis bør forudsættes at have et sikkerhedsniveau, som svarer til det, der gælder i eksportlandet, in casu Danmark. Denne forudsætning har primært betydning i de tilfælde, hvor overførslen forudsætter en tilladelse fra Datatilsynet. I denne forbindelse er det værd at fremhæve, at det styrende for disse krav er karakteren af de behandlede data, idet en dataansvarlig ikke kan anvende et lavere sikkerhedsniveau, blot fordi vedkommende eksempelvis ikke har den tilstrækkelige edb kapacitet. Dette udgangspunkt har i praksis betydning for vurderingen af, om det er tilrådeligt, at oplysninger kan overføres til en bestemt importør, jfr. yderligere i kapitel 5 og især 6. Sikkerhed medfører omkostninger, og det er derfor ikke altid, at der stilles krav om state of the art sikkerhed, men i forhold til dataoverførsler må hensynet til den dataansvarliges økonomi antages at spille en mindre rolle som følge af den usikkerhed, som mange overførsler i sig selv indebærer.

Som fremhævet ovenfor har principperne i § 5 og sikkerhedsreglerne betydning for såvel import som eksport af persondata. De samme krav skal som

11. Den omstændighed, at de specifikke sikkerhedskrav ikke kan læses ud af direktivet eller loven, giver undertiden anledning til kritik af at reguleringen har en for lav retlig kvalitet. Det er dog næppe muligt at undgå anvendelsen af retlige standarder, der må udfyldes via andre retskilder.

udgangspunkt opfyldes. Dette gælder for så vidt også for de øvrige regler, som omtales i det følgende, men deres betydning er dog først og fremmest relateret til eksport af data.

6. Hjemmel

En forudsætning for, at persondata kan behandles, er, at der er en hjemmel hertil. Dette er på ingen måde nogen selvfølgelighed i den private sektor, hvor det traditionelle retlige udgangspunkt er, at enhver adfærd kan foretages medmindre den retligt er forbudt. I vestlige samfund er udgangspunktet således retlig frihed, idet det dog har været et karakteristisk udviklingstræk i moderne tid, at området for denne frihed er blevet stadig mere begrænset. Dette er også tilfældet på dette område, hvor der altså gælder et almindeligt hjemmelsprincip, der svarer til det, som kendes i den offentlige ret. I de fleste tilfælde skal denne hjemmel søges i POL §§ 6-8¹², som angiver forskellige former for betingelser afhængig af, hvilken oplysningstype der er tale om, jfr. hertil i kapitel 1. Jo mere sensitiv oplysningen er, desto strengere betingelser skal være opfyldt. Det har derfor betydning, hvilke oplysningstyper som i det konkrete tilfælde er omfattet af overførselssituationen. I overensstemmelse med det ovenfor angivne skal der her kun knyttes enkelte kommentarer til visse af disse behandlingsbetingelser, idet der i øvrigt henvises til kapitel 5.

7. Samtykke

Fælles er, at oplysninger kan behandles, såfremt den registrerede giver et samtykke, idet det er forudsat, at det skal være klart, at en sådan viljeserklæring foreligger. Samtykke er blot en af flere mulige hjemler til at behandle oplysninger, jfr. under 8 og 9. Der er således ikke tale om en hovedregel, om end det i forhold til følsomme persondata (§§ 7-8) ud fra et menneskeretligt orienteret synspunkt kan være ønskeligt, at den dataansvarlige først søger at opnå et samtykke.

Et gyldigt samtykke skal være informeret, specifikt og frivilligt (§ 3 nr.8) samt være udtrykkeligt. Samtykket kan således ikke gives indirekte eller

12. For personnumre er der fastsat en særlig regel i § 11. Direktivets artikel 8(7) overlader det til medlemsstaterne at fastsætte regler herom, hvilket skyldes, at et generelt dækkende identifikationssystem ikke findes i alle landene.

Kapitel 2 Dansk ret

stiltiende. Der er yderligere grund til at fremhæve, at samtykket til enhver tid kan tilbagekaldes (§ 38), hvilket udgør et usikkerhedsmoment for den dataansvarlige. Der kan selvstændigt samtykkes til overførsel til tredjelande, jfr. nærmere i kapitel 5, hvor de særlige spørgsmål, dette aktualiserer, drøftes. I denne situation kan der foreligge to samtykker i de tilfælde, hvor et sådant indhentes, efter at den nationale behandling er blevet iværksat.

Under forudsætning af, at der ikke foreligger en modstrid med § 5 (saglighed), kan samtykke altid udgøre hjemlen, hvilket kan opfattes som en anerkendelse af de registreredes informatoriske selvbestemmelsesret.¹³ Medmindre den dataansvarlige på anden måde har løbende kontakt til de registrerede, er samtykkemuligheden dog besværlig, og i mange tilfælde vil den ligeledes være ressourcekrævende. Indhentelse af samtykke er dermed ikke altid særlig praktisk.

8. Almindelige oplysninger

Mange dataansvarlige vil på denne baggrund foretrække en anden hjemmel end samtykke, såfremt muligheden herfor foreligger. Dette er mest sandsynligt i henseende til almindelige persondata (§ 6(1), artikel 7), idet der især foreligger to mulige hjemler.¹⁴ For det første kan behandling ske, når dette er nødvendigt som led i et kontraktforhold mellem den dataansvarlige og den registrerede (nr.2), hvilket bl.a. indebærer mulighed for at behandle oplysninger om ansatte, om end det må pointeres, at det skal være klart, at behandlingen er nødvendig, idet det ikke er tilstrækkeligt, at den blot er hensigtsmæssig. Et yderligere eksempel er behandling af oplysninger i relation til brug af betalingskort, eksempelvis spærrelister, hvor der i overførselssituationen vil kunne fastsættes vilkår, der via den danske kortudsteder binder importøren. For det andet kan behandling ske, når den er nødvendig af hensyn til den dataansvarliges eller en tredjemands interesse, og denne interesse er mere tungtvejende end den registreredes modgående interesse (nr.7). Der skal foreligge et såkaldt værdispring, men kravene hertil er ikke store, hvorfor det i praksis sædvanligvis antages, at dette er tilfældet. Persondatabehandling i den

13. Det kan anmærkes, at samtykke ikke entydigt er en fordel for alle registrerede, idet det forudsætter at situationen kan overskues. For svage borgere kan samtykke dermed være noget af et tveægget sværd.

14. Ud over de i teksten nævnte muligheder kan behandling været begrundet i, at den er nødvendig som følge af en retlig forpligtelse, eller den angår den registreredes vitale interesser, jfr. § 6(1 nr.3 og 4).

private sektor er i vidt omfang baseret på denne bestemmelse, men det kan bemærkes, at et sådant værdispring ikke kan begrunde en overførsel til tredje-lande, jfr. i kapitel 5.

I det hele taget er det generelle udgangspunkt, at der ikke skal være større begrænsninger i forhold til almindelige persondata, idet sædvanlig erhvervs-udøvelse skal kunne finde sted. Selvom der i § 6(1 nr. 2-7) stilles krav om, at behandlingen skal være nødvendig, bliver denne betingelse sædvanligvis ikke i forhold til den nationale persondatabehandling fortolket restriktivt i praksis. Behandlingen skal blot være velbegrundet. Generelt foreligger der således sjældent egentlige problemer i forhold til behandling af almindelige data, der ikke anses for særligt integritetsrisikable.

Bedømmelsen af, hvorvidt betingelserne er opfyldt, skærpes dog, såfremt det af anden lovgivning fremgår at oplysningerne er underlagt tavshedspligt og dermed er fortrolige.¹⁵ Det er mest udtalt i den offentlige sektor, at oplysninger anses for fortrolige, men i den private sektor kan dette være fastsat i sektorlovgivning. Et eksempel herpå er behandling af oplysninger inden for den finansielle sektor. Særlige anvendelsesformål kan ligeledes begrunde en anderledes vurdering, jfr. nedenfor i relation til markedsføring.

9. Følsomme oplysninger

Ved behandling af de følsomme oplysningstyper (§§ 7 og 8)¹⁶ er det derimod ofte vanskeligt at finde en hjemmel, når der ikke foreligger et samtykke, jfr. yderligere i kapitel 5. De i loven angivne muligheder er snævre, og det almindelige udgangspunkt er, at der, medmindre særlige forhold foreligger, ikke uden samtykke bør behandles følsomme oplysninger i den private sek-

15. Det fremgår ikke direkte af loven, at der er to hovedtyper af almindelige oplysninger, idet dette følger af Datatilsynets praksis. Denne beror på, at § 6(1) omfatter et særdeles stort antal oplysningstyper, og det derfor er ønskeligt at tage hensyn til, hvor integritetsrisikable disse i almindelighed må antages at være. Ved vurderingen heraf er det naturligt at tage udgangspunkt i, hvorledes de enkelte oplysninger vurderes i anden lovgivning, der dermed anvendes til at udfylde personoplysningslovens meget brede kategorier.

16. § 7 svarer til direktivets artikel 8, medens § 8 er en særegen dansk opfindelse, der har til formål at sikre, at oplysninger, som efter den ældre registerlovgivning blev betragtet som følsomme, fortsat kun kan behandles såfremt strengere betingelser end dem, der er angivet i § 6, bliver opfyldt. Selvom § 8 formelt er en del af implementeringen af artikel 7 om almindelige oplysninger, har de omfattede oplysninger således en særlig status og kan karakteriseres som semifølsomme.

tor. Dette udgangspunkt har ikke blot betydning nationalt, men har ligeledes konsekvenser for mulighederne for, at overføre sådanne data, idet der skal foreligge en særlig sikkerhed for at overførslen ikke udløser en integritetskrænkelserisiko, jfr. yderligere herom nedenfor og især i senere kapitler.

Hovedparten af de oplysninger, som er kategoriseret som følsomme, giver ikke anledning til forundring, eftersom der foreligger en udbredt konsensus om, at denne karakteristik er velbegrundet. Der kan dog være særlig grund til at anmærke, at oplysninger om fagforeningsmæssigt tilhørsforhold betragtes som en følsom oplysning (§ 7(1)). Dette kan umiddelbart forekomme lidt overraskende og mærkeligt her i landet, men beror på traditioner i andre EU-lande, hvor der i større udstrækning findes konkurrerende fagforeninger, som afspejler forskellige samfundsmæssige eller politiske opfattelser. Denne kategorisering betyder, at der stilles krav om et særligt opmærksomhedsniveau ved behandling af oplysninger om ansatte, idet muligheden for at lade denne behandling hvile på arbejdsaftalen er begrænsede, såfremt behandlingen omfatter medlemsoplysninger, jfr. yderligere i kapitel 5.¹⁷

10. Markedsføring

Ved vurderingen af, om der er hjemmel til behandling, spiller behandlingens formål hovedsageligt ikke nogen fremtrædende rolle. Dette har dog betydning i et praktisk vigtigt tilfælde, der angår behandling af personoplysninger med henblik på markedsføring. Dette kan bl.a. være relevant i forhold til kundedata. Personopplysningsloven indeholder ikke specielle bestemmelser om registrering med henblik på dette formål, men derimod (§ 6(2-4) og § 36) regler, der vedrører, under hvilke betingelser oplysninger kan videregives med henblik herpå.¹⁸ Tager en overførsel henblik på, at importøren skal kunne foretage markedsføring, må det antages, at disse regler skal være opfyldt. Dette er vel ikke ganske åbenbart, eftersom reglerne angår den nationale behandling og principielt ikke vedrører importørens behandling. Den omstændighed, at bestemmelserne specifikt angår videregivelse, taler dog med

17. Der er en udtalt tendens til at være skeptisk over for at lade behandling af ansatte bero på et samtykke. Dette skal være frivilligt, og selvom kravene hertil ikke i almindelighed er store, er det ulige forhold mellem arbejdsgiver og ansat medvirkende til at stille spørgsmålstegn ved det betryggende i at lade behandlingen bero på et samtykke.

18. Disse bestemmelser udgør en særegen dansk regulering, der så vides ikke korresponderer med tilsvarende regler i andre medlemsstater.

Se nærmere om reguleringen, Peter Blume: Databeskyttelsesret p.183-95.

11. Samme betingelser?

betydelig styrke for, at de skal opfyldes af eksportøren i forbindelse med en overførsel, og at denne bør sikre, at importøren, i hvert fald når denne befinder sig uden for EU, også overholder disse bestemmelser. Det kan herved tillægges betydning, at netop beskyttelse i forhold til anvendelse af personoplysninger til markedsføringsformål er tillagt stor vægt i databeskyttelsesretten.

Kort angivet indebærer disse regler, at oplysninger om specifikt foretagne køb etc. samt følsomme oplysninger kun kan videregives med samtykke fra den registrerede (forbrugeren), medens generelle kundeoplysninger kan videregives uden samtykke, men først efter at forbrugeren har haft lejlighed til at udøve en særlig i loven beskrevet indsigelsesret (§ 36), der er ganske krævende for den dataansvarlige. Samlet er der tale om en ganske intensiv regulering. I denne henseende forudsættes der således et særligt opmærksomhedsniveau hos den dataansvarlige.¹⁹

11. Samme betingelser?

En række af de bestemmelser, der er fastsat i § 27(3) vedrørende dataoverførsler uden for EU, angiver en betingelse, der modsvarer en behandlingshjemmel i den nationale kontekst. Et eksempel herpå er, at oplysninger kan overføres i forbindelse med retskrav, på samme måde som de kan behandles nationalt på dette grundlag (§ 7(2) nr.4, jfr. § 6(1) nr.3)). I sådanne tilfælde opstår spørgsmålet, om disse betingelser, der specifikt vedrører overførsel og som er ens for alle oplysningstyper, skal forstås på samme måde som i den nationale kontekst. Dette spørgsmål er næppe fuldt ud afklaret i praksis og kan give anledning til nogen tvivl, jfr. herved i kapitel 5, hvor spørgsmålet om, hvad der nærmere skal forstås ved et retskrav, drøftes nærmere.

For en umiddelbar betragtning er det ikke givet, at den samme behandlingsbetingelse skal anvendes ens nationalt og i overførselssituationen. Overførsel af oplysninger er noget særegent og etablerer en speciel ramme, der kan indebære, at de enkelte betingelser skal udfyldes på en anden måde end i den nationale kontekst. Denne udfyldning kan indebære en mere restriktiv

19. De nævnte bestemmelser omfatter også den situation, hvor en virksomhed markedsfører på vegne af en anden virksomhed. Her sker der således ikke nogen videregivelse, og sker denne markedsføring på vegne af en udenlandsk virksomhed, foreligger der dermed ikke nogen overførsel. I denne situation skal særlige betingelser ud over de her angivne ikke opfyldes, om end den registrerede bør oplyses om, at den pågældende virksomhed befinder sig i udlandet.

Kapitel 2 Dansk ret

fortolkning med henblik på at skabe garantier for de registrerede, der er specielt udsatte i overførselssituationen. Der kan spores en tendens hertil, hvorved det betones, at det bør tages alvorligt, at en dataoverførsel er noget særligt, og at der ved vurderingen det retlige grundlag må tages højde herfor. For en fortsættelse af denne overvejelse henvises som nævnt især til kapitel 5.

12. Rettigheder

Lovmedholdelig behandling af personoplysninger forudsætter endvidere nationalt, at den registrerede gives de rettigheder, der er fastslået i lovens §§ 28-40. I forhold til en vurdering af, om de nationale forudsætninger for en overførsel er til stede, er det ikke påkrævet at gå nærmere ind i dette rettighedskatalog, idet dette sædvanligvis aktualiseres på stadier, som ligger før overførslen og dermed normalt ikke direkte indgår ved en vurdering af, hvorvidt overførslen kan finde sted, rettighederne i nogle situationer er inkluderet i de krav, der er medtaget i de særlige overførselsgrundlag, der behandles i kapitel 6. Rettighederne kan endvidere have en vis betydning ved en bedømmelse af den fremgangsmåde, der skal følges i forbindelse med selve overførslen, idet der herom henvises til omtalen i kapitel 4.

13. Tilsyn

Lovens kontrol- og tilsynsordning inddrages bedst i de kommende kapitler, men her er det dog naturligt at omtale Datatilsynet, som er den centrale myndighed såvel nationalt som i henseende til overførsler. Det er et væsentligt element i europæisk databeskyttelsesret, at der skal være en uafhængig myndighed, som varetager tilsyn med og kontrol af, at de fastsatte regler bliver overholdt. Domstolene kan også benyttes, men det er lagt til grund, at det ikke er tilstrækkeligt for sikringen af databeskyttelsen alene at have denne mulighed. Der findes datatilsyn i alle de lande, som er omfattet af direktivet, men de ikke organiseret på samme måde, ligesom deres kompetencer varierer i et vist omfang. Nogle af disse forskelle inddrages i senere kapitler. Omtalen nedenfor tager sigte på det danske tilsyn. Uden for direktivets område er det derimod ikke givet, at der findes tilsyn i importlandet. Dette er tilfældet i en række lande, men i størstedelen af verden findes der ikke myndigheder, som kan matche de europæiske tilsyn. Fraværet af et datatilsyn kan udgøre en komplikation, når den konkrete overførsel skal vurderes, jfr. herom senere.

14. Artikel 29-gruppen

Det danske Datatilsyn er organiseret som en funktionelt uafhængig myndighed under Justitsministeriet, hvilket indebærer, at dets afgørelser ikke kan påklages til ministeriet eller anden administrativ myndighed, jfr. §§ 56 og 61, men alene kan indbringes for domstolene, hvilket i praksis sker yderst sjældent. Det er i øvrigt sædvanligt i de fleste medlemsstater, at kun ganske få sager bliver forelagt for domstolene. Tilsynet består af et sekretariat og et råd, der er en enhed. Rådet, der især tager stilling til principielle og nye spørgsmål, er således ikke noget klageorgan.

I forhold til overførsler spiller tilsynet en væsentlig rolle i en række henseender. Udgangspunktet er ganske vist, at det er den dataansvarlige, der skal sikre sig, at en overførsel er lovlig, men dette udgangspunkt er dog modificeret. Dette er først og fremmest sket ved, at en række typer af overførsler til lande uden for EU forudsætter en tilladelse, jfr. hertil især i kapitel 5. Det er således i forhold til disse overførsler nødvendigt for eksportøren at sandsynliggøre, at lovens regler er overholdt.

I almindelighed er det vigtigt at være opmærksom på, at tilsynet ikke udelukkende fungerer reaktivt, men også søger at spille en proaktiv rolle. Foreligger der et overførselsbehov, vil den dataansvarlige virksomhed på et tidligt stadium kunne tage kontakt til tilsynet med henblik på at afdække, på hvilken måde en sådan overførsel vil kunne finde sted inden for lovens rammer. I denne henseende er det væsentligt at være opmærksom på, at det danske tilsyn traditionelt er ganske pragmatisk og derfor er indstillet på at finde frem til løsninger, der kan tilgodese legitime erhvervsmæssige mål. Selvsagt under forudsætning af, at dette er muligt inden for lovens brede rammer. Tilsynet bør derfor af eksportvirksomheden betragtes som en medspiller og ikke som en modspiller. Den proaktive funktion forudsætter, at den dataansvarlige tager et initiativ, og som allerede angivet kan det tit være hensigtsmæssigt at tage dette på et tidligt stadium. Herved kan det undgås, at der bliver foretaget investeringer i løsninger, som senere må revideres.

14. Artikel 29-gruppen

På det generelle niveau spiller Datatilsynet ligeledes en vigtig rolle. Både lovens og direktivets regler er forholdsvis åbne, og det er derfor løbende nødvendigt at tage stilling til en række spørgsmål af såvel generel som specifik karakter. Denne stillingtagen er medvirkende til at danne en praksis, som har indflydelse på bedømmelsen af efterfølgende konkrete overførselssituationer.

Centralt placeret i denne henseende er den arbejdsgruppe, der er etableret i medfør af direktivets artikel 29. Gruppen består af repræsentanter for datatil-

synene i alle medlemsstaterne samt Kommissionen.²⁰ Selvom gruppens udtalelser og anbefalinger alene er vejledende og dermed ikke er forpligtende for medlemsstaterne eller Kommissionen, har gruppen opnået betydelig indflydelse. Dette skyldes, at det er naturligt, at det enkelte tilsyn i sin nationale praksis som udgangspunkt følger de synspunkter, det har været med til at formulere i gruppen.²¹ I relation til dataoverførsler har artikel 29-gruppen været særlig aktiv, hvilket vil fremgå af fremstillingen i de kommende kapitler.

Gruppens aktiviteter på dette område kan karakteriseres på følgende måde. For det første kan den udtale sig om forskelle mellem reguleringen i de enkelte medlemsstater, jfr. artikel 30(2). Dette på mange måder relevante spørgsmål har ikke hidtil ikke haft nogen fremtrædende placering i gruppens arbejde, hvilket kan skyldes, at det er ganske følsomt, jfr. herom i kapitel 4. For det andet har gruppen medvirket ved vurderingen af, om bestemte ikke EU-lande har en retlig regulering, der tilstrækkeligt modsvarer direktivet, således at der uhindret kan ske dataoverførsler til disse, jfr. artikel 30(1b). For det tredje har gruppen formuleret en række generelle momenter, der skal tillægges betydning ved en sådan bedømmelse af den retlige regulering i tredjelande. Disse generelle momenter indgår med stor vægt i den nationale praksis og ligeledes i Kommissionens bedømmelsesgrundlag, jfr. hertil især i kapitel 5. For det fjerde har gruppen udtalt sig om adfærdskodekser, der er udarbejdet på fællesskabsplan, jfr. artikel 30(1d) samt i kapitel 6. For det femte har gruppen udtalt sig om og bidraget til udviklingen af særlige retlige instrumenter, der kan danne rammen om overførsler til tredjelande, der måske ellers ikke ville kunne finde sted, jfr. hertil i kapitel 6. Gruppens arbejde omfatter en bred vifte af aktiviteter, som er relateret til dataoverførsler, og alt i alt er artikel 29-gruppen centralt placeret i den europæiske databeskyttelsesret.

20. I betragtning af, at Artikel 29-gruppen rådgiver Kommissionen og udtaler sig om dennes initiativer, er det på sin vis lidt underligt, at Kommissionen er medlem af gruppen, selvom det er uden stemmeret. Det er ligeledes ofte Kommissionen, der varetager sekretariatsopgaver for gruppen. Denne konstruktion er sikkert i nogle tilfælde en styrke, men i tilfælde, hvor der foreligger uenighed, jfr. om Safe Harbor ordningen i kapitel 6, forekommer den problematisk.

21. I denne forbindelse må anmærkes, at der ikke nødvendigvis er enighed om de udtalelser, gruppen fremsætter. Sædvanligvis bliver dissenser ikke offentliggjort, men fremgår kun af mødereferater, der er fortrolige. Af forretningsordenen (Rules of Procedure af 11.9.1996) artikel 12(1) fremgår, at dissenser offentliggøres på anmodning, men det sker kun meget sjældent. Det er alt i alt ikke givet, at et datatilsyn i alle henseender vil føle sig forpligtet af en bestemt udtalelse. En større åbenhed forekommer ønskelig.

14. Artikel 29-gruppen

Det danske tilsyn er kun et af 25 tilsyn, og det er derfor på ingen måde givet, at tilsynets opfattelse fra starten svarer til den, som gruppen giver udtryk for. Dette kan skyldes flere forhold. De nationale tilsyn repræsenterer forskellige retskulturer og dermed også i et vist omfang forskellige måder at betragte databeskyttelsen på. Dette kan nødvendiggøre kompromiser eller medføre, at bestemte opfattelser ikke slår igennem på dette niveau. Mere jordnært har det betydning, at det er særdeles tidskrævende at deltage i gruppens arbejde, der i perioder er præget af et højt aktivitetsniveau. Dette kan betyde, at det danske tilsyn ikke altid har mulighed for at præge arbejdet, idet dette forudsætter, at der kan afsættes tilstrækkelige ressourcer hertil. Der må således ske en prioritering i forhold til tilsynets øvrige opgaver. Selvom der således ikke nogen sikkerhed for sammenfald mellem artikel 29-gruppens og Datatilsynets opfattelse, er dette dog i praksis sædvanligvis tilfældet. Særligt ved behandlingen af sager om dataoverførsler er et sådant sammenfald nærliggende.

Gruppens udtalelser og anbefalinger er dermed sammen med Datatilsynets afgørelser en væsentlig retskilde på dette område.²² Det er således inden for dette univers, at de dataansvarlige og de registrerede agerer, når det i de konkrete situationer skal vurderes, om dataoverførsler kan finde sted.

22. Praksis følges bedst via Datatilsynets hjemmeside, www.datatilsynet.dk. Under kategorien internationalt er der indsat links til artikel 29-gruppens udtalelser, idet de nyeste sædvanligvis først optræder på Kommissionens hjemmeside for databeskyttelse, hvortil der også er et link.

Det bemærkes, at i de kommende kapitler henvises til Artikel 29 gruppens udtalelser under betegnelsen WP (working paper).

KAPITEL 3

De tre dimensioner

1. Forskellige dimensioner

Det er sædvanligt og i og for sig naturligt ved behandlingen af spørgsmålet om dataoverførsler at koncentrere opmærksomheden om, hvorvidt og under hvilke betingelser persondata kan flyttes fra et land til et andet. Eksporten bliver sat i centrum. Dette synes at være temaet og udtryk for den interesse, eksportør og importør har. Tilsvarende er det i denne relation, at den registrerede har en interesse i, at der kun gennemføres de overførsler, som ikke aktualiserer en øget risiko for, at oplysninger vil blive misbrugt med integritetskrænkelser til følge. Det er denne beskyttelsesinteresse, reglerne skal varetage, og derfor må der være en eksportkontrol.

Under den registreredes perspektiv er det nærliggende at lægge til grund, at dette er det eneste tema, som skal tillægges betydning ved vurderingen af den retlige regulering. Denne tematisering forekommer derimod ikke fuldt ud dækkende, når problemstillingen betragtes under eksportørens og måske især under importørens perspektiv. Når denne indfaldsvinkel vælges, synes det, som om de overvejelser, der sædvanligvis bliver præsenteret i relation til den retlige regulering, er for snævre og dermed får det svære og komplekse overførselsproblem til at fremtræde lettere, end det faktisk er.

Dette skyldes, at der til en dataoverførsel er knyttet tre dimensioner. For det første om eksportlandets regler for national behandling er overholdt. For det andet om det er retligt muligt at flytte disse persondata fra land a til land b. For det tredje er der en dimension, som er relateret til anvendelsen af de data, som er blevet flyttet. Spørgsmålet er her, om det er retligt og faktisk muligt for importøren at anvende de data, der er blevet overført. Med andre ord er der både en international og en national facet, og disse er i det praktiske liv snævert forbundne. Det er åbenbart, at det ikke for de implicerede parter er tilstrækkeligt, at der er mulighed for at foretage en dataoverførsel, såfremt det efterfølgende grundet importlandets retlige regulering viser sig, at det ikke er muligt at benytte de overførte data til det formål, der begrundes, at

Kapitel 3 De tre dimensioner

en overførsel er ønskelig. Denne sammenhæng er som nævnt normalt overset eller i hvert fald underbetonet, men den er en del af forklaringen på, at overførsler i praksis giver anledning til mange problemer.

2. Første dimension: Eksportlandets ret

Den nationale dimension er i kapitel 2 behandlet primært under eksportperspektivet. Det er her fremhævet, at den grundlæggende forudsætning for, at en dataoverførsel kan finde sted, er, at persondatabehandlingen nationalt er lovlig. I denne forbindelse kan det nævnes, at det ofte er blevet fremhævet som en art paradoks, at fri dataoverførsel forudsætter, at der er fastsat en databeskyttelsesretlig regulering. Konkretiseret indebærer denne iagttagelse under eksportperspektivet, at personoplysningsloven ikke er nogen barriere for, men derimod et grundlag for dataoverførsler. Denne betragtning har basalt en retspolitisk karakter, idet den tilkendegiver, at dataeksport ikke politisk vil kunne blive accepteret, såfremt der ikke var udformet en beskyttelsesregulering, som giver de registrerede et vist mål af tryghed. Noget tilsvarende gør sig i en vis udstrækning gældende i importlandet, jfr. om den tredje dimension nedenfor. Indførelse af nationale regler om databeskyttelse tilvejebringer en målestok for en bedømmelse af beskyttelsesniveauet i forskellige lande og dermed fremmes mulighederne for overførsler. Dette illustreres af de blokeringer af overførsler, som, måske ikke så meget her i landet som i andre lande, fandt sted, inden databeskyttelseslovgivningen blev gennemført. Denne situation var hovedårsagen til den EU-retlige regulering, der omtales i kapitel 4-5.

Det er som udgangspunkt velbegrundet, at en overførsel forudsætter, at persondatabehandlingen er lovlig efter eksportlandets ret. Var dette ikke tilfældet, ville overførsler kunne virke underminerende i forhold til det almindelige beskyttelsesniveau, hvorved de ville medføre utryghed og under alle omstændigheder ikke være omgivet af den fornødne tillid. For mange dataansvarlige ville det være fristende at overføre oplysninger til lande uden snærende retlige bånd og dermed komme uden om de bindinger, som lovgivningen indebærer. For en umiddelbar betragtning er overførselens første dimension derfor naturlig og synes ikke at være ledsaget af nogen spørgsmålstejn. Retspolitisk kan dens styrke dog overvejes, og det er ikke nogen selvfølge, at overførsel som sådan skal betragtes som en behandling, jfr. hertil i kapitel 8.

3. Anden dimension: Overførselsregler

I de tilfælde, hvor der ikke er sikkerhed for, at der foreligger korresponderende beskyttelsesniveauer mellem to lande, er der tradition for at der i eksportlandet stilles krav om, at særlige betingelser skal opfyldes, for at en overførsel kan finde sted. Sådanne regler tager via skærpede behandlingsbetingelser sigte på at fastholde en databeskyttelse på et under eksportlandets perspektiv acceptabelt niveau uden at der nødvendigvis skal være tale om et fuldstændigt ensartet niveau. De fastsatte regler tilsigter at kompensere den utilfredsstillende retstilstand i importlandet. Målet er på ny at sikre sig imod en underminering af databeskyttelsesniveauet. Dette er i dag aktuelt i relation til overførsler uden for EU, der især tematiseres i kapitel 5 og 6.

Det er som ovenfor nævnt sædvanligt, at det er disse bestemmelser, som placeres i centrum ved en behandling af overførselsspørgsmålet. Dette er på mange måder naturligt, eftersom reglerne er afgørende for, hvor store muligheder der er for at gennemføre overførsler. Under en retlig betragtningsmåde er disse regler de centrale, og de fylder derfor også meget i denne bog. Under en praktisk indfaldsvinkel fylder de som det fremgår nedenfor dog ikke hele universet, eftersom det for en vellykket overførsel ikke er tilstrækkeligt, at persondata kan komme ud af eksportlandet, idet de også må kunne komme ind i og blive anvendt i importlandet.

4. Tredje dimension: Importlandets ret

Importlandets ret er en praktisk vigtig faktor, der kan være retligt relevant i forhold til dataoverførsler. Denne nationale ret udgør en komplikation, men skaber samtidig grobund for en realistisk forståelse af problemstillingen. Denne ret er ligeledes en komplikation for en bog som denne, eftersom det for en fuldstændig kortlægning af overførselsproblemets praktiske omfang i og for sig er nødvendigt at behandle den retlige regulering i alle de lande, hvortil det er sandsynligt, at der vil ske overførsler. Dette er selvsagt ikke realistisk, allerede fordi ingen har det tilstrækkelige kendskab til et sådant antal reguleringer. En sådan kortlægning er derfor ikke aspirationen her, som derimod er at klargøre, at denne problemstilling foreligger.

Når en dataansvarlig skal vurdere, om en dataoverførsel til en bestemt importør kan finde sted, skal den dataansvarlige ikke blot tage stilling til, om dette er muligt ifølge eksportlandets regler, herunder de specifikke overførselsregler, men tillige i en dialog med importøren vurdere, om de overførte data vil kunne behandles i overensstemmelse med de formål, der begrundes,

Kapitel 3 De tre dimensioner

at en overførsel fremtræder som hensigtsmæssig. Det må vurderes, om de overførte personoplysninger overhovedet vil kunne anvendes. I den konkrete situation må der således foretages en bedømmelse af et eller flere landes persondataretlige regler, samt på hvilken måde de fortolkes, med henblik på at afdække, om der skulle foreligge barrierer, som stiller sig hindrende i vejen for den ønskelige udnyttelse af de overførte persondata. Det må endvidere vurderes, om der i importlandet er anden lovgivning, som eksportøren i og for sig har et sagligt begrundet ønske om at opfylde, men som skaber problemer i forhold til databeskyttelsen.

I de tilfælde, hvor der foreligger særlige overførselsregler (den anden dimension), hvilket i dag er tilfældet ved dataeksport til tredjelande, jfr. kapitel 5, vil der være en vis sammenhæng mellem de to vurderinger. Det vil således kunne have betydning for, om overførselsbetingelserne er opfyldt, inden for hvilke retlige rammer oplysningerne efter overførslen vil blive behandlet. Den omstændighed, at en sådan behandling som følge af forhold i importlandet slet ikke er mulig, vil typisk medføre, at overførslen ikke aktualiseres, og skaber dermed rent retligt ingen problemer, idet det snarere er en for stor frihed for importøren til at behandle persondata, der kan fremtræde problematisk og skabe modstand imod overførslen. Eksportøren er ikke i alle tilfælde forpligtet til at sikre, at der er den tilstrækkelige databeskyttelse i importlandet, men det vil dog ofte være forudsat, at der gøres en indsats for at etablere en sådan situation.¹ Foreligger der ikke en tilstrækkeligt tryk databeskyttelsesmæssig situation, skabes der et behov for en særlig regulering, jfr. herom især i kapitel 6.

Det kan yderligere fremhæves, at medfører retlige forhold i importlandet, at det eksempelvis er særligt ressourcekrævende at gennemføre persondata-behandlingen kan dette begrunde, at den ikke gennemføres, selvom overførslen ikke er retligt hindret. Det økonomiske incitament er ikke til stede. En retlig regulering kan skabe en faktuel situation, som stiller sig hindrende i vejen for overførslen. Et eksempel kan være omfattende bureaukratiske procedurer eller krav om, at særligt krævende sikkerhedsforanstaltninger skal gennemføres. Dette spor skal ikke forfølges nærmere her, idet det afgørende i denne sammenhæng er, at en hensyntagen til importlandets ret udgør en integreret del af udfyldningen af de særlige overførselsregler. Dette moment tillægges betydning ved anvendelsen af de foreliggende regler samt ved udformningen af særlige overførselsgrundlag, jfr. hertil i kapitel 6.

1. Se hertil WP 114 af 25.11.2005 p.5-6 og som nævnt yderligere især i kapitel 5.

4. Tredje dimension: Importlandets ret

Det er specielt i de tilfælde, hvor der ikke er særlige overførselsregler, dvs. ved overførsler inden for EU, jfr. kapitel 4, at den tredje dimension får en selvstændig praktisk betydning, og hvor det kan iagttages, at den påkalder sig stigende opmærksomhed. I denne situation er der etableret et retligt rum, der karakteriseres ved frihed, og hvor der for en umiddelbar betragtning ikke skulle foreligge noget egentligt overførselsproblem.² Det er dog kun tilfældet, hvis man anlægger den endimensionale indfaldsvinkel. Tages det derimod i betragtning, at den vellykkede overførsel forudsætter, at importøren kan benytte de modtagne data, og at dette ikke må være for ressourcekrævende, bliver det klart, at der ikke i praksis uden videre er tilvejebragt nogen fuldstændig løsning. Som det fremgår i næste kapitel, er dette grundet direktivets karakter et hovedproblem inden for EU, der har sin rod i den manglende reelle harmonisering af de enkelte medlemsstaters lovgivning. Det er bemærkelsesværdigt, at der fortsat er fundamentale forskelle, idet der eksempelvis som nævnt i kapitel 1 end ikke er fuldstændig enhed om, hvorledes et grundlæggende begreb som persondata skal defineres. Det er eksistensen af sådanne forskelle, som understreger importsynsvinklens relevans.

Som et eksempel på en sådan disharmoni kan her nævnes overførsel af personoplysninger i manuel form. En virksomhed placeret i et andet EU-land vil her mødes med en vanskelighed, såfremt disse oplysninger ønskes overført til Danmark. Dette skyldes, at personoplysningslovens område som fremhævet i kapitel 1 er bredere end direktivets. Ifølge sidstnævntes artikel 3(1) gælder reglerne for oplysninger, »der er eller vil blive indeholdt i et register«, hvorimod loven for så vidt angår den private sektor gælder for enhver systematisk behandling, jfr. § 1(2). Ved overførsel af manuelle data, der falder uden for direktivet og de fleste EU-landes nationale lovgivning, men til gengæld er omfattet af personoplysningsloven, må eksportøren således foretage en selvstændig vurdering af, om oplysningerne overhovedet kan behandles i Danmark, idet det herved er forudsat at oplysningerne i øvrigt frit kan overføres fra den pågældende medlemsstat.³ Vurderinger af denne karak-

2. Principielt er reguleringen udformet således, at importlandets ret ikke har nogen betydning, da denne ikke kan hindre, at der sker en overførsel.
3. Dette er ikke nødvendigvis givet, selvom det i Lindqvist-dommen (betragtning 98) fastslås at direktivet kan udvides nationalt, så længe dette ikke strider mod fællesskabsretten. – Da direktivet ikke omfatter denne form for persondatabehandling gælder dets princip om fri dataoverførsel ikke uden videre, jfr. i øvrigt hertil i kapitel 4. Princippet om, at behandlingen nationalt skal være lovlig, gælder for eksport fra Danmark, jfr. POL § 27(5), men ikke nødvendigvis for eksport fra lande, der ikke regulerer anden manuel behandling end manuelle registre.

Kapitel 3 De tre dimensioner

ter ressourcebelaster selvsagt overførslerne og kan i nogle situationer medføre, at de ikke bliver gennemført.

Medtagelsen af denne dimension illustrerer, at det er nødvendigt at indtage såvel eksportørens som importørens situation, når en overførsel skal vurderes i praksis. Denne forståelse af problemstillingen har ikke mindst betydning på et forholdsvis tidligt stadium i den beslutningsproces, der gennemløbes, inden en overførsel søges sat i værk. Det indgår således i grundlaget for en beslutning om at foretage en overførsel, om den overhovedet i det konkrete tilfælde er meningsfuld. Det er her nødvendigt, at der foregår en nøje tilrettelagt og omhyggelig kommunikation mellem de to parter, der tager sigte på at afklare de foreliggende retlige og faktuelle omstændigheder med udgangspunkt i en præcisering af, hvilken behandling der skal finde sted hos importøren, herunder hvilke formål denne behandling tilsigter at opfylde.

Den tredje dimension udgør først og fremmest en komplikation, men som den givne beskrivelse viser, kan den have en vis positiv betydning ved at tilvejebringe en disciplin omkring overførselssituationerne. Den gør det således nødvendigt, at det nøje gennemtænkes, hvorfor en overførsel i den konkrete situation skal finde sted, herunder om denne er tilstrækkeligt kommercielt begrundet. Dette vil tit ske alligevel, men netop fordi overførsler i nogle tilfælde kan være ressourcekrævende, og fordi det også over for omverdenen er ønskeligt at dokumentere, at de er velbegrundede, er det særligt vigtigt nøje at overveje den enkelte overførsel. Set fra eksportørens synsvinkel har denne proces den yderligere fordel, at der herved kan ske en klarlægning af den form for behandling, som importøren agter at foretage. Dette er vigtigt, såfremt der efterfølgende overfor eksportøren bliver rejst tvivl om overførselens berettigelse.

5. Flere lande

Den omstændighed, at de nationale behandlingsmuligheder må tages i betragtning ved en vurdering af overførsler, har en særlig praktisk betydning i de tilfælde, hvor der skal ske overførsel fra eller til mange lande. Det er specielt her, at denne dimension afslører sig som en komplikation, der let kan medføre en reel begrænsning af overførselsmulighederne. For internationale virksomheder placeret i flere lande kan der ofte være en interesse at overføre data til et bestemt land med henblik på, at der kan ske en koordineret behandling af disse data. Dette kan være særlig relevant i koncerner, hvor det kan

6. Udfordring

bemærkes, at artikel 29-gruppen har fremhævet, at de enkelte selskaber først og fremmest skal overholde deres lands ret.⁴ En sådan samling af virksomhedens persondata forudsætter for det første, at det i alle eksportlande er muligt at foretage den pågældende overførsel, og for det andet, at oplysningerne kan behandles i importlandet, hvilket bl.a. i en del tilfælde forudsætter, at dette set under alle overførselslandes perspektiv er acceptabelt. Set under virksomhedens perspektiv er det ressourcemæssigt ønskeligt, at det er de samme regler, som skal tages i betragtning ved en bedømmelse heraf.

Denne beskrivelse svarer ikke i synderligt omfang til den virkelighed, der foreligger i dag. Selvom når der er tale om lande, som har et fælles overordnet retsgrundlag, direktivet, foreligger der ikke en sådan harmoni, idet der tværtimod i mange tilfælde er en afvigende national forståelse af regelgrundlaget og ligeledes en forskelligartet praksis hos de enkelte datatilsyn. Ved vurderingen af en overførsel til lande, om hvilke der ikke foreligger en generel positiv kommissionsafgørelse, foretager hvert lands datatilsyn på tilsvarende måde sin egen bedømmelse af importlandets ret, og denne vurdering er ikke nødvendigvis den samme. Det har herved betydning, at der ikke i direktivet er institueret en one stop ordning, der kan danne grundlag for en samordnet vurdering af overførslen. Der er på denne baggrund ikke nogen garanti for, at en koordineret overførsel kan finde sted, og det kan være denne omstændighed frem for selve overførselsreglerne, som blokerer for den løsning, den pågældende virksomhed efterstræber.

En tilsvarende problemstilling kan som nævnt foreligge, såfremt der er tale om flere importlande. Også i denne situation er det nødvendigt, at der sker en klarlægning af retsgrundlaget i hvert enkelt land, hvilket bl.a. kan resultere i betydelige udgifter til juridisk bistand. En sådan klarlægning vil i almindelighed være nødvendig som følge af, at eksportøren sædvanligvis har en interesse i, at der faktisk kan ske en behandling, og endvidere ofte er forpligtet til at sikre sig imod, at de overførte data vil blive misbrugt.

6. Udfordring

Alt i alt er det nationale ujævnheder, der er hovedårsagen til, at persondata ikke flyder frit over grænserne i dag. Der er mange årsager til, at denne situation foreligger. Her kan der være grund til at fremhæve, at der endda kan

4. WP 74 af 3.6.2003 p.7: »the internal rules of a corporate group cannot replace the data protection obligations by which the members of a corporate group are bound by law«.

Kapitel 3 De tre dimensioner

være tilfælde, hvor hensynet til databeskyttelse benyttes som et alibi for regler, der reelt indebærer en handelsbarriere.⁵ I hvilken udstrækning dette sker, er en af uenighederne på den internationale scene, idet nogle lande har mistænkt EU for at følge en sådan linie.

Dataoverførsler repræsenterer alt i alt en kompleks udfordring, som grundlæggende beror på, at den databeskyttelsesretlige regulering set under et internationalt perspektiv er uudviklet, jfr. kapitel 8. For langt de fleste lande repræsenterer en sådan regulering et ukendt territorium. Set under et dataoverførselsperspektiv savnes der koordinering og harmonisering. Der er et udtalt behov for en mere sammenhængende og overskuelig retlig regulering. Det må ligeledes konstateres, at der ikke er noget, som indicerer, at der i denne henseende vil ske afgørende forbedringer inden for de kommende år. På det retspolitiske plan er der et stort behov for såvel mod som fantasi, jfr. hertil i kapitel 8. De foreliggende disharmonier skaber overførselsproblemet, og det er på baggrund af og på trods af disse disharmonier, at konkrete overførsler må søges gennemført på en måde, som fortsat sikrer en acceptabel integritetsbeskyttelse.

For beskrivelsen af gældende ret, der tager sin begyndelse i kapitel 4, har det betydning, at der foreligger de nævnte tre dimensioner. Beskrivelsen tager sit udgangspunkt i overførselsreglerne og kan dermed fremtræde på samme måde som andre fremstillinger af denne problemstilling. Der vil dog løbende blive taget højde for, at der er to andre dimensioner, og det vil blive søgt eftervist, hvorledes disse må præge opfattelsen af selve overførselsreglerne. Det er således lagt til grund, at en realistisk beskrivelse af overførselsspørgsmålet må medtænke de tre dimensioner. Dette er påkrævet, for at de dataansvarlige, de registrerede og tilsynsmyndighederne kan forholde sig på den rette måde til de konkrete overførselssituationer.

5. Jfr. OECD Guidelines on the protection of privacy and transborder flows of personal data (1980) punkt 18: »Member states should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.«

KAPITEL 4

Inden for EU

Den gældende retlige regulering er baseret på en distinktion mellem dataoverførsler til tre typer af lande. For det første lande, som er medlem af EU samt medlemslande i EØS.¹ Det er overførsler mellem disse lande, der er temaet i dette kapitel. For det andet tredjelande, der er anerkendt som havende et tilstrækkeligt beskyttelsesniveau i forhold til direktivet, jfr. artikel 25(1). For det tredje tredjelande, der ikke antages at have et sådant niveau. Overførsler til tredjelande behandles i kapitel 5 og 6.

1. Fri overførsel

Efter i direktivets artikel 1(1) at have fremhævet fysiske personers grundlæggende rettigheder, herunder retten til privatlivets fred i henseende til information, fastsættes det i stk.2, at »medlemsstaterne må ikke af grunde, der har forbindelse med den i stk.1 foreskrevne beskyttelse, indskrænke eller forbyde fri udveksling af personoplysninger mellem medlemsstaterne«. Det fremgår af denne bestemmelse, at det er direktivets formål at personoplysninger frit skal kunne overføres mellem medlemsstaterne. I præambelens punkt 3-8 beskrives dette formål nærmere, idet det heraf fremgår at direktivet er et led i etableringen af det indre marked. EF Domstolen har i sin afgørelse i den såkaldte Lindqvist sag (C-101/01) ligeledes fremhævet, at fri dataoverførsel er direktivets egentlige formål, idet Domstolen i denne forbindelse lægger vægt på, at dette formål harmonerer med den traktatmæssige hjemmel for direktivets udstedelse (artikel 100A²). På denne baggrund tilkendegiver Domstolen den opfattelse, at der ved anvendelsen af direktivets øvrige bestemmelser skal tages hensyn til dette formål, og at der således ikke bør anlægges en fortolk-

1. Ifølge EØS-Komiteens beslutning 83/99 af 25.6.1999 er disse lande, Island, Liechtenstein og Norge, forpligtet til at implementere direktivet, hvilket da også er sket senest for Liechtensteins vedkommende ved lov nr.55 af 8.5.2002.
2. Nu efter Amsterdam-traktaten artikel 95.

Kapitel 4 Inden for EU

ning, som ikke harmonerer med formålet og dermed begrænser overførselsmuligheden (antagelse nr.97). Dette er også tilfældet i forhold til de af direktivets regler, der ikke direkte er baseret på en hensyntagen til det indre marked.

I personoplysningsloven findes der ikke en bestemmelse hvoraf det udtrykkeligt fremgår, at der er fri dataoverførsel inden for EU. At en sådan regel er gældende, kan udledes modsætningsvist af § 27, som alene fastsætter særregler for overførsler til tredjelande, der i § 3 nr.9 defineres som lande, der ikke er medlemmer af EU eller ikke med EU har indgået aftaler, som indeholder regler svarende til direktivets.³ Det er på sin vis uheldigt, at princippet om fri dataoverførsel ikke fremgår tydeligere af loven, der således ikke på dette punkt er retsinformatisk tilfredsstillende,⁴ men det er dog utvivlsomt, at denne regel er gældende.

Ifølge direktivet gælder princippet om fri overførsel for overførsler mellem medlemsstaterne. Spørgsmålet om overførsler til og fra EU-institutionerne er ikke nævnt, idet dette nok skyldes at ingen har tænkt på denne problemstilling. Institutionernes persondatabehandling er særligt reguleret i forordning 45/2001 af 18.12.2000, hvis regler i stor udstrækning svarer til direktivets. Det fremgår af præamblen betragtning 13, at forordningens formål er at muliggøre fri overførsel, idet det i betragtning 18 præciseres, at medlemsstaterne fortsat har de forpligtelser, der følger af direktivet. Ifølge artikel 8 kan institutionerne videregive oplysninger til medlemsstaterne, bl.a. når »modtageren godtgør nødvendigheden af videregivelsen af personoplysningerne, og der ikke er grund til at formode, at den registreredes legitime interesser vil kunne lide skade derved«. Overførslen er således ikke helt fri eller ubetinget.

Personoplysningsloven nævner ikke spørgsmålet, idet det kan bemærkes, at udenlandske myndigheder sædvanligvis ved anvendelsen af lovens regler kategoriseres på samme måde som private. I dette tilfælde er der dog ikke tale om en myndighed i en anden stat, hvorfor denne opfattelse ikke er direkte anvendelig. I mange tilfælde vil en overførsel kunne være foreskrevet i andre

3. Dermed er Grønland og Færøerne tredjelande, jfr. Betænkning 1345/1997 p.224, og overførsel af persondata til disse dele af det danske rige skal derfor bedømmes ud fra de regler, der omtales i kapitel 5. Overførsel fra Danmark, men derimod ikke fra andre medlemsstater, bliver i praksis bedømt forholdsvist liberalt.

4. I en række andre medlemsstaters lovgivning er princippet om fri overførsel angivet, jfr. Østrigs Datenschutzgesetz 2000 § 12(1), der præciserer, at dette ikke gælder for den offentlige sektor uden for EU-retten, Portugals lov 67 af 26.10.1998 § 18 med et forbehold i henseende til told og skat, Grækenlands lov 2472/97 § 9(1), samt Tysklands Bundesdatenschutzgesetz § 4b/1, der også nævner EU-institutionerne.

2. Begrundelsen for fri overførsel

EU-regler som eksempelvis en forordning. I andre tilfælde lægges det her til grund, at i betragtning af at EU-institutionerne må antages at have den samme beskyttelse som fastsat i direktivet, omfatter princippet om den frie dataoverførsel institutionerne, selvom overførsler fra disse ikke er helt frie, og fuld gensidighed dermed ikke foreligger. Det vil være kunstigt at betragte institutionerne som et tredjeland. Et grundlag herfor kan hentes i artikel 286(1) i EF Traktaten, der lader de databeskyttelsesretlige fællesskabsregler gælde for institutionerne.⁵ De i det følgende angivne synspunkter gælder således også for denne type overførsler, der dog næppe i henseende til den private sektor har en fremtrædende placering.

Forinden det overvejes, i hvilken udstrækning princippet om fri dataoverførsel afspejler virkeligheden kan det være hensigtsmæssigt at se nærmere på, hvad der egentlig kan udledes af direktivets artikel 1(2) og direktivet i øvrigt, jfr. i øvrigt yderligere hertil nedenfor. Ifølge sin ordlyd indebærer bestemmelsen en forpligtelse til ikke at hindre dataoverførsel, når dette er begrundet med en henvisning til de overordnede beskyttelseshensyn, som direktivet varetager. Dette er ikke ensbetydende med, at der er etableret en ubegrænset frihed til at overføre persondata, men alene at der ikke må fastsættes særlige betingelser for, at overførslen kan finde sted. Der må endvidere fremhæves, at bestemmelsen ikke er til hinder for, at dataudveksling hindres af andre grunde end dem, som er omfattet af artikel 1(1). Det kan endvidere lægges til grund, at bestemmelsen kun gælder i forhold til en persondatabehandling, der er omfattet af direktivet.⁶ Det er derfor nødvendigt at fastlægge, hvorledes direktivet er afgrænset, herunder om det omfatter hele Fællesskabsrettens område eller kun en mindre del af dette. Det kan dermed indledningsvis konstateres, at bestemmelsen ikke skaber nogen fuldstændig frihed, og at dens område ikke er ubegrænset. Allerede af disse grunde kan kapitlet ikke slutte her.

2. Begrundelsen for fri overførsel

Det er hensigtsmæssigt først at indkredse, på hvilket grundlag direktivet fastsætter princippet om fri dataoverførsel. Som det er fremgået af tidligere kapit-

5. Den her tilkendegivne opfattelse er anført af Peter Hustinx, European Data Protection Supervisor, som svar på en forespørgsel fra forfatteren. Hustinx karakteriserer den gældende regulering som en art *lex imperfecta*.

6. Jfr. i denne forbindelse POL § 4(6), hvori det fastslås, at loven finder anvendelse i forhold til en virksomhed etableret i EU, når persondatabehandlingen ikke er omfattet af direktivet, jfr. i øvrigt i kapitel 1.

Kapitel 4 Inden for EU

ler, er årsagen til, at der overhovedet foreligger et overførselsproblem, at der eksisterer disharmoniske beskyttelsesniveauer mellem landene. Dette var også situationen i medlemsstaterne på det tidspunkt, hvor direktivet blev gennemført. Nogle medlemsstater, f.eks. Danmark og Sverige, havde i mange år (1978/1973) haft lovregulering, mange lande havde ratificeret og gennemført Europarådets databeskyttelseskonvention, jfr. om denne i kapitel 5, men der var også medlemslande uden nogen retlig regulering, f.eks. Spanien. Denne disharmoni medførte i praksis, at dataoverførsler blev blokeret med uheldige økonomiske konsekvenser til følge, og mange opfordringer fra Kommission og Parlament⁷ om at tilslutte sig Europarådets konvention havde ikke båret frugt,⁸ idet kun 7 af de daværende medlemsstater havde ratificeret konventionen. Denne situation medførte, at det for realiseringen af det indre marked var praktisk nødvendigt, at Kommissionen fik gennemført et direktiv, selvom dette initiativ ikke blev modtaget med lige stor begejstring i alle medlemsstater.

Set under perspektivet det indre marked er det i betragtning af informationsfundets betydning for den internationale handel særdeles uheldigt at disharmonier i den nationale regulering hindrer dataudveksling. En sådan tilstand kan let føre til en reduceret synergi inden for EU og dermed svækkes dets position på verdensmarkedet. EU bliver ikke tilstrækkeligt en enhed, såfremt overførsler mellem medlemsstaterne bliver blokeret. Direktivet har på denne baggrund til hensigt at rette op på denne situation ved at etablere det retlige grundlag for, at persondata kan overføres, uden at dette giver anledning til integritetsorienterede betænkeligheder. På denne måde er direktivet centralt placeret i reguleringen af det indre marked.

3. Harmonisering?

Betryggende dataoverførsler forudsætter ideelt set, at der sker en harmonisering af den retlige regulering i medlemsstaterne således, at det i realiteten er uden betydning for de registrerede, hvor deres data befinder sig. En sådan harmonisering var da også et mål, da Kommissionen i 1990 iværksatte det arbejde, der siden skulle føre frem til direktivet. Det oprindeligt fremsatte

7. Dette skete første gang i 1976, jfr. EFT 1976 C 100.

8. Et historisk tankeeksperiment kunne være et spørgsmål om, hvorvidt et direktiv var blevet gennemført, såfremt disse opfordringer havde båret frugt. Sikkert, men dog ikke givet, idet Kommissionen måtte bruge mange kræfter på at trække en del modvillige medlemsstater til trug.

3. Harmonisering?

forslag til direktiv⁹ var vel ikke fuldt ud harmoniserende, men det tilstræbte dog en betydelig større ensartethed i medlemsstaternes nationale regulering, end der senere er blevet tale om. Denne reguleringsmodel gav dog anledning til betydelig modstand fra medlemsstaterne, herunder Danmark, og ligeledes, hvilket kan være værd at have i erindring i forhold til de problemstillinger, som drøftes i dette samt senere kapitler, fra det private erhvervsliv, der på dette tidspunkt ikke havde noget sikkert blik for betydningen af en samordnet og koordineret regulering af dataoverførsler. I en vis forstand kendte erhvervslivet ikke sin besøgstid. Mange ønskede, at databeskyttelse fortsat skulle være et nationalt anliggende, og havde svært ved at acceptere en EU-retlig regulering, hvis forbindelse til det indre marked ikke alle anså for åbenbar.

I 1992 blev subsidiaritetsprincippet en del af EU-retten, og da Kommissionen fremsatte sit andet forslag til direktiv i 1993, var dette betydeligt mindre harmoniserende på samme måde som slutresultatet i 1995. Dette forløb illustrerer bl.a., at der også inden for EU foreligger væsentlige retskulturelle forskelle, som har betydning for, med hvilken intensitet databeskyttelse kan reguleres. Direktivet har i et vist omfang medvirket til at udjævne disse forskelle, men som det fremgår nedenfor, er de fortsat virksomme i henseende til, på hvilken måde direktivet fortolkes og udfyldes i de enkelte medlemsstater. Det kan tilføjes, at de retskulturelle forskelle ikke er blevet mindre af, at direktivet i dag omfatter 25 medlemsstater.¹⁰

Det er efterhånden et klassisk spørgsmål inden for databeskyttelsesretten, på hvilken måde det vedtagne direktiv retligt skal kategoriseres. Svaret herpå er, at direktivet i sin helhed hverken er harmoniserende eller er et minimumsdirektiv, men at det derimod indeholder begge typer af bestemmelser. Det er ikke i alle tilfælde klart, om en bestemmelse har den ene eller anden karakter. Konsekvensen heraf er, at direktivet er svært at anvende. Domstolen har ganske vist udpeget visse af reglerne som harmoniserende og antaget, at direktivet principielt er udtryk for en fuldstændig harmonisering,¹¹ men domstolens angivelse heraf er dog ikke sket på en helt klar måde, eftersom det samtidig (Lindqvist antagelse nr.97) er fastslået, at direktivet indebærer betydelige frihedsgrader for medlemsstaterne. I almindelighed er det en fortolkning af direktivets enkelte regler, der er afgørende for, hvilken karakter de har. Det er ikke nødvendigt inden for rammerne af denne bog at gennemføre denne øvel-

9. Dette er optrykt i EFT 1990 C 277/3.

10. Ved hver udvidelse af EU-medlemskredsen kommer princippet om fri dataoverførsel til at omfatte flere lande.

11. Jfr. Lindqvist-dommen antagelse nr.96.

Kapitel 4 Inden for EU

se i forhold til alle bestemmelser i direktivet, idet der om de specifikke regler om dataoverførsel til tredjelande henvises til kapitel 5 og 6.

Her er det tilstrækkeligt i almindelighed at fastslå, at direktivet ikke har tilsigtet og ej heller har medført en fuldt ud harmoniseret databeskyttelse. Der er fortsat ganske betydelige nationale forskelle, som i hvert fald ikke er i uoverensstemmelse med direktivet, og som kan spille en rolle ved vurderingen af, om dataoverførsler fra de enkelte medlemsstater kan finde sted.¹² En væsentlig årsag til, at disse forskelle har stor faktisk betydning, er, at de ikke beror på de formelle bestemmelser i medlemsstaternes lovgivning, som ofte afskriver direktivets regler, men derimod beror på fortolkningen af disse bestemmelser. Det er ofte grundet den anvendte reguleringsform, jfr. under 4, vanskeligt at fastslå, at sådanne fortolkninger er direktivstridige, og indtil videre savnes tilstrækkelig praksis fra EF Domstolen til, at en bestemt direktivfortolkning kan tillægges den nødvendige autoritet. Det må betragtes som sandsynligt, at mange af de foreliggende disharmonier vil få lov til at leve i »bedste« velgående mange år endnu.

Herved brister den klassiske forudsætning for fri dataoverførsel, dvs. at der foreligger tilsvarende beskyttelsesniveauer i staterne, og den manglende harmoni sætter dermed spørgsmålstegn ved, om det i artikel 1(2) angivne formål altid kan realiseres. Denne tvivl fremgår endog af direktivets præambel, hvor det i betragtning nr. 9 fastslås, at der kan opstå nationale forskelle som følge af direktivets implementering, og at disse forskelle kan have konsekvenser for den frie udveksling af oplysninger. Det erkendes således her, at målet næppe vil kunne realiseres fuldt ud.

På denne baggrund er der særligt grund til at fremhæve, at direktivet ved denne udtalelse i præamblen fastholder princippet om, at der må foreligge et sammenligneligt beskyttelsesniveau, for at overførsler frit kan finde sted. Udtalelsen må læses således, at der (undtagelsesvist) kan tages hensyn til importlandets ret, selvom dette i og for sig er i strid med direktivets basale tankegang. Man undgår således den »fælde«, der består i at kræve fri overførsel uden samtidig at kræve modsvarende beskyttelsesniveauer. Dette må betragtes som meget væsentligt. Skulle artikel 1(2) altid ubetinget følges, ville direktivet kunne udgøre et grundlag for et brud med det grundlæggende princip, hvorefter den registreredes beskyttelse ikke må forringes som følge af over-

12. Dette konstateres i Kommissionens første rapport vedr. direktivets implementering, COM(2003) 265 final af 15.5.2003, jfr. især p.11-12. – I rapportens p.10 konstateres dog, at der ikke har været konkrete tilfælde, hvor dataoverførsler er blevet blokerede. Hertil kan føjes, at dette ikke er ensbetydende med, at disharmonierne er uden betydning i denne sammenhæng.

4. Direktivets reguleringsform

førsler. Hermed ville der ligeledes være opstået et legitimeringsproblem i forhold til de krav, som EU ønsker at stille i forhold til tredjelande, jfr. kapitel 5. Dette er ikke ensbetydende med, at dette princip er helligt og hævet over diskussion, men en eventuel fravigelse af princippet burde i givet fald have været systematisk indarbejdet i direktivet. Det er et plus, at dette ikke er sket implicit som en tyv om natten, jfr. i øvrigt den retspolitiske drøftelse heraf i kapitel 8.

4. Direktivets reguleringsform

Det er som også nævnt ovenfor ikke alene den ufuldstændige harmonisering, der i øvrigt efter direktivets gennemførelse er blevet kritiseret af repræsentanter for den private sektor, som skaber problemer. Den måde, hvorpå mange databeskyttelsesretlige regler, herunder direktivets, udformes, giver i sig selv anledning til harmoniseringsproblemer, der er uafhængige af, om det enkelte land har udnyttet en frihedsgrad i direktivet. Reguleringens genstand, der har en grundlæggende abstrakt karakter, kombineret med dens bredde, har medført, at der er opstået en tradition, hvorefter disse regler udformes åbent og i en del tilfælde har karakter af retlige standarder, der får deres egentlige substans via den måde, hvorpå de anvendes i praksis. Dette er eksempelvis tilfældet for de grundlæggende principper i artikel 6, jfr. omtalen af disse i kapitel 2. Den præcise forståelse af disse principper kan ikke læses i reglerne. Dette betyder, at selvom en regel i to medlemsstater fremtræder ens, er dette ikke nødvendigvis tilfældet, når reglens praktiske anvendelse tages i betragtning. Alle juridiske regler er fortolkelige, men i relation til retlige standarder er fortolkningsmulighederne særligt talrige og i mange tilfælde ligeledes uforudsigelige.¹³

Det er ikke blot i relation til de egentlige retlige standarder, at der kan opstå ujævnheder. Mange af de grundlæggende begreber har ikke noget entydigt meningsindhold, hvilket skaber grundlag for varierende nationale udfyldninger. Dette er søgt forebygget ved, at der i artikel 2 er angivet en række legaldefinitioner, som kan betragtes som harmoniserende. Selvom der bortses fra, at også legaldefinitioner er fortolkelige, kan det konstateres, at disse ikke har medført fuldstændig ensartethed. Eksempelvis opfattes som også nævnt i

13. Jfr. om regler af denne karakter Bernhard Gomard, *Juristen* 2005 p.191, hvorefter »til forståelse af standarder og af generelle regler i lovgivningen og opfattelser i supplerende retskilder må der benyttes en anden og friere fortolkning end til tydningen af detaljerede lovbestemmelser«.

Kapitel 4 Inden for EU

kapitel 3 et kernebegreb som persondata ikke på fuldt ud samme måde i medlemsstaterne, idet det i og for sig ganske bemærkelsesværdigt varierer, hvilke oplysninger der anses som persondata.¹⁴ Der kan endvidere konstateres divergenser i henseende til, hvornår en oplysning er identificerbar (data »gemt« under en kode). Det kan derfor samlet konstateres, at reguleringsformen er en af årsagerne til, at der uanset direktivet fortsat er mange forskelle mellem medlemsstaternes retlige regulering.

Det kan yderligere konstateres, at det databeskyttelsesretlige apparat i medlemsstaterne er forskelligt. Alle stater har, som direktivet foreskriver, et datatilsyn, men dets organisering og kompetencer er varierende.¹⁵ Nogle tilsyn har eksempelvis mulighed for selvstændig håndhævelse i form af bøder, medens andre som det danske må benytte politiet hertil. Mere praktisk er der væsentlige forskelle med hensyn til de ressourcer, tilsynene råder over, idet der kan skelnes mellem rige og fattige tilsyn, hvor det danske vist nok befinder sig midt imellem. I betragtning af, at tilsynene har stor betydning for den reelle databeskyttelse, er disse forskelle væsentlige, om end de kun har indirekte betydning i forhold til den frie dataoverførsel. I forhold til import af persondata såvel fra en anden medlemsstat som fra et tredjeland, jfr. om sidstnævnte i kapitel 5, har disse forskelle dog en ikke uvæsentlig praktisk betydning i forhold til de reelle muligheder for at gennemføre overførsler. Forskellene kan have en afskrækkende virkning.

Af tilsvarende praktisk betydning er de forskellige ordninger vedrørende anmeldelse af behandlinger til tilsynsmyndigheden. I den ene ende af skalaen befinder Spanien sig, idet enhver behandling skal anmeldes, medens en række andre lande kun kræver anmeldelse, når behandlingen vedrører en følsom situation, jfr. direktivets betragtning 53. I forhold til overførselsproblemet tredje dimension (importlandets ret) kan det endvidere i denne sammenhæng anmærkes, at de forskellige formularer, der skal bruges ved en anmeldelse, udgør en belastning for virksomheder, der opererer i flere medlemsstater.

14. Problemstillingen er især aktualiseret i England, hvor der i retspraksis anlægges en snæver definition. Den ledende dom er afsagt af Court of Appeal i sagen *Michael John Durant v. Financial Services Authority* (EWCA CIV 1746), hvor der lægges vægt på, at en oplysning skal være af betydning for personen, som skal være i fokus, idet »mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data«. Dommen blev søgt anket, men 29.11.2005 afviste House of Lords at behandle sagen. Mange forventer at Kommissionen herefter vil anlægge sag mod England ved EF Domstolen.

15. Dette er ligeledes tilfældet i henseende til den uafhængighed, tilsynet tilsikres. Som et bemærkelsesværdigt eksempel kan nævnes, at direktøren for det polske datatilsyn er tilsikret immunitet, der kun kan hæves af parlamentet (Sejm), jfr. lov 133/1997 § 11.

5. Andre hensyn end privatliv

Databeskyttelsesrettens bureaukrati kan give anledning til en uønskelig usikkerhed i forbindelse med overvejelser om dataeksport.

Disse forskelle eller ujævnheder skaber således for det første vanskeligheder for de dataansvarlige, som har et aktuelt overførselsbehov, idet divergenserne som nævnt sætter fokus på betydningen af importlandets ret. Selvom denne ret principielt ikke skulle have nogen betydning, har den alligevel betydelig indvirkning på overførselsmulighederne, og de foreliggende forskelle medfører bl.a. store udgifter til juridisk bistand, hvilket principielt ikke burde være nødvendigt. Forskellene skaber støj for den internationale handel, og der artikuleres tit et ønske om, at der i denne henseende gennemføres en simplificering af den samlede regulering. For det andet kan denne situation skabe en vis uigennemskuelighed for Kommissionen, hvis opgave er at vogte over, at direktivet bliver gennemført på en korrekt måde. Det er svært udefra at identificere en uheldig anvendelse af direktivet, når denne beror på en fortolkning af de ofte ikke entydige regler. For tiden, hvor der kun foreligger en rendyrket afgørelse fra EF Domstolen vedrørende direktivets anvendelse, er der således også af denne grund basis for betydelige diskrepanser mellem medlemsstatene, og dermed foreligger der en udfordring til den forudsætning om gensidighed, som er grundlaget for princippet om fri dataoverførsel.

5. Andre hensyn end privatliv

Som nævnt ovenfor gælder princippet i artikel 1(2) kun i den udstrækning, at en overførsel ikke må hindres med henvisning til hensynet til privatlivsbeskyttelse. Dette er en naturlig begrænsning, eftersom det er dette hensyn, der motiverer direktivets regler. Der er således ikke ifølge direktivet noget til hinder for, at en stat hindrer overførsler, når dette eksempelvis begrundes med skattepolitiske eller socialpolitiske hensyn. Det lægges her til grund, at denne reservation først og fremmest har betydning for dataoverførsler inden for den offentlige sektor, hvorimod den næppe har nogen praktisk betydning i forhold til kommercielt betingede overførsler i den private sektor. Så vidt det vides, findes der ikke her i landet lovgivning, der med henvisning til ikke offentligretlige hensyn opsætter betingelser for eller forbyder dataoverførsel i den private sektor. Idet det blot bemærkes, at en sådan mulighed foreligger, er der således ikke nogen grund til at opholde sig yderligere ved denne reservation.

6. Inden for direktivets område

Princippet om fri dataoverførsel gælder alene inden for direktivets område, der er nærmere fastlagt i artikel 3(2). Det fremgår bl.a. heraf – som noget i og for sig selvfølgelig – at direktivet kun gælder inden for fællesskabsrettens område. Hvorledes dette område er afgrænset, er det en større øvelse at udrede, men det er dog ikke nødvendigt at gennemføre denne her. Det kan fremhæves, at de aktiviteter, der pågår inden for den såkaldte 3. søjle, ikke er omfattet af direktivet, jfr. også nedenfor.

Ved udarbejdelsen af personoplysningsloven blev det lagt til grund, at det vil være uhensigtsmæssigt at have forskellige regler alt efter, om en person-databehandling er omfattet af EU-retten, eller dette ikke er tilfældet. En sådan regulering ville kunne skabe vanskeligheder i praksis. Loven gælder dermed for alle behandlinger, som ikke er reguleret ved sektorlovgivning, og selvom princippet om fri dataoverførsel inden for EU som nævnt kun indirekte kan udledes af loven, gælder dette princip således for alle persondatabehandlinger, der er omfattet af loven.¹⁶ Dette er tilfældet i dansk ret, men ikke nødvendigvis EU-retligt i forhold til de persondatabehandlinger, der ikke er medtaget i direktivet. Denne forskel har dog ikke nogen praktisk betydning i forhold til eksport af persondata fra Danmark.

Der kan således være grund til at fremhæve, at det ikke er alle de regler, der indgår i POL, som har et direkte EU-retligt fundament. Dette gælder eksempelvis for § 1(3), der lader loven omfatte behandling af virksomhedsoplysninger i en række relationer, idet direktivet overlader det til medlemsstaterne at bestemme, om sådanne oplysninger skal være omfattet, jfr. præambelens betragtning nr.24. Denne iagttagelse har som nævnt ikke umiddelbart direkte betydning for princippet om fri dataoverførsel, men kan dog have en indirekte betydning i og med, at regler af denne karakter præger vurderingen af, om der foreligger en sammenlignelighed med det land, hvortil en overførsel påtænkes. Under en importsynsvinkel udgør sådanne regler en komplikation, eftersom det er nødvendigt for en eksportør i et andet EU-land at vurdere, om overførte oplysninger, der frit kan behandles i eksportlandet, vil kunne behandles i importlandet. Det vil være påkrævet at afsætte ressourcer til at bedømme, om en påtænkt dataeksport er hensigtsmæssig.

16. Regulerer en sektorlov persondatabehandlinger, der er omfattet af direktivet, gælder princippet om fri dataoverførsel selvsagt også for disse.

6. Inden for direktivets område

Bestemmelser af denne karakter kan dog muligvis også have betydning for dataeksport fra Danmark, idet den første betingelse herfor som tidligere fremhævet er, at den nationale behandling er lovlig. Det kan her overvejes, hvilken betydning det har, om denne vurdering er baseret på regler, der ikke er direktivbestemte. Fører sådanne regler til, at behandlingen ikke er lovlig vil dette kunne blokere for en dataeksport, som vil kunne finde sted i andre medlemsstater. Dette kan opfattes som problematisk, selvom det forudsættes, at de pågældende regler ikke er i strid med andre dele af EU-retten; de følger blot ikke af direktivet. Kan der ikke på et andet EU-retligt grundlag ske overførsel, og der dermed er en blokering, foreligger der en uheldig situation og en utilfredsstillende manglende gensidighed mellem medlemsstaterne, uanset at spillet spilles uden for direktivets område.

I artikel 3(2) nævnes en række specifikke områder, som, uanset om de er omfattet af EU-retten, ikke er dækket af direktivet. Der er hovedsageligt tale om reguleringsområder, som er relateret til den offentlige sektor, og som dermed ikke har interesse her, men herudover nævnes behandling »som foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter«, jfr. herved POL § 2(3), der ligeledes undtager denne form for behandling med den i og for sig paradoksale konsekvens, at princippet om fri dataoverførsel ikke umiddelbart gælder. Det er desuagtet muligt, at overførsel frit kan ske, men det er ikke direktivet, der udgør grundlaget herfor. Man må her falde tilbage på det traditionelle udgangspunkt for reguleringen af privates indbyrdes forhold, hvorefter det, der ikke er forbudt, er tilladt. Fri overførsel på dette grundlag kan dog kun finde sted, såfremt overførslen rent faktisk kan karakteriseres som personlig eller familiemæssig og dermed finder sted i et lukket kredsløb.¹⁷ En overførsel, der eksempelvis sker fra en alment tilgængelig hjemmeside på Internettet, er således ikke omfattet af bestemmelsen og skal dermed vurderes som enhver anden form for behandling, jfr. herved EF Domstolens afgørelse i Lindqvist-sagen (antagelse nr.47). Lidt bagvendt kan man sige, at sådanne overførsler grundet direktivet kan ske frit inden for EU, idet dette primært er en teoretisk iagttagelse, eftersom disse overførsler i praksis ikke vil være begrænset til EU's område.

17. Jfr. den i kapitel 1 omtalte afgørelse i Datatilsynets Årsberetning 2000 p.37.

Kapitel 4 Inden for EU

7. Fri overførsel

Med de her angivne modifikationer er der fri dataoverførsel inden for EU.¹⁸ Betydningen heraf er, at den dataansvarlige ikke skal opfylde særlige betingelser for at foretage en sådan overførsel, og at det ikke er nødvendigt at indgive anmeldelse til eller opnå tilladelse fra Datatilsynet for at foretage en sådan overførsel. Er anmeldelse eller tilladelse påkrævet i forhold til den nationale behandling, skal denne indhentes, men omfatter således ikke overførslen. Det er således overladt til den dataansvarlige at foretage et skøn over, hvorvidt overførslen kan finde sted, idet dette særligt har betydning i forhold til de ikke anmeldelsespligtige persondatabehandlinger, idet den »gode anmeldelse« vil nævne at sådanne overførsler påtænkes.¹⁹ Dette skøn er relateret til det, som i kapitel 3 er betegnet overførselsproblemets første dimension. Den dataansvarlige må vurdere, hvorvidt den behandling, der danner grundlaget for overførslen, er en lovlig behandling i forhold til POL og om der er bestemte procedurer, som skal følges når en overførsel skal gennemføres. Det er særligt spørgsmålet om sikkerhed, der skal overvejes i denne forbindelse.

Overførslen betragtes i sig selv som enhver anden form for behandling. Om grundlaget for denne vurdering kan der hovedsageligt henvises til fremstillingen i kapitel 1 og 2 samt den databeskyttelsesretlige litteratur. Forudsættes det her, at der foreligger det tilstrækkelige behandlingsgrundlag, og at lovens principper er respekteret, tilbagestår alene spørgsmålet, om de registrerede, hvis data agtes overført, har rettigheder, som skal respekteres. Denne problemstilling belyses nedenfor, idet det bemærkes, at det her anførte også har betydning for overførsel til tredjelande, der behandles i kapitel 5 og 6.

8. Oplysningspligt

I første række foreligger spørgsmålet om, hvorvidt den dataansvarlige har en oplysningspligt, jfr. POL §§ 28 og 29. Ifølge disse bestemmelser skal der, når oplysninger indsamles, gives den registrerede forskellige former for information, idet formålet hermed er at tilvejebringe åbenhed omkring persondatabehandlingen. Denne forpligtelse, som ikke forudsætter en anmodning fra den registrerede, foreligger, både når oplysninger indsamles direkte fra den regi-

18. Se i denne forbindelse i kapitel 1 vedrørende lovvalget inden for EU.

19. Datatilsynet vil dog normalt kun kunne tage dette ad notam.

8. Oplysningspligt

strerede, og når dette sker indirekte ved at de indhentes fra andre kilder. Modtager en virksomhed således oplysninger fra en anden virksomhed, har den førstnævnte således en oplysningspligt, medmindre den registrerede på forhånd er informeret om, at en sådan videregivelse vil finde sted. Det skal være klart, at en sådan information er givet.

I forhold til overførsler må det overvejes, om disse regler indebærer en forpligtelse til at informere om, at en sådan vil finde sted. Det følger af Datatilsynets praksis, at såfremt den dataansvarlige på indsamlingstidspunktet er bekendt med, at en overførsel vil ske, skal der gives information herom. I denne forbindelse skal det oplyses, til hvilke lande²⁰ overførslen vil finde sted, og med henblik på hvilket formål denne finder sted. Er den dataansvarlige på indsamlingstidspunktet ikke bekendt med, at en overførsel vil finde sted, kan der i sagens natur ikke informeres herom. Dette må antages at gælde, selvom den dataansvarlige ikke kan udelukke, at en overførsel senere vil blive aktuel.

Ifølge § 30(1) er der ikke oplysningspligt, såfremt en sådan vil stride mod »afgørende hensyn til private interesser«. Denne vurdering skal foretages konkret i forhold til hver af de oplysninger, som ønskes overført, og ifølge Datatilsynets vejledning nr.126 af 10.7.2000 (den såkaldte rettighedsvejledning) punkt 2.3.4. kan information kun undlades, når der er »nærliggende fare for, at privates eller offentliges interesser vil lide skade af væsentlig betydning«. Det er således en ganske snæver undtagelse, men det kan dog i denne forbindelse overvejes, om det kan være en erhvervshemmelighed, at der finder en overførsel sted. Det kan vel ikke afvises, at en sådan situation kan forekomme, og det må i givet fald konkret vurderes, hvilke konsekvenser dette har, idet det bl.a. må tages i betragtning, hvilke momenter ved overførslen der må anses for at være fortrolige. Det kan således tænkes, at der i det hele ikke skal gives oplysning om overførslen, eller at dette blot ikke skal ske så specifikt, som det ellers er tilfældet; f.eks. at importlandet ikke oplyses. Det er den dataansvarlige virksomhed, som skal foretage denne vurdering, idet det må betones, at det vil være yderst sjældent, at § 30 vil kunne anvendes i forhold til dataoverførsler. Dette skyldes også, at der i almindelighed ikke er nogen pligt til at oplyse importørens identitet, hvilket mest nærliggende kan være en erhvervshemmelighed.

20. Den dataansvarlige er ikke forpligtet til at oplyse, hvem der specifikt er importøren, men skal efter omstændighederne oplyse, hvilke kategorier af modtagere der kan være tale om, jfr. også nedenfor samt under 9.

Kapitel 4 Inden for EU

Det kan herefter overvejes om der pligt til at informere på et tidspunkt, der ligger efter indsamlingen. En sådan forpligtelse kan ikke udledes af §§ 28 og 29 og i rettighedsvejledningen punkt 2.1.3 og 2.2.3 er det tilkendegivet, at der kun i særlige tilfælde skal gives oplysning om nye formål eller anden information, som er aktualiseret efter indsamlingen. Såfremt overførslen i forhold til indsamlingsformålet må betragtes som ikke forenelig, jfr. § 5(2), vil en ny oplysningspligt blive aktualiseret, idet det herved forudsættes, at der fortsat er en behandlingshjemmel. En sådan forpligtelse kan endvidere have sit grundlag i § 5(1), såfremt det lægges til grund, at denne information er en følge af princippet om god databehandlingsskik. Det følger ikke af Datatilsynets praksis, at der er en sådan forpligtelse, og selvom dette kunne siges at være i overensstemmelse med lovens almindelige aspiration om transparens, kan en informationspligt ikke i almindelighed antages at foreligge.

Det kan dog ikke udelukkes, at en informationsforpligtelse vil kunne være aktuel i særlige situationer.²¹ I et sådant tilfælde må der ved vurderingen tages hensyn til, hvor ressourcebelastende en sådan foranstaltning vil være for den dataansvarlige. I en situation, hvor den dataansvarlige af andre grunde løbende kommunikerer med de registrerede, eller hvor dette let kan ske, eksempelvis ved udsendelse af en standardmail, taler en del for, at der skal informeres. I andre situationer, hvor en selvstændig kommunikation skal iværksættes, lægges det her til grund at en sådan forpligtelse sædvanligvis ikke foreligger.

På dette punkt kan der i øvrigt være en forskel i forhold til overførsel til tredjelande, der behandles i kapitel 5. EU- og EØS-lande må betragtes som bona fide lande, hvor en overførsel principielt ikke kan aktualisere en integritetskrænkelserisiko og dermed ikke et specielt behov for information. Dette gælder ikke uden videre for tredjelande, hvilket kan begrunde, at der ud fra princippet om god skik i nogle tilfælde kan foreligge en informationsforpligtelse når der sker overførsel til sådanne lande. Den EU-retlige ramme påvirker således udfyldningen af lovens rettighedskatalog.

9. Indsigt

En registreret har efter POL § 31 ret til indsigt med hensyn til, hvilke oplysninger der bliver behandlet. Dette forudsætter en begæring fra den registrerede, og det bemærkes, at denne begæring ikke skal imødekommes, såfremt

21. At der vil kunne foreligge en udvidet informationsforpligtelse, tilkendegives i WP 114 af 25.11.2005 p.8, der vedrører dataoverførsler til tredjelande.

undtagelsesbestemmelsen i § 30 kan finde anvendelse. Fremsættes der en anmodning om indsigt, har den registrerede et krav om at få oplyst, hvilke oplysninger der aktuelt behandles, formålet hermed og kategorier af modtagere, hvilket i dette tilfælde vil sige dem, hvortil oplysninger overføres. Ved kategorier forstås typer og således ikke de specifikke modtagere; f.eks. forsikringsselskaber, men ikke det specifikke selskab. Kender den dataansvarlige det pågældende selskabs identitet, vil det dog kunne følge af princippet om god skik, at dette skal oplyses, medmindre § 30 finder anvendelse. Yderligere skal der gives tilgængelig information om, hvorfra oplysningerne stammer, jfr. herom nedenfor. En indsigtsanmodning skal besvares snarest muligt og sædvanligvis i hvert fald inden 4 uger. Der er sædvanligvis kun krav på indsigt hver sjette måned, jfr. § 33, idet det kan bemærkes, at fremsættes begæring om et skriftligt svar, kan den dataansvarlige tage en vis betaling herfor, jfr. § 34(2).

Der kan i forhold til en sådan indsigtsanmodning foreligge flere situationer. For det første kan den dataansvarlige være i besiddelse af oplysninger, der er eller vil blive overført. Som bekendt kan information være flere steder, og at der er sket en overførsel, er ikke til hinder for, at den dataansvarlige fortsat kan være i besiddelse af oplysningerne. I denne situation indebærer indsigtsretten formentlig, at der er en forpligtelse til at oplyse, at en overførsel har fundet sted, herunder til hvilket land dette er sket, hvorimod der ikke som nævnt i almindelighed er nogen forpligtelse til at oplyse præcist, hvem der har modtaget oplysningerne, men alene hvilken kategori af modtagere der er tale om. Den omstændighed, at overførslen har fundet sted tidligere, udelukker således ikke nødvendigvis, at der skal informeres om denne, når oplysninger fortsat også er i den dataansvarliges besiddelse. Dette må dog konkret forudsætte, at overførslen er foretaget inden for et vist rimeligt tidsrum, inden indsigtsanmodningen fremsættes. Der foreligger ikke tilsynspraksis, der nærmere kan verificere denne forståelse af gældende ret.

En anden situation foreligger, såfremt den dataansvarlige har foretaget en overførsel med den konsekvens, at den pågældende ikke længere på det tidspunkt, hvor begæringen fremsættes, er i besiddelse af oplysningerne. I en sådan situation kan en indsigtsbegæring besvares med, at der ikke behandles oplysninger om den pågældende. En dataansvarlig er således ikke forpligtet til at oplyse, at der på et tidligere tidspunkt er behandlet oplysninger, jfr. rettighedsvejledningen punkt 3.2.1, og uanset, at der ikke findes afgørelser herom, kan en sådan forpligtelse efter mit skøn ej heller udledes af princippet om god databehandlingsskik. Dette skyldes, at der i givet fald ville være tale om en anden type rettighed end den, som indsigtsadgangen tager sigte på. Det er muligt, at en sådan form for retrospektiv indsigt vil være ønskelig, men dette

Kapitel 4 Inden for EU

vil forudsætte en ændring af loven. Problemstillingen skal ikke drøftes videre her, jfr. dog under 9.1.

Som nævnt ovenfor skal der efter § 31(1 nr.4) gives information om, hvorfra behandlede oplysninger stammer. Denne forpligtelse foreligger kun, såfremt den dataansvarlige er bekendt hermed, og pålægger dermed ikke som udgangspunkt den dataansvarlige en særlig aktivitetspligt i denne henseende. Forpligtelsen kan have en vis betydning, såfremt der er tale om importerede oplysninger, idet det kunne antages at en dataansvarlig skal have et større opmærksomhedsniveau i denne situation, eftersom den registrerede kan have en særlig interesse i at få oplyst, at kilden er udenlandsk, idet dette bl.a. kan bidrage til en vurdering af datakvaliteten. Der er dog ikke tilsynsmyndighedspraksis, som kan understøtte dette synspunkt, idet det i rettighedsvejledningens punkt 3.2.1 endog antages, at den dataansvarlige ikke har nogen pligt til at føre et register over, hvorfra oplysninger stammer, jfr. også nedenfor. I den private sektor er der ikke som i den offentlige forvaltning nogen notatpligt.

9.1. Register over overførsler

Det kan desuagtet yderligere overvejes, om en dataansvarlig er forpligtet til at føre et register over de tilfælde, hvor data er blevet overført. For en sådan forpligtelse taler, at det kan tjene som dokumentation for, at overførselsreglernes overholdes, og kan være nyttigt, såfremt der senere opstår spørgsmål i denne relation. Et sådant register kan muliggøre, at eksportøren bedre kan medvirke til, at overførte oplysninger behandles forsvarligt i importlandet, hvilket specielt kan være relevant i forhold til tredjelande, men i almindelighed er der ikke nogen forpligtelse hertil, jfr. yderligere herom i kapitel 5 og 6. Der er dog ikke noget retligt grundlag for at antage, at der skal føres et register over eksporterede data, jfr. ovenfor om importsituationen, idet der snarest er tale om en fremgangsmåde, som kan betragtes som hensigtsmæssig og tit nyttig også under den dataansvarliges perspektiv.

Er der faktisk oprettet et sådant register, vil det afhænge af dettes specificeringsgrad, hvorvidt det udløser et krav om indsigt. Dette vil være tilfældet, såfremt registeret indeholder personidentificerbare data, men derimod ikke, såfremt det eksempelvis blot på en uspecificeret måde angiver, at der på et bestemt tidspunkt er sket overførsel af kundeoplysninger. Spørgsmålet må således vurderes konkret. Det kan yderligere fremhæves, at beror opbevaringen af information om foretagne overførsler alene på en funktionalitet i det edb system, som eksportøren har anvendt til at foretage overførslen, vil dette ikke medføre en indsigtsret. Spørgsmålet aktualiseres således alene, såfremt et egentligt register er blevet oprettet.

I almindelighed kan det til sidst bemærkes, at indsigtsretten ikke indebærer nogen begrænsning af retten til fri overførsel, men at den dataansvarlige blot skal have indrettet procedurer, der gør det muligt at besvare anmodninger om indsigt. En sådan forpligtelse kan ligeledes undertiden være aktuel for importøren, jfr. hertil i kapitel 6 vedrørende dataeksport til tredjelande.

10. Korrektion

Et af de grundlæggende principper, der blev omtalt i kapitel 2, er princippet om datakvalitet, idet den dataansvarlige skal sikre, at der kun bliver behandlet korrekte oplysninger, og det er dermed kun sådanne oplysninger, som kan overføres. Den dataansvarlige kan blive opmærksom på, at datakvaliteten ikke er god, grundet en henvendelse fra den registrerede, og er sådanne oplysninger videregivet skal der på begæring gives modtageren underretning herom, jfr. § 37(2) samt rettighedsvejledningens punkt 4.3.2.

Denne forpligtelse kan påhvile eksportøren i forhold til importøren i et andet land, idet den registrerede kan have en særlig interesse heri. En underretningspligt foreligger dog kun, såfremt den ikke er »umulig eller er uforholdsmæssig vanskelig«. Det vil afhænge af den konkrete eksportsituation, om dette er tilfældet, idet det her vil have betydning, om der er løbende relation mellem eksportør og importør. Det må herved tilføjes, at denne bedømmelse angår underretningen, og der skal dermed ikke tages hensyn til, hvor sandsynligt det er, at importøren faktisk vil foretage en korrektion.

11. Indsigelsesret

Blandt de øvrige rettigheder, der er angivet i loven, er det herefter alene indsigelsesretten i § 35, som har interesse i forbindelse med dataoverførsler.²² Det fremgår af denne bestemmelse, at en registreret kan fremsætte indsigelse mod, at oplysninger bliver behandlet, og såfremt denne indsigelse er berettiget, må behandling ikke længere finde sted. En sådan indsigelse kan fremsættes i forhold til en behandling, der i øvrigt er lovlig, og den kan således tænkes at være relateret til den frie dataoverførsel. Bestemmelsens formål er at

22. I forhold til overførsler til tredjelande fremhæves i praksis ofte bestemmelsen i § 39 (direktivets artikel 15) om rettigheder i forbindelse med automatiserede afgørelser. Bestemmelsen har dog et snævert anvendelsesområde.

Kapitel 4 Inden for EU

gøre det muligt for en registreret at stoppe en lovlig behandling, såfremt der foreligger sådanne individuelle omstændigheder, der medfører, at den konkret bedømt er integritetskrænkende. Databeskyttelse som en individuel rettighed bliver herved betonet. Det er den dataansvarlige, der i første omgang skønner, hvorvidt en indsigelse skal imødekommes, idet en afvisning heraf kan påklages til Datatilsynet.

Medens det kan tænkes ved overførsel til tredjelande, er det umiddelbart vanskeligt at konstruere et eksempel på, at en indsigelse i forhold til den frie overførsel er berettiget, men det ikke afvises, at sådanne situationer vil kunne forekomme. Under alle omstændigheder er en dataansvarlig forpligtet til at tage stilling til en fremsat indsigelse, inden dataoverførslen foretages. En negativ afgørelse kan den registrerede påklage til Datatilsynet, jfr. § 58(2), idet en klage nationalt ikke har opsættende virkning. Det kan dog overvejes, om en klage suspenderer overførslen, således at den dataansvarlige må afvente tilsynets afgørelse. Til støtte herfor kan anføres, at en overførsel har en mere definitiv karakter end mange andre former for persondatabehandling. Der er ikke nogen egentlige støttepunkter for at antage, at klagen har suspensiv virkning, men dette kan dog muligvis underbygges af princippet om god skik i § 5(1). Spørgsmålet er uafklaret i praksis.

Det må endvidere fremhæves, at en indsigelse kun har betydning for fremtiden. Fremsættes en berettiget indsigelse således, efter at overførslen har fundet sted, har den dermed ikke nogen konsekvenser for den foretagne overførsel, men afhængig af den konkrete situation kan den afskære importøren for at foretage anden behandling. Sidstnævnte vil primært kunne være aktuelt i forbindelse med de former for overførsler, der tematiseres nedenfor i kapitel 6. Der vil normalt ikke være grund til at kritisere en foretagen overførsel, da en indsigelse er baseret på individuelle omstændigheder, som det ikke kan forventes, at den dataansvarlige af egen drift bør være opmærksom på.

12. Sammenfatning

Sammenfattende kan det herefter lægges til grund, at der mellem EU- og EØS-lande gælder et princip om fri dataoverførsel. De dataansvarlige skal ikke opfylde særlige betingelser for at gennemføre overførsler. Dette er dog ikke ensbetydende med, at oplysninger i alle tilfælde kan overføres, idet dette i praksis kan være modvirket af begrænsninger af dataanvendelsen foranlediget af særlige regler i importlandet foranlediget af dets udfyldning af direktivet. Det kan i denne forbindelse også spille en rolle, at der i medlemsstaterne er anlagt forskellige niveauer med hensyn til håndhævelsen af de databe-

12. Sammenfatning

skyttelsesretlige regler, jfr. hertil i kapitel 7. Nogle importlande fremtræder dermed mere afskrækkende end andre, og dette kan i praksis medføre, at i og for sig fornuftige overførsler ikke gennemføres.

Princippet om fri dataoverførsel er ledsaget af undtagelser og især er det vigtigt at være opmærksom på, at overførsel kun kan ske, såfremt den efter POL er relateret til en lovlig behandling, og at dette bl.a. betyder at lovens rettighedsregler finder anvendelse. Når der således tales om fri dataoverførsel, er der tale om frihed med begrænsninger og frihed under ansvar. Men dog alligevel frihed, hvilket illustreres af reguleringen af de dataoverførsler, som er sat på dagsordenen i de kommende kapitler.

KAPITEL 5

Overførsel til tredjelande

1. Forhistorie

Det har til alle tider været en aspiration, at personoplysninger skal kunne overføres til andre lande, men aspirationen har ligeledes været, at dette skal ske på en i forhold til integritetsbeskyttelsen betryggende måde. Der har været et ønske om at etablere en form for global konsensus om en sådan beskyttelse, således at personoplysninger ideelt kan udveksles mellem alle lande. En ideel aspiration er udviklingen af en global databeskyttelseskultur. En ubegrænset eller ureguleret frihed til at foretage dataoverførsler har derimod aldrig været på dagsordenen.

23. september 1980 udstedte OECD sine Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retningslinierne fastslår en række grundlæggende databeskyttelsesprincipper, som i dag i EU antages at udgøre de basale minimumskrav, som reguleringen i et tredjeland under alle omstændigheder skal opfylde for at en dataoverførsel fra et EU land skal være acceptabel.¹ Disse retningslinier, der blev genbekræftet ved en konference om e-handel i Ottawa oktober 1998, fastslår i nr.17 et princip om fri dataoverførsel mellem stater, der har tilsluttet sig retningslinierne, men der åbnes mulighed for at der kan gøres undtagelse herfra, når der er særlige grunde hertil. Der er således ikke som i direktivet tale om en i princippet ufravigelig grundsætning, jfr. kapitel 4.

En tilsvarende regulering fremgår af Europarådets konvention 108 af 28. januar 1981 »om beskyttelse af det enkelte menneske i forbindelse med elektronisk behandling af personoplysninger«. Konventionen angiver på samme måde som OECD's retningslinier en række grundlæggende databeskyttelsesprincipper. Fri dataoverførsel mellem konventionsstaterne fastslås i artikel 12, der i stk.2 angiver, at »en kontraherende part må ikke med det ene

1. Jfr. WP 19 af 3.5.1999 p.4.

Kapitel 5 Overførsel til tredjelande

formål at beskytte privatlivets fred, forbyde overførsel af personoplysninger til en anden kontraherende parts territorium eller gøre sådan overførsel betinget af særlig tilladelse«. Også her er der fastsat en række undtagelser fra princippet (stk.3), og der er dermed ikke nogen ubetinget forpligtelse til at acceptere overførsler mellem konventionsstaterne. Efter i 1987 at have gennemført en revision af lov om private registre, der bl.a. åbnede mulighed for registerindsigt, ratificerede Danmark konventionen i 1989, og den udgør således en bindende folkeretlig forpligtelse. Dette er i dag ligeledes tilfældet for alle øvrige medlemsstater samt EU som sådan,² jfr. yderligere om konventionens betydning nedenfor under 7.

Inden personopplysningsloven trådte i kraft var der i § 21 i lov om private registre (lovbekendtgørelse 622/2.10.1987) fastsat en i forhold til overførsel af følsomme persondata ganske restriktiv regulering, der ikke skelnede mellem forskellige kategorier af lande, jfr. dog stk.4. I registerlovens tidsalder påkaldte dataoverførsler sig sjældent interesse her i landet, og bestemmelsen, der i dag alene har historisk interesse, omtales derfor ikke nærmere her.³

2. Udgangspunkt

Især OECD's retningslinier og i nogen mindre udstrækning Europarådets konvention har fortsat en vis praktisk betydning,⁴ men den bestemmende regulering under et europæisk perspektiv udspringer af direktivet, som udgør udgangspunktet ved en bedømmelse af globale dataoverførsler. Det er det beskyttelsesniveau, der er udmøntet i direktivet, som danner målestokken for en vurdering af sådanne overførslers tilladelighed. Dette udgangspunkt har givet anledning til en vis kritik, der hovedsageligt er baseret på den iagttagelse, at en europæisk opfattelse søges udstrakt til et område, der ikke kan be-

2. Normalt er en konvention kun åben for stater, men ved en justering af konventionen 15.6.1999 blev det gjort muligt, at EU kunne tilslutte sig denne.

3. Om bestemmelsen henvises til Peter Blume: *Personregistrering* (3.udg. København 1996) p.128-132. Se endvidere vedrørende praksis Registertilsynets Årsberetning 1980 p.89-92, 1991 p.136-40, og 1995 p.109-10.

4. Årsagen til at OECD's retningslinier fremhæves, er, at disse hovedsageligt benyttes i lande, der ikke har gennemført en generelt dækkende databeskyttelseslovgivning. På denne måde har retningslinierne en mere direkte betydning for national ret, end tilfældet er for konventionen, der for det meste omfatter lande med national lovgivning.

2. Udgangspunkt

tragtes på dette grundlag.⁵ Direktivets regulering af overførselsspørgsmålet er i overensstemmelse med klassisk databeskyttelsesretlig tankegang, men det er et åbent spørgsmål, om denne tankegang kan forenes med nutidens informatiserede økonomi, og det kan ligeledes give anledning til tvivl, om direktivet er tilstrækkelig åbent i forhold til andre retskulturer, jfr. yderligere hertil i kapitel 8.

Medens direktivet i hvert fald i hovedsagen sikrer, at der i de forskellige EU-lande er gennemført en retlig regulering, der etablerer et beskyttelsesniveau som fastsat i direktivet, foreligger en sådan sikkerhed ikke for lande, som ikke omfattes af direktivet. Dette er de såkaldte tredjelande, der udgør hovedparten af verdens lande. Under hensyntagen til det grundlæggende princip om sammenlignelige beskyttelsesniveauer, der også er fremhævet i de ovenfor nævnte tidlige internationale instrumenter, er det ikke på denne baggrund ønskeligt eller forsvarligt af hensyn til integritetsbeskyttelsen uden videre at have fri dataoverførsel til disse tredjelande.

En sådan ordning ville meget let underminere den beskyttelse, som direktivet intenderer at give unionens borgere, idet en del dataansvarlige vil være fristet til at overføre oplysninger til lande, der ikke begrænser anvendelsen af persondata. Der ville således i praksis opstå en række data havens, som i en internationaliseret verden kunne medføre, at direktivet i betydelig udstrækning mistede sin mening. Selvom en overførsel til et tredjeland er en behandling, der skal være nationalt lovlig, jfr. POL § 27(5), vil denne forudsætning ikke i sig selv tilstrækkeligt kunne sikre imod overførsler til lande, hvor persondata kan behandles uden begrænsninger. Dette er baggrunden for direktivets ordning, hvor det i dettes forarbejder fremhæves, at fandtes en særlig regulering ikke, ville der »være risiko for, at Fællesskabets indsats for at sikre personer et højt beskyttelsesniveau ville blive undermineret ved videregivelse til tredjelande, der ikke garanterer en tilstrækkelig beskyttelse. Endvidere forudsætter en fri udveksling af oplysninger mellem medlemsstaterne, som søges indført med dette direktivforslag, at der vedtages fælles regler med hensyn til videregivelse af oplysninger til tredjelande«.⁶ Som det fremgår, er der en sammenhæng mellem fri adgang til overførsler i EU og en ensartet

5. Christopher Kuner: *European Data Privacy Law and Online Business* (Oxford 2003) anfører således p.87, at »indeed, many of the controversies surrounding European data protection law have been caused by the fact that legal instruments designed mainly for intra-European use have been forced by the expanding information economy to be applied to global problems on a scale for which they were not intended«.

6. KOM(92) 422 endl.udg. – SYN 287 af 15.10.1992. – Se også Registertilsynets Årsberetning 1993 p.29.

Kapitel 5 Overførsel til tredjelande

dataeksportkontrol i forhold til den øvrige verden. En fuldstændig harmonisering af betingelserne for disse dataoverførsler er dog ikke blevet resultatet i praksis, jfr. nærmere nedenfor.

Det er på denne baggrund udgangspunktet i gældende ret, at en persondataoverførsel til et tredjeland udgør en særlig behandlingstype, som kun kan finde sted, såfremt specielle betingelser er opfyldt.⁷ Disse krav er relateret til denne form for overførsler og udgør således et lag, der er placeret oven på de nationale behandlingsbetingelser, og som udfylder overførselsspørgsmålets anden og til dels også dets tredje dimension. Som fremhævet i tidligere kapitler dækker betegnelsen »fri dataoverførsel« således den situation, at der ikke er fastsat sådanne særlige betingelser. I forhold til de fleste tredjelande finder sådanne særegne behandlingsbetingelser anvendelse. Regler af denne karakter er dog kun nødvendige, såfremt der ikke foreligger den ønskelige sammenlignelighed, og det kan ikke på forhånd udelukkes, at der findes tredjelande, som kan matche direktivets regulering, og hvor sådanne betingelser altså ikke er nødvendige.⁸

3. Forskellige tredjelande

Direktivet udelukker ikke, at der kan være fri overførsel til tredjelande, idet det af artikel 25(1) fremgår, at der må skelnes mellem lande, der »sikrer et tilstrækkeligt beskyttelsesniveau«, og lande, hvor dette ikke er tilfældet. På det generelle niveau foreligger således to typer af tredjelande, jfr. yderligere hertil nedenfor. Der er endvidere i direktivets artikel 26(2) åbnet mulighed for, at der ved siden af de almindelige regler kan iværksættes en række specielle former for regulering, der kan muliggøre dataoverførsler i den private sektor. Der kan bl.a. være tale om adfærdskodekser og kontraktregulering. Disse specielle reguleringsmuligheder, der tager sigte på lande, som ikke opfylder tilstrækkelighedsnormen, behandles særskilt i kapitel 6.

7. Før direktivets ikrafttræden (1998) sås undertiden særlige ordninger. Et meget omtalt eksempel er sagen om togkortet til Deutsche Bahn, hvor kortet kun kunne betales med visa, således at personoplysningerne skulle behandles i South Dakota. I 1995 indgik datatilsynet i Berlin en aftale herom, der indebar, at tysk ret fandt anvendelse, og at tilsynet kunne gennemføre inspektioner i USA.

8. Det bemærkes, at direktivets artikel 25 og 26 ikke på alle punkter er implementeret på samme måde i medlemsstaterne, jfr. COM (2003) 265 final p.18. Fremstillingen i dette kapitel er baseret på den danske forståelse af disse regler.

4. Generelt anerkendte lande

Hovedproblemet består herefter i at afklare, på hvilken måde det kan fastlægges, om der som grundlag for overførsler foreligger et tilstrækkeligt beskyttelsesniveau i et tredjeland. Dette kan indebære, at en konkret dataoverførsel kan ske frit, eller mere videregående, at det generelt fastslås, at et bestemt tredjeland regulerer opfylder denne norm, således at der frit kan overføres oplysninger til dette. Direktivets artikel 25(6) gør det således muligt for Kommissionen at træffe en sådan afgørelse, hvilket indtil videre er sket i henseende til Argentina, Canada (med visse reservationer), Guernsey, Isle of Man⁹ og Schweiz.¹⁰

Der gennemføres et omfattende udredningsarbejde forud for en sådan anerkendelse, idet det pågældende lands regulering nøje vurderes, herunder om det er tilstrækkeligt sandsynligt, at fastsatte regler korresponderer med virkeligheden. Dette sker i første omgang i artikel 29-gruppen, hvis undersøgelser resulterer i en anbefaling til Kommissionen.¹¹ Et forslag til beslutning forelægges herefter i artikel 31-udvalget, der består af repræsentanter for medlemsstaternes regeringer, jfr. artikel 25(6) og 31(2), hvor den nærmere procedure er beskrevet. Som det yderligere omtales nedenfor, skal anerkendte lande i almindelighed have et tilstrækkeligt beskyttelsesniveau, men ikke nødvendigvis have fuldt ud de samme regler som direktivets. Der stilles ikke et krav om ækvivalens. Den foretagne vurdering er dog i almindelighed ganske streng og nøjeregnende, hvilket illustreres af, hvor få lande der er blevet godkendt.¹²

9. For en god ordens skyld bemærkes, at Guernsey og Isle of Man har selvstyreordninger i forhold til Storbritannien, der indebærer, at disse områder uafhængigt råder over den databeskyttelsesretlige regulering.
10. Den i kapitel 6 omtalte Safe Harbor ordning er ligeledes godkendt, men denne ordning har så særegne træk, at den bedst kategoriseres som et særligt overførselsgrundlag.
11. Jfr. WP 22 af 7.6.1999 (Schweiz), WP 24 af 7.9.1999 (Ungarn, der i dag er medlemsland), WP 39 af 26.1.2001 (Canada, hvor det bl.a. nævnes at reguleringen i den private sektor kun omfatter erhvervsvirksomheder), WP 40 af 26.1.2001 (Australien med negativ indstilling bl.a. grundet, at ikke alle sektorer er reguleret, at tilsynets undersøgelseskompetence er begrænset til statsborgere eller personer med fast bopæl, og at der kun er garanti imod reeksport af data vedrørende australske statsborgere), WP 63 af 3.10.2002 (Argentina med fremhævelse af dette lands særlige habeas data grundrettighed), WP 79 af 13.6.2003 (Guernsey), WP 82 af 21.11.2003 (Isle of Man).
12. Det er tankevækkende, at det i WP 63 p.14-15 vedrørende Argentina kritiseres, at tilsynsmyndighedens direktør udnævnes og afskediges af justitsministeren, når det tages i betragtning, at dette svarer til den danske ordning!

Kapitel 5 Overførsel til tredjelande

Til lande, der har opnået godkendelse, kan oplysninger frit overføres, om end dette ikke synes at være helt åbenbart i forhold til reguleringen i personopplysningsloven. Efter dennes § 3 nr.9 er disse lande fortsat at betragte som tredjelande, og de er derfor omfattet af § 27. Det følger herefter af § 50(2), at en overførsel af oplysninger omfattet af § 50(1), dvs. i praksis først og fremmest følsomme oplysninger, i en række tilfælde forudsætter en tilladelse fra Datatilsynet, jfr. om denne ordning under 13.

I betragtning af, at Kommissionens afgørelse er bindende for medlemsstaterne, der herefter ikke har adkomst til at fastsætte særlige betingelser, er dette en noget problematisk regulering, som bør overvejes i forbindelse med en revision af loven, hvor § 3 nr.9, som ikke er direktivbestemt, bør ændres¹³ eller ophæves. I § 50(3) er der ganske vist åbnet mulighed for, at justitsministeren kan fastsætte undtagelser fra tilladelseskravet, men dette er endnu ikke sket i forhold til de generelt godkendte lande. Som det fremgår nedenfor, kan det være vanskeligt for en dataansvarlig i konkrete tilfælde at afgøre om et ikke godkendt land har et tilstrækkeligt beskyttelsesniveau, og her kan det være ræsonnabelt at forudsætte en tilsynstilladelse, men i tilfælde, hvor Kommissionen generelt har fastslået dette, er et tilladelseskrav en barriere, der er svært forenelig med det EU-retlige system. Dette er tilfældet, selvom tilladelsen gives kurant, idet det kan anmærkes, at der for tilladelsen skal betales et gebyr på 1.000 kr., jfr. § 63(2).

Artikel 25(4) giver mulighed for, at Kommissionen kan fastslå, at bestemte tredjelande ikke har et tilstrækkeligt beskyttelsesniveau, idet medlemsstaterne herefter skal lægge dette til grund. Sådanne beslutninger er ikke blevet truffet, og der er således ikke blevet etableret en sortliste, hvilket også diplomatisk ville kunne være problematisk. Det kan diskuteres, hvor stor en værdi en sådan sortliste ville have, idet den så vidt ses ikke ville udelukke konkrete overførsler til de pågældende lande i medfør af artikel 26 (1-2). Listen ville være en unødvendig manifestation.

5. Tilstrækkelighed

I almindelighed er der behov for at indkredse, på hvilken måde det afgøres, om et land eller en singulær konkret overførsel opfylder normen om tilstrækkelighed. Det kan indledningsvis fremhæves, at der ikke stilles krav om, at

13. I Estlands personopplysningslov af 12.2.2003 er der efter § 28(3) fri overførsel til stater, der er godkendt af Kommissionen.

5. Tilstrækkelighed

det pågældende land har en regulering, som fuldt ud svarer til direktivets. Det er dermed ikke forudsat, at der er sket en form for implementering af direktivet, hvilket da også ville overspænde EU's betydning i den globale verden. Reguleringen skal ikke være ens eller ækvivalent, men blot medføre et sammenligneligt beskyttelsesniveau. Selvom dette er en mere realistisk ordning, gør den på ingen måde opgaven nemmere.

Direktivet er som udgangspunkt ikke til megen hjælp, idet det ikke direkte indeholder nogen uddybning endsige præcisering af, hvad der skal forstås ved tilstrækkelighed i artikel 25(1), jfr. ligeledes præambelens Betragtning 56 og 57. I artikel 25(2) angives dog en række retningslinier for, på hvilken måde denne vurdering skal foretages. Det anføres i denne bestemmelse, at »samtlige forhold« skal tages i betragtning, idet der skal lægges vægt på oplysningstypenes art, behandlingsformålet, behandlingstiden, de regler af enhver karakter,¹⁴ som gælder i tredjelandet, samt dettes sikkerhedsforanstaltninger. Denne bestemmelse er udformet på en sådan måde, at den tager sigte på den dataansvarliges konkrete vurdering af tilstrækkelighed, og synes således ikke umiddelbart direkte retningsgivende for de generelle vurderinger, som er nævnt ovenfor. I praksis danner bestemmelsen dog udgangspunkt for sådanne bedømmelser. Det følger af bestemmelsen, at et land, der ikke er generelt anerkendt, i nogle situationer kan have et tilstrækkeligt niveau med fri overførsel til følge, medens dette i andre situationer ikke er tilfældet, jfr. mere om denne komplikation nedenfor.

Der er særlig grund til at fremhæve, at det ikke er noget krav, at det tilstrækkelige niveau er opnået ved anvendelse af en bestemt form for retlig regulering. Dette har i øvrigt en indirekte betydning i forhold til de specielle tilfælde, der behandles i kapitel 6. Særligt er der grund til at betone, at der ikke stilles krav om, at der skal være lovgivning, som dog i forhold til den i praksis foretagne udfyldning af direktivet må antages at være nødvendig, såfremt et tredjeland skal opnå en generel anerkendelse. Det kan bemærkes, at det er i god overensstemmelse med den måde, EU-retlig regulering i almindelighed gennemføres på, at der ikke i alle tilfælde stilles krav om lovgivning. Når bortses fra forordninger, der ikke skal (må) implementeres, er det sædvanligvis overladt til medlemsstaterne, på hvilken måde de gennemfører EU retten i deres nationale ret, idet dette blot skal ske således, at forpligtelserne faktisk bliver overholdt. Det tilsvarende gælder således her, og i det hele ville det kunne opfattes som problematisk, såfremt det blev foreskrevet,

14. I WP 74 af 14.1.1998 anføres, at der kan tages hensyn til regler, der ikke er retsregler, forudsat at de overholdes.

Kapitel 5 Overførsel til tredjelande

hvorledes en suveræn stat formelt skulle udforme sin retlige regulering. En sådan ordning ville formodentlig internationalt være blevet betragtet som for vidtgående, og den ville ligeledes kunne have været en blokering i forhold til den overordnede målsætning om at så mange lande som muligt gennemfører en regulering, som opfylder tilstrækkelighedsprincippet.

Vurderingen af, om tilstrækkelighedsnormen er opfyldt, foretages i sagens natur, inden overførslen finder sted, men en sådan vurdering kan også være aktuel efter overførslen. Dette kan bero på, at der efterfølgende er sket ændringer i tredjelandets ret. Det er de samme momenter, der indgår i vurderingen, idet en efterfølgende negativ bedømmelse vil indebære, at persondata ikke længere frit kan overføres.¹⁵ Det vil derimod ikke i alle tilfælde i praksis være muligt at tilbagekalde allerede overførte data.

6. Udfyldning af tilstrækkelighedsnormen

Artikel 25(2) bringer os ikke meget længere frem mod en klarlægning af, hvorledes tilstrækkelighedsnormen skal forstås. En sådan afklaring er søgt tilvejebragt af artikel 29-gruppen. I gruppens centrale udtalelse herom, WP 12 af 24.7.1998, er der formuleret en række almindelige synspunkter, som fungerer som vejledende for praksis såvel generelt som konkret. Udgangspunktet er en skelnen mellem krav til indholdet i den databeskyttelsesretlige regulering og krav til regler vedrørende procedure og håndhævelse. Artikel 29-gruppen lægger således afgørende vægt på, at det ikke er nok, at der findes gode regler om databeskyttelse, hvis disse regler ikke er bakket op af et vist apparat, der kan sikre deres håndhævelse. Der må være tale om virkelig ret og ikke blot ret på papiret. Det forekommer utvivlsomt, at man må sikre sig mod, at der i tredjelandet blot er skabt en illusion om databeskyttelse. EU må være på vagt imod retligt bondefangeri.

Indledningsvis omtales i det følgende de indholdsmæssige krav, der først omfatter en række principper, som især har deres fundament i et udvalg af direktivets bestemmelser. Med udgangspunkt i artikel 6 fremhæves, at der skal være regler om formålsbestemthed¹⁶ og om datakvalitet, idet dette suppleres med et krav om regler om berigtigelse samt bestemmelser om at data-

15. Der er ikke eksempler på, at et tredjeland har mistet sin godkendelse som tilstrækkelig, men der er ikke tvivl om, at denne mulighed foreligger.

16. I Tysklands Bundesdatenschutzgesetz af 1.1.2003 fastsættes i § 4c, at importøren skal informeres om, at oplysningerne kun må behandles i overensstemmelse med det formål, der begrundes overførslen.

6. Udfyldning af tilstrækkelighedsnormen

behandlingen skal være proportional. Det er i denne sammenhæng interessant at bemærke, at ikke alle de grundlæggende principper i artikel 6 er blevet medtaget, idet tidsbegrænsningsprincippet eksempelvis er udeladt. Dette er i og for sig overraskende, eftersom de grundlæggende principper som fastsat i artikel 6 sædvanligvis alle betragtes som den fundamentale del af databeskyttelsen. I en række andre udtalelser fremhæves dog også de øvrige principper, hvorfor der ikke skal lægges for meget i, hvad der er udeladt i WP 12, jfr. herved også nedenfor om specifikke krav. Det foretagne uddrag kan ses som en illustration af, at der kun stilles krav om tilstrækkelighed, og at der derfor i konkrete tilfælde kan være regler eller principper, som ikke behøves tillagt vægt. I forhold til en generel godkendelse må det derimod antages, at tredjelandet skal opfylde alle de i artikel 6 nævnte principper. Dernæst stilles der krav om at den dataansvarlige skal være forpligtet til at gennemføre sikkerhedsforanstaltninger, jfr. direktivets artikel 17. Dette krav betragtes normalt som centralt i henseende til sikringen af, at databeskyttelsen faktisk virker, idet manglende sikkerhed virker underminerende i forhold til den øvrige regulerings effektivitet.

Som rettigheder for den registrerede fremhæves for det første, at der skal være regler, som sikrer transparens, idet der her refereres til oplysningspligten, jfr. direktivets artikel 10 og 11. For det andet skal der sikres ret til indsigt, jfr. herved artikel 12. Som det omtales i kapitel 6, giver indsichtsretten, der i europæisk ret betragtes som fundamental, anledning til bekymring i nogle tredjelande, idet denne ret frygtes at danne udgangspunkt for større mængder af erstatningssøgsmål med heraf følgende store økonomiske udgifter for den dataansvarlige. Endelig skal der for det tredje være en ret til at gøre indsigelse, jfr. artikel 14(1a). Sidstnævntes medtagelse kan for så vidt undre, idet denne ret i hvert fald i dansk ret ikke tillægges nogen særlig praktisk betydning.

De hidtil nævnte krav har en direkte basis i direktivet, men som et yderligere krav fastsættes, at der skal findes regler, som hindrer, at overførte data bliver reeksporteret til lande, der ikke opfylder de nævnte krav, idet dette dog ikke gælder, såfremt de undtagelser fra tilstrækkelighedsprincippet, der er angivet i artikel 26(1), er opfyldt,¹⁷ jfr. om disse nedenfor under 12. En regu-

17. Se om denne problemstilling Christopher Kuner p.129-32, der finder det uklart, hvorledes spørgsmålet om reeksport skal bedømmes i forhold til artikel 26(1).

Med den skepsis i forhold til artikel 26(1), som artikel 29-gruppen i dag giver udtryk for, jfr. WP 114 af 25.11.2005 samt nedenfor under 11, er det nærliggende at antage, at det kun ganske sjældent kan komme på tale at acceptere reeksport på dette grundlag.

Kapitel 5 Overførsel til tredjelande

lering af reeksport er et nødvendigt krav, idet videre overførsler ellers ville kunne underminere den ordning, som direktivet søger at etablere. Alt ville let komme ud af kontrol. Forbuddet mod reeksport er således væsentligt, og det kan særlig fremhæves, at det nok især er dette krav, som forudsætter at der er institueret kontrolmekanismer. Det må erkendes, at risikoen for reeksport i praksis udgør en væsentlig usikkerhedsfaktor, der forstærkes af den omstændighed, at persondata kan være flere steder på samme tid. Det er ofte meget svært at kontrollere, hvor personoplysninger befinder sig, og ligeledes hvorfra de er blevet overført. Risikoen for, at der sker reeksport illustrerer, at overførsler uanset de fastsatte regler må baseres på tillid til modtagerlandet og på forventninger om, at de fastsatte regler faktisk vil blive overholdt, jfr. yderligere om dette moment senere.

Det hidtil nævnte er krav, der i alle tilfælde skal være opfyldt, men i forhold til konkrete overførsler kan der yderligere stilles specifikke krav, hvor artikel 29-gruppen nævner nogle eksempler. Omfatter overførslen følsomme data, skal der træffes særlige foranstaltninger, idet der som et eksempel nævnes en regel, hvorefter behandling forudsætter samtykke. Er formålet direkte markedsføring, skal den registrerede have en indsigelsesret.¹⁸ Er formålet at oplysningerne skal danne basis for automatiserede afgørelser skal de rettig-heder, der fremgår af direktivets artikel 15, være opfyldt. Dette er som nævnt alene eksempler på særlige situationer, og hvordan de kan håndteres, og er dermed ikke noget udtømmende katalog over de regler, der skal være opfyldt ved en konkret overførsel.

Betydningen af denne del af gruppens policy-fastlæggelse er, at den dels danner et udgangspunkt for en vurdering af, om tilstrækkelighed generelt foreligger, dels kan inspirere til en afgrænsning af de momenter, der kan kræves opfyldt i forbindelse med konkrete overførsler. Det kan konstateres, at for så vidt angår det indholdsmæssige gives tilstrækkelighedsnormen en stor bredde, og at der i hvert fald for en umiddelbar betragtning vil være mange dataimportører i tredjelande, som vil have vanskeligheder med at opfylde disse krav. Der er således alt i alt tale om en ganske streng udfyldning af direktivets tilstrækkelighedsnorm, som kan efterlade det indtryk, at artikel-29 gruppen reelt er skeptisk over for at modificere direktivets ordning i noget nævneværdigt omfang.

Det må herved tages i betragtning at vurderingen af, om en af reglerne i artikel 26(1) er anvendelig, foretages i tredjelandet.

18. Siden fremkomsten af WP 12 har der været en tendens til i stigende omfang at forudsætte et samtykke (opt in), når formålet er markedsføring, jfr. herved direktiv 58/02 artikel 13.

6. Udfyldning af tilstrækkelighedsnormen

Dette indtryk bestyrkes, når de krav til fremgangsmåde og håndhævelse, der formuleres af gruppen, medtages i vurderingen. Disse krav er baseret på det naturlige udgangspunkt, at det ikke er tilstrækkeligt at der er gode regler, men at det tillige er påkrævet, at de overholdes i praksis, om end det realistisk erkendes, at dette ikke kan sikres 100 %, jfr. herved i kapitel 7. Det skal efter gruppens opfattelse sikres, at den dataansvarlige importør er bekendt med sine forpligtelser, og at der er fastsat effektive sanktioner i tilfælde af regelbrud. Hertil kommer, at der skal være en eller anden form for tilsyn. Det foreskrives ikke, at der skal være et datatilsyn, selvom et sådant tilsyn betragtes som essentielt i europæisk ret. Dette må antages at skyldes, at det vil være for indtrængende i andre landes retlige systemer, såfremt der blev stillet krav om en bestemt myndighedsstruktur. Det forudsættes således blot, at der udøves et tilsyn, og at der dermed er offentlige myndigheder, som har dette som en af deres opgaver. Det tillægges herved særlig betydning at der findes et organ, som kan bistå de registrerede, når disse vil gøre deres retsposition gældende. Endelig fremhæves, at der skal være mulighed for erstatning i tilfælde af regelbrud, idet der skal ske anvendelse af domstole eller voldgift.

Det kan konstateres, at kravene i henseende til fremgangsmåde og håndhævelse ikke er så præcise som de indholdsmæssige krav, men det afgørende er at der bliver stillet begge typer af krav. Som nævnt ovenfor er disse krav ikke udelukkende rettet til tredjelande, som har en interesse i at opnå generel godkendelse, men har tillige betydning ved udformningen af generelle ordninger som ramme for konkrete overførsler mellem virksomheder, jfr. nærmere herom i kapitel 6.

Afslutningsvis er der grund til at nævne, at artikel 29-gruppen fremhæver forskellige typer af overførsler, der må påkalde sig særlig opmærksomhed og agtpågivenhed, når det skal overvejes, om en overførsel kan finde sted. I denne forbindelse (WP 12 p.29) fokuseres på overførsler, der vedrører følsomme oplysninger, oplysninger der kan medføre et økonomisk tab (f.eks. kreditkort), oplysninger, der indebærer risiko for personlig sikkerhed, oplysninger, der kan begrunde afgørelser med vidtrækkende følger (f.eks. kreditgivning), oplysninger der kan skade eller ødelægge omdømme, oplysninger, der kan medføre handlinger, som væsentligt forstyrrer privatlivets fred (f.eks. telefonopkald), massive mængder af oplysninger (f.eks. via Internettet), oplysninger, der danner grundlag for fordækt indsamling af oplysninger (f.eks. cookies). Denne liste, der sikkert vil kunne udvides, og som altså ikke er udtømmende, illustrerer behovet for, at tilsynsmyndigheden er informeret i hvert fald om bestemte former for overførsler til utilstrækkelige lande, men bortses fra måske det sidste eksempel, er der ikke tale om overførsler, som

Kapitel 5 Overførsel til tredjelande

under alle omstændigheder bør være udelukkede. De er blot særligt integritetsrisikable.

7. Forholdet til konvention 108

I det følgende behandles problemstillingen primært under et landeperspektiv, idet det bl.a. vurderes, i hvilken udstrækning kategorien tredjeland er entydig. Som fremhævet i begyndelsen af kapitlet blev de første bestræbelser i vores del af verden på at etablere et fundament for internationale dataoverførsler udfoldet i Europarådets regi. Basis for disse er konvention 108/81. Alle EU-medlemslande er også medlemmer af Europarådet, hvis medlemsskare på for tiden 46 lande ligeledes omfatter stater, der ikke er medlemmer af EU. Hertil kommer, at lande, der ikke er medlemmer af Europarådet, ligeledes har mulighed for at ratificere konventionen, hvilket dog endnu ikke er sket. I dag har 33 lande ratificeret konventionen.

Spørgsmålet er herefter, om der uden videre kan ske dataoverførsel til lande, der har ratificeret og gennemført konventionen, som i øvrigt dannede forlæg for direktivet, jfr. præambelens betragtning nr.11. Dette er ikke uden videre tilfældet,¹⁹ idet konventionen dels ikke forpligter konventionsstaterne til at etablere et datatilsyn dels ikke indeholder regler om reeksport. Set under direktivets perspektiv er konventionen dermed ikke fuldt ud tilfredsstillende. Under indtryk heraf er sådanne regler dog efterfølgende blevet fastsat i en protokol til konventionen,²⁰ og har det pågældende land tiltrådt denne protokol og fastsat sådanne bestemmelser i sin nationale ret, må det antages, at reguleringen lever op til tilstrækkelighedsnormen. En generel anerkendelse skal dog fortsat fastslås efter den procedure, der er angivet i direktivets artikel 25(6).

Den her tilkendegivne opfattelse harmonerer dog ikke med alle medlemsstaternes lovgivning. I den svenske personoplysningslov (1998:204) fastsættes § 34(2), at der frit kan ske overførsel til lande, der har ratificeret konventionen. I den tilsvarende norske lov 31/2000 nævnes i § 29(2) mere modificeret, at en sådan ratifikation kan inddrages som et moment ved vurderingen. I Tjekkiets lov 101 af 4.4.2001 § 27(2), i Polens lov nr.133 af 29.8.1997 § 47(2) og i Irlands lov 6/03 S.12(4 a i), angives, at der frit kan ske overførsel,

19. Jfr. WP 12 af 24.7.1998.

20. Protokol (ETS 181) af 8.11.2001, der er trådt i kraft 1.7.2004. Blandt tilsluttede ikke EU-lande er Albanien, Kroatien og Slovakiet.

8. Forskellige sektorer

når dette følger af en international forpligtelse. I den norske lovs § 30b går det skridt videre, at der kan ske overførsel, når dette er pligtigt som følge af en folkeretlig aftale eller som følge af medlemskab af en international organisation.²¹

I den her nævnte regulering lægges således til grund, at en folkeretlig forpligtelse kan medføre, at en overførsel kan finde sted, uanset at direktivets betingelser ikke er opfyldt. Dette vil i praksis kunne medføre overførsler til lande, der ikke har et tilstrækkeligt beskyttelsesniveau, og selvom der i disse tilfælde foreligger en konflikt mellem to retlige systemer, folkeretten og EU-retten, lægges det her til grund, at direktivet har forrang, og at der derfor ikke uden videre bør ske overførsel i denne situation. Dette må antages at være opfattelsen i dansk ret. Problemstillingen illustrerer i øvrigt de disharmonier, der foreligger mellem medlemsstaterne.

8. Forskellige sektorer

Et land udgør ikke nødvendigvis en enhed under en databeskyttelsesretlig betragtningsmåde. I lande, der ikke har gennemført en generelt dækkende lovgivning, kan der således være sektorer, hvor reguleringen lever op til normen om tilstrækkelighed, og andre, hvor dette ikke er tilfældet. Et sådant land vil ikke generelt kunne anerkendes, men en partiel anerkendelse er en mulighed, selvom der endnu ikke er set eksempler herpå, idet dette måske skyldes, at en sådan godkendelse ikke er blevet søgt. Det kan særligt fremhæves, at der i en række lande, eksempelvis USA (Privacy Act 1974), er en vis tradition for retligt bestemt databeskyttelse i den offentlige sektor, hvilket hænger sammen med den traditionelle opfattelse af, at menneskerettighederne alene vedrører forholdet mellem stat og individ. I den udstrækning relationen virksomhed og individ ikke antages at have en menneskeretlig dimension, kan den private sektor i større udstrækning overgives til den regulering, der determineres af markedet, hvor konkurrenceforholdene antages at ville medføre en form for databeskyttelse. Tilbageholdenhed med hensyn til statslig regulering af den private sektor kan i fortsættelse heraf bero på den rolle, som staten i medfør af landets forfatning er tildelt, idet USA igen er en god illustration heraf.

21. Michael Wiik Johansen m.fl.: Personopplysningsloven (Oslo 2001) nævner p.220 som eksempler Røde Kors og FN. Der ses ikke i dansk ret at være taget stilling til denne særlige overførselssituation. Det kan dog ikke antages, at dataoverførsler frit kan ske.

Kapitel 5 Overførsel til tredjelande

I den private sektor, der er denne bogs tema, er der således en større sandsynlighed for, at der ikke findes et tilstrækkeligt beskyttelsesniveau i tredjelande. Det er dog ikke givet, at dette er tilfældet for alle dele af den private sektor, idet det er karakteristisk for reguleringen i en del lande, at der i visse sektorer, f.eks. kreditoplysning og kreditvurdering, er en regulering, selvom de fleste sektorer ikke er undergivet formel retlig regulering. Dette kan skyldes, at der er oplevet et særligt behov, idet persondatamisbrug i sådanne udvalgte sektorer har umiddelbart følelige konsekvenser for den enkelte borger, eller at der har foreligget meget omtalte sager, som har fået lovgivningsmagten til at reagere. Denne ujævnhed indebærer, at når en bestemt overførsel bliver overvejet, er det påkrævet ganske detaljeret at undersøge importlandets ret, og denne undersøgelse kan i nogle tilfælde afsløre, at der på det konkrete reguleringsområde foreligger et retligt fundament, der muliggør en overførsel, idet dette vil forudsætte sikkerhed for, at oplysningerne ikke bliver videregivet til andre sektorer. Det er på denne baggrund ikke nogen enkel opgave at foretage en vurdering af de forskellige tredjelande. Selvom mange virksomheder opererer inden for bestemte områder, som de opnår retlig erfaring med og dermed har gode muligheder for at bedømme, er det tit krævende at tage stilling til, om en bestemt overførsel kan finde sted.

9. Føderale lande

Denne opgave kompliceres yderligere af, at mange lande har en føderal struktur eller en anden form for speciel forfatningsstruktur. Det kan ikke tages for givet, at der i sådanne lande er en ensartet databeskyttelse. Det vil afhænge af den pågældende lands forfatning, i hvilken udstrækning delstater har kompetence til at regulere dette område.²² I de tilfælde, hvor et sådant statsstyre foreligger, vil der både indholdsmæssigt og i forhold til håndhævelse kunne foreligge afvigende beskyttelsesniveauer inden for nationalstaten. Der kan eksempelvis være tale om situationer, hvor der indholdsmæssigt er retsenhed, men hvor håndhævelsen sker decentralt og dermed forskelligartet. Selvom et land ikke generelt er anerkendt som havende et tilstrækkeligt beskyttelsesniveau, kan der i disse tilfælde være dele af landet, som lever op til en sådan

22. Se illustrativt WP 22 om Schweiz (26 kantoner og 4 officielle sprog) og WP 39 om Canada (provinser og territorier). Af begge udtalelser fremgår det, at der er tale om en komplikation.

norm. Dette må indgå i vurderingen af en konkret overførsel og understreger på ny behovet for juridisk viden om importstedet.

Der kan undertiden være tale om en betydelig komplikation, idet dette måske særligt er tilfældet i relation til USA, hvor det er blevet iagttaget, at der ikke findes to delstater, som har den samme databeskyttelsesretlige regulering.²³ Ved dataeksport til USA, hvor den særlige Safe Harbor ordning, der omtales i kapitel 6, ganske vist kan udgøre en vis lettelse, kan det således være særlig nærliggende at være opmærksom på forudsætningen om, at reeksport bør være reguleret. Der kan være tilfælde, hvor personoplysninger f.eks. kan overføres til en virksomhed i Californien, men hvor dette forudsætter, at oplysningerne ikke senere overføres til andre stater i USA. I sådanne tilfælde foreligger der en særlig udtalt risiko for en manglende transparens, som kan give anledning til utryghed. Det er særdeles vanskeligt at sikre, at der ikke sker en reeksport, og overførselens gennemførlighed vil dermed kunne bero på, om der foreligger tilstrækkelig tillid til, at importørvirksomheden faktisk vil respektere de fastsatte begrænsninger. I en vis forstand er tillid i sådanne tilfælde bedre end kontrol, der reelt kan repræsentere en illusion.

10. Tillid

I fortsættelse heraf er der grund til i almindelighed at fremhæve, at det ikke alene er den kolde jura, der i praksis har betydning ved vurderingen af overførselsmuligheder. Andre momenter spiller også en rolle. I forhold til generel anerkendelse og andre almindelige ordninger er det åbenbart, at der foreligger et politisk moment. Det kan have betydning for de almindelige relationer mellem EU og et bestemt tredjeland, hvorledes sidstnævntes regulering bliver vurderet i databeskyttelsesretlig sammenhæng, idet en negativ bedømmelse kan have økonomiske konsekvenser. Dette kan udløse et diplomatisk pres med henblik på at opnå et positivt resultat, og der kan således i en vis forstand komme falske lodder på vægtskålen. Når bortses fra Safe Harbor ordningen, jfr. om denne i kapitel 6, kan der dog ikke påvises tilfælde, hvor der er gennemført en generel ordning, som ikke har et tilstrækkeligt grundlag i det pågældende lands retlige regulering. Det virker, som om EU i denne henseende har formået at holde fanen højt.

23. Jfr. om reguleringen i USA, Peter Blume: Databeskyttelsesret (2.udg. 2003) p.256-57 med henvisninger.

Kapitel 5 Overførsel til tredjelande

Mere uformelle momenter spiller derimod sandsynligvis en vis rolle i henseende til vurderingen af konkrete overførsler. Papir er som bekendt taknemmeligt, og det er meget nemt at skrive regler eller en lov om databeskyttelse, der fremtræder som den bedste i verden. Det er på denne baggrund ikke tilstrækkeligt blot at sammenligne reglerne med direktivets, men det må yderligere tages i betragtning, om det er sandsynligt, at reglerne vil blive overholdt og håndhævet i praksis. Databeskyttelsen må som tidligere fremhævet være mere end »black letter law«, og derfor er velbegrundet tillid til, at reglerne respekteres, i en del tilfælde af meget stor betydning.

Denne del af bedømmelsen beror dermed ikke alene på det databeskyttelsesretlige scenario, men er ligeledes baseret på en oplevelse af eller viden om det pågældende lands retskultur. Vurderingen angår således, om der foreligger en tradition for, at retlige regler overholdes, eller om disse snarere fungerer som en art sminke oven på reelle forhold, der kan være ganske anderledes. Med en anden formulering, om retlige regler opleves som påbud om en bestemt adfærd eller snarere som en opfordring til at udøve denne adfærd. I mange, vel de fleste, tilfælde er denne vurdering ikke vanskelig, selvom man selvfølgelig skal prøve at undgå at blive styret af fordomme. Databeskyttelse er en vesteuropæisk opfindelse, og det er væsentligt at undgå en chauvinisme, hvorefter bestemte landes retlige kultur uden videre ikke accepteres.

Alt i alt kan det fastslås, at ved siden af den formelle retlige vurdering har det ved en bedømmelse af overførselsmuligheder betydning, om der foreligger den nødvendige tillid til tredjelandets retssystem. Der er således også på denne måde en delikat diplomatisk dimension knyttet til vurderingen af tilstrækkelighed. Det kan tilføjes, at tilsvarende vanskelige vurderinger ligeledes aktualiseres ved anvendelsen af en række af de særlige ordninger, der tematiseres i kapitel 6.

11. Undtagelser

Ingen regel uden undtagelse, og dette gælder også i forhold til reglen om, at der ikke må overføres oplysninger til lande, som ikke har et tilstrækkeligt beskyttelsesniveau. Det er blevet betragtet som for vidtgående at fastsætte et absolut forbud imod sådanne overførsler, dels fordi dette ville kunne medføre situationer, som er for upraktiske og for generende i forhold til den internationale handels behov, dels fordi der er tilfælde, hvor det utvivlsomt er i den registreredes interesse, at der kan ske en overførsel. Konsekvenserne forbundet med et absolut forbud ville være vanskelige at overskue. Hertil kommer, at et sådant forbud i realiteten ikke ville kunne håndhæves. På denne bag-

11. Undtagelser

grund er der i direktivets artikel 26(1), jfr. POL § 27(3), fastsat en række undtagelser, som for en dels vedkommende har væsentlig betydning for den private sektor.²⁴

Disse omtales nedenfor, men forinden er det hensigtsmæssigt at angive nogle mere almene kommentarer til, hvorledes undtagelserne fungerer. Som med andre af direktivets bestemmelser er det i første række medlemsstaterne, der skal sikre, at undtagelserne bliver anvendt på en korrekt måde. Det fremgår af artikel 26(1), at staterne ikke er forpligtede til at gennemføre alle de nævnte undtagelser, og der er derfor visse afvigelser mellem de nationale love, idet forskellene dog hovedsageligt er relateret til spørgsmålet om, hvorledes de enkelte undtagelser skal fortolkes og anvendes. Der er bl.a. varierende opfattelser af, i hvilken udstrækning samtykke bør kunne begrunde overførsler, idet der eksempelvis er stor tilbageholdenhed heroverfor i Frankrig, medens opfattelsen er mere liberal i Tyskland. Forskellene er mest udtalte i relation til følsomme persondata.

Uanset sådanne afvigelser er det forudsat, at bestemmelserne bliver anvendt på grundlag af en fælles retsforståelse. Dette mål er dog ikke let at realisere, eftersom det i første omgang er et nationalt anliggende at udfylde og anvende bestemmelserne. Der er som nævnt adgang til i de nationale love at fastsætte fravigelser, hvilket i og for sig er problematisk, fordi sådanne kan forvirre omverdenens opfattelse af EU. Er der ikke sådanne lovbestemte afvigelser, må det således lægges til grund, at artikel 26(1) tager sigte på harmonisering, men det er en udbredt opfattelse, at en sådan harmoni rent faktisk ikke foreligger. Nationale forskelle eksisterer. Under alle omstændigheder er der en risiko for, at der opstår ujævnheder, og at der dermed foreligger forskellige betingelser for de virksomheder, som på dette grundlag ønsker at foretage overførsler. For en koncern med selskaber i flere medlemslande giver sådanne ujævnheder et incitament til at foretage en vis forumshopping.²⁵ Tilbøjeligheden hertil forstærkes af, at direktivet ikke opererer med en one stop ordning således, at hvert lands datatilsyn, afhængig af om der natio-

24. I WP 114 af 25.11.2005 beskrives artikel 26(1) som en art inkonsistens i direktivet, men et sådant perspektiv bortser fra de praktiske behov, som bestemmelsen imødekommer, og som ikke fuldt ud vil kunne tilfredsstilles via de generelle ordninger, der kan fastsættes efter artikel 26(2), jfr. om disse i kapitel 6.

25. Først anvendes princippet om fri overførsel inden for EU til at samle oplysningerne i det for koncernen mest favorable EU-land, hvorefter de eksporteres herfra til tredjelandet. Om denne fremgangsmåde er anvendt, vides ikke, men det er uheldigt, at den er en mulighed. En af direktivets generelle målsætninger er netop at begrænse interessen i forumshopping.

Kapitel 5 Overførsel til tredjelande

nalt er fastsat regler om anmeldelse eller tilladelse, skal involveres, selvom det er de samme datatyper, der eksporteres til det samme tredjeland. Det må alt i alt betragtes som en af svaghederne ved direktivet, at der ikke er tilvejebragt tilstrækkelig enhed på dette område, eftersom den nuværende ordning potentielt kan skade EU's globale omdømme. Denne svaghed beror på, at det ved direktivets gennemførelse var et udbredt ønske i mange medlemsstater at undgå et for harmoniserende direktiv.

Det kan ydermere fremhæves, at der ikke er fastsat en pligt til at give indberetning til Kommissionen når disse undtagelser bliver benyttet,²⁶ idet direktivet ligeledes overlader det til medlemsstaterne at bestemme i hvilket omfang den nationale tilsynsmyndighed skal inddrages. En indberetningspligt til Kommissionen ville være blevet opfattet som bureaukratisk og sikkert også med rette, men konsekvensen af at den ikke er fastsat, er, at Kommissionen ikke har gode muligheder for at sikre, at der ikke opstår store ujævnheder. Det er svært at opnå en tilstrækkelig harmonisering, og på denne baggrund er der i det hele en vis risiko for, at der bliver sendt uklare signaler til tredjelandslande, som kan opleve, at det er nemmere at få overført oplysninger fra en medlemsstat end fra en anden.

Af de her nævnte årsager er det vist nok den almindelige opfattelse, at undtagelsesmulighederne ganske vist ikke kan undværes, men at de bør benyttes i begrænset omfang, og at der så vidt muligt bør iværksættes generelle ordninger, som mindsker behovet for konkrete undtagelser, og dermed samtidig reducerer de ulemper, som er forbundet med den manglende harmonisering jfr. nærmere om disse ordninger i kapitel 6. En restriktiv fortolkning af undtagelserne vil øge behovet for sådanne ordninger.

Artikel 29-gruppen har da også som et almindeligt synspunkt fastslået, at undtagelserne skal fortolkes og anvendes restriktivt, således at de registreres fundamentale rettigheder ikke krænkes. Generelt er gruppen skeptisk i forhold til artikel 26(1), idet det som en væsentlig svaghed fremhæves, at eksportøren ikke har nogen pligt til at sikre, at de overførte oplysninger beskyttes i importlandet, om end den »gode« eksportør bør påtage sig en sådan pligt. Der er således en risiko for integritetskrænkelser forbundet med anvendelsen af undtagelserne, og på denne baggrund bør disse regler kun anvendes, når de med stor grad af sikkerhed omfatter den pågældende overførsel.

26. I det første udkast til direktiv, KOM (90) 314 endl.udg –SYN 287 af 24.9.90 er det i artikel 25 fastsat at Kommissionen og de øvrige medlemsstater skal underrettes med en mulighed for inden for 10 dage at fremsætte indsigelser.

12. De specifikke undtagelser

I modsætning hertil forudsætter de særlige ordninger, der har deres grundlag i artikel 26(2), jfr. POL § 27(4), at der er en beskyttelse i importlandet. Under hensyntagen til denne forskel antager artikel 29-gruppen, at en eksportør først skal vurdere om en af de særlige ordninger, jfr. om disse i kapitel 6, kan anvendes, før det vurderes, om en af undtagelserne kan benyttes.²⁷ Dette beror bl.a. på den opfattelse, at der ved den konkrete anvendelse af en artikel 26(2)-ordning er tilvejebragt et tilstrækkeligt niveau hos importøren. Ud fra direktivet er det dog ikke åbenbart, at den dataansvarlige skal indrette sig ud fra en sådan rækkefølge, og det kan ikke efter min vurdering antages, at en dataansvarlig er forpligtet til at anvende et af de særlige overførselsgrundlag, såfremt en af undtagelserne kan benyttes. Det kan i fortsættelse heraf fremhæves, at rækkefølgen i artikel 26 (stk.1 før stk.2) og starten af artikel 26(2) (»med forbehold af stk.1«²⁸) med styrke taler imod denne opfattelse, der synes at være udtryk for en vis frihåndstegning fra artikel 29-gruppens side. Det vil endvidere uanset den større sikkerhed for integritetsbeskyttelse, som artikel 26(2) ordningerne i almindelighed indebærer, strække princippet om god databehandlingsskik for langt, såfremt et sådant krav blev stillet.

12. De specifikke undtagelser

I det følgende omtales med udgangspunkt i POL § 27(3) de undtagelser, der har betydning for overførsler i den private sektor, idet det kan bemærkes, at personoplysningsloven medtager alle de undtagelser, der er listet i direktivet.²⁹ Det kan i almindelighed fremhæves, at disse regler ikke skelner mellem forskellige oplysningstyper. Som udgangspunkt finder de på tilsvarende måde anvendelse på overførsel af almindelige og følsomme oplysninger, idet det herved er vigtigt at være opmærksom på grundforudsætningen om, at person-databehandlingen nationalt skal være lovlig. Det er en almindelig opfattelse,

27. Jfr. hertil WP 114 af 25.11.2005 p.5 ff. – Mads Bryde Andersen: IT-retten (2.udg. København 2005) p.630-31 synes også at antage, at POL § 27(3) er subsidiær i forhold til § 27(4).

28. Dette er for så vidt endnu tydeligere i POL § 27(4), der indledes med »uden for de i stk.3 nævnte tilfælde«.

29. Christopher Kuner: European Data Privacy Law and Online Business (Oxford 2003) anfører p.126-27, at det ville have været ønskeligt, om en værdispringregel svarende til § 6(1 nr.7) havde været medtaget. Dette ville dog have medført for ubestemte muligheder for overførsler.

Kapitel 5 Overførsel til tredjelande

at undtagelserne skal anvendes særlig restriktivt, når der er tale om følsomme oplysninger, jfr. herved tillige nedenfor under 13.

Det kan endvidere fremhæves, at selvom undtagelserne er udformet således, at de skal være opfyldt i relation til en specifik personoplysning, er det ikke udelukket, at de kan anvendes som grundlag for overførsel af oplysninger om flere registrerede. Den pågældende undtagelse skal blot være opfyldt for alles vedkommende.

Oplysninger kan efter nr.1 overføres, såfremt den registrerede giver et udtrykkeligt samtykke hertil. Kravene til det gyldige samtykke er de samme som på nationalt grundlag, jfr. § 3 nr.8. Samtykket skal således være informeret og specifikt, idet dette betyder, at den registrerede specifikt skal vide, at oplysninger vil blive overførte, til et eller flere bestemte tredjelande. Formålet med den påtænkte overførsel skal også være kendt. Det kan diskuteres, om den dataansvarlige er forpligtet til at informere om retstilstanden eller andre forhold i tredjelandet. Dette er næppe i almindelighed tilfældet, men foreligger der et særligt behandlingsformål tilknyttet den personlige integritet, eller er der tale om et særligt risikabelt tredjeland, kan det følge af princippet om god databehandlingsskik, at en sådan information bliver givet. Det afgørende er, at den registrerede ved, hvad det er, han giver samtykke til, og relevante oplysninger bør derfor ikke skjules. Samtykket skal sædvanligvis indhentes i forbindelse med, at overførslen finder sted. Er al den nødvendige information til stede før det tidspunkt, hvor overførslen er aktuel, vil samtykket kunne gives på dette tidspunkt. Der stilles som sædvanligt ikke formkrav til samtykket, hvilket indebærer, at det også kan gives digitalt; eksempelvis ved et musklik på en hjemmeside. Eftersom den dataansvarlige har bevisbyrden for, at et samtykke er givet, må det frarådes at basere overførslen på et mundtligt samtykke.

Samtykket skal endvidere være frivilligt. Denne betingelse udfyldes ikke strengere end ved national behandling og er derfor i mange tilfælde ikke til hinder for, at samtykke kan anvendes. Da mange overførsler vedrører oplysninger om ansatte, er der grund til at fremhæve, at det netop i ansættelsesrelationen vil være tvivlsomt, om der er den tilstrækkelige frivillighed. Et andet overførselsgrundlag bør normalt foretrækkes³⁰

30. Jfr. WP 114 af 25.11.2005 p.11 samt p.13, hvor der ligeledes udtrykkes tvivl om, hvorvidt ansættelseskontrakten kan udgøre dette alternative grundlag.

Det har i nu snart flere år været overvejet, om der bør udstedes et særligt direktiv eller en rammeafgørelse vedrørende databeskyttelse på arbejdspladser, men indtil videre har disse overvejelser ikke båret frugt.

12. De specifikke undtagelser

Forudsætningen for, at et gyldigt samtykke kan danne grundlag for en overførsel, er på samme måde som for de øvrige undtagelsers vedkommende, at der i det konkrete tilfælde ikke er forhold, der strider mod grundprincipperne i § 5. I Datatilsynets afgørelse af 19.5.2004 vedrørende ansatte revisors samtykke til overførsel af oplysninger til USA som følge af den såkaldte Sarbanes Oxley Act 2002 blev det lagt til grund, at samtykke af denne grund ikke er anvendeligt, da overførslen stred mod § 5(1-3) og i øvrigt anså tvivlsom i forhold til § 5(4-5). Den dataansvarlige må derfor i alle tilfælde foretage en selvstændig vurdering af, om principperne i § 5 er opfyldt.

Samtykket kan til enhver tid tilbagekaldes, jfr. § 38. En sådan tilbagekaldelse har kun virkning for fremtiden og udgør dermed kun en risiko for den dataansvarlige i situationer, hvor samtykket vedrører en løbende overførsel af oplysninger. Tilbagekaldelsen vil ikke have betydning i forhold til en overførsel, der har fundet sted, selvom der kan argumenteres for, at »den gode eksportør« bør søge at udvirke dette, jfr. yderligere nedenfor. Det må i almindelighed antages, at tilbagekaldelsesadgangen ikke yder den samme beskyttelse af den registrerede, som tilfældet er nationalt. Det kan i denne forbindelse specielt overvejes, om en tilbagekaldelse har den konsekvens, at importøren skal stoppe persondatabehandlingen. Dette er næppe tilfældet, selvom behandlingens grundlag i eksportlandet er samtykket, idet oplysningerne nu befinder sig i en jurisdiktion, hvor § 38 ikke gælder. Det kan herved særligt fremhæves, at en overførsel på grundlag af samtykke ikke forudsætter en tilladelse, jfr. hertil under 13, og at det derfor ikke kan fastsættes som et vilkår for overførslen, at et tilbagekaldt samtykke har denne virkning. Det lægges derfor her til grund, at en tilbagekaldelse som udgangspunkt ikke har nogen betydning for persondatabehandlingen i importlandet.³¹ Der kan dog muligvis skelnes mellem den situation, hvor eksportøren fortsat har forbindelse med importøren, og den situation, hvor dette ikke er tilfældet. I den førstnævnte situation kan det være nærliggende at forudsætte, at eksportøren foretager sig noget aktivt med henblik på at sikre, at tilbagekaldelsen får virkninger. En sådan aktivitet vil være udtryk for god skik, selvom der ikke er nogen garanti for, at den bærer frugt.

Det vil ofte være ressourcekrævende og lidet praktisk at basere en overførsel på samtykke fra de registrerede, og i almindelighed kan denne fremgangsmåde ikke antages at være særlig udbredt, når der bortses fra enkeltstående overførsler. I tilfælde, hvor der er en direkte og løbende kontakt mellem

31. I Datatilsynets ovenfor nævnte afgørelse af 19.5.2004 blev det anset for tvivlsomt, om en tilbagekaldelse af samtykket ville få nogen faktiske virkninger.

Kapitel 5 Overførsel til tredjelande

virksomheden og den registrerede, er fremgangsmåden dog anvendelig. Et eksempel kan være tegning af en udenlandsk forsikring via et dansk forsikringsselskab.

Overførsel kan ske, såfremt det er nødvendigt for »opfyldelsen af en aftale mellem den registrerede og den dataansvarlige eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en sådan aftale« (nr.2). Det er således en forudsætning, at den registrerede enten er kontrahent eller forud for aftalen initiativtager. Det må anses forudsat, at den registrerede er bekendt med, at en overførsel finder sted. Det er alene individuelle aftaler, der kan danne grundlag for overførsel. Denne kan således ikke støttes på en kollektiv aftale, f.eks. en overenskomst.

Det er endvidere en forudsætning, at overførslen er nødvendig, hvilket må forstås således, at aftale eller foranstaltning ikke ellers kan gennemføres med en eller anden skadevirkning for den registrerede. Nødvendigheden må således være relateret til aftalen og ikke blot til noget, som er relateret til aftalen som eksempelvis opfølgende markedsføring. Både i forhold til denne bestemmelse og de nedenfor nævnte tillægges det stor betydning i praksis, at nødvendighedsbetingelsen klart er opfyldt, idet artikel 29-gruppen (WP 114) med stor styrke har understreget dette. Den dataansvarlige skal derfor nøje vurdere, om overførslen er nødvendig. Eksempler på denne bestemmelses anvendelse er bestilling af flybilletter eller betalinger foretaget med et internationalt kreditkort. Bortset fra store og vigtige områder som disse antages denne overførselsmulighed i praksis at have et forholdsvis begrænset anvendelsesområde.

For det tredje kan overførsel finde sted, når denne »er nødvendig af hensyn til indgåelsen eller udførelsen af en aftale, der i den registreredes interesse er indgået mellem den dataansvarlige og tredjemand« (nr.3). Som det fremgår, er det her en forudsætning, at overførslen er i den registreredes interesse. Eksempelvis kan der være tale om oplysninger om den registreredes identitet som modtager af en international bankoverførsel. Anvendelsesområdet for denne undtagelse må antages at være begrænset, idet artikel 29 gruppen (WP 114 p.14) i denne forbindelse særligt fremhæver, at der skal udvises tilbageholdenhed ved outsourcing til databehandlere i tredjelande.

For denne og den foran nævnte undtagelse gælder, at deres begrundelse er den registreredes interesse, og at det ville virke tungt og formalistisk, såfremt denne kun kunne varetages via samtykket. Dette vil let kunne resultere i en upraktisk retstilstand. Uanset at samtykke ikke altid udgør nogen garanti i forhold til svage borgere, bør det fremhæves, at det for den registrerede principielt er en svaghed ved aftalegrundlaget i nr.2 og 3, at der ikke her forelig-

12. De specifikke undtagelser

ger en tilbagekaldelsesmulighed, men at dette til gengæld under eksportørens perspektiv tilvejebringer en mere stabil overførselssituation.

Det kan i øvrigt overvejes, om de overførselsmuligheder, der er forbundet med kontrakt, kan finde anvendelse i den situation, hvor der forinden forgæves er søgt indhentet et samtykke. Med andre ord om eksportøren først kan prøve en mulighed for derefter at forsøge sig med en anden. De forskellige overførselsmuligheder, der omtales i dette afsnit, er alternativer, som eksportøren kan vælge imellem, og en sådan fremgangsmåde synes derfor ikke udelukket, selvom der muligvis kunne argumenteres herfor på grundlag af princippet om god databehandlingsskik. Derimod kan der foreligge tilfælde, hvor en overførsel baseret på et nu tilbagekaldt samtykke ikke kan fortsættes på et andet grundlag. Dette gælder dog næppe, såfremt det alternative overførselsgrundlag oprindeligt forelå, og indhentelse af samtykke derfor ikke var påkrævet. Spørgsmålet ses ikke afklaret i praksis.³²

Der kan ske overførsel, såfremt dette er nødvendigt for, »at et retskrav kan fastlægges, gøres gældende eller forsvares« (nr.4).³³ Artikel 29-gruppen (WP 12 p.26) nævner, at denne form for overførsel kan være aktuel i forbindelse med internationale tvister og retssager. Hvornår et retskrav foreligger, afhænger som udgangspunkt af lovgivningen i øvrigt. Bestemmelsen er ikke ganske klar, i den forstand at det især ikke fremgår, om retskravet kan have sin rod i tredjelandets lovgivning. Imod en sådan antagelse taler, at der herved bliver åbnet ukontrollerbare og for tilsynsmyndigheden uoverskuelige muligheder for overførsler, men den omstændighed, at det er en betingelse, at overførslen skal være nødvendig, kan muligvis begrunde, at der kan være tale om retskrav baseret på udenlandsk ret, hvilket synes at kunne udledes af artikel 29-gruppens ovenfor nævnte opfattelse, der har en vis støtte i præambelens betragtning nr.58. Eftersom denne overførselsmulighed må antages at være praktisk vigtig for internationale virksomheder, overvejes spørgsmålet nærmere i det følgende.

Det kan først fremhæves, at bestemmelsen er udformet forskelligt i medlemsstaternes lovgivning, hvilket har en vis interesse for vurderingen af dens omfang. Dette kan skyldes, at direktivets regel er lidt afvigende udformet på

32. Det her angivne svarer til opfattelsen hos Kristian Korfits Nielsen, Henrik Waaben: *Lov om behandling af personoplysninger* (København 2001) p.355-356 i relation til POL § 38.

33. Det kan bemærkes, at denne mulighed først meget sent kom ind i direktivet. Den var således ikke medtaget i andet direktivudkast 1992.

Kapitel 5 Overførsel til tredjelande

de forskellige sprog.³⁴ Ifølge den engelske Data Protection Act 1998 Schedule 4 (par.5) kan der ud over med henblik på retskrav ske overførsel, når dette »is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), og når »necessary for the purpose of obtaining legal advice«. Tilsvarende er fastsat i den irske lov 6/2003 (S 12(4) (a i)). I Finlands lov 523/99 angiver § 23 nr.5 (i engelsk udgave), at overførsel kan ske »for purposes of drafting or filing a lawsuit or for responding to or deciding such a lawsuit«. De fleste medlemsstaternes lovgivning holder sig tæt til direktivets tekst, men de her nævnte bestemmelser giver yderligere grundlag for at overveje problemstillingen. Som det fremgår af de citerede bestemmelser, er den angivne overførselsmulighed ikke udelukkende bundet til begrebet »retskrav«, men de kan alligevel understøtte en mulig udvidet forståelse af dette begreb.

I forhold til national behandling (særlig POL § 7(2 nr.4)) er det sædvanligvis antaget, at et retskrav udelukkende kan udspringe af national ret, der dog ikke omfatter aftaleretlige krav,³⁵ EU retten og internationale konventioner. Det er Kommissionens opfattelse, at dette også er tilfældet ved overførsler, idet det bemærkes at EF Domstolen ikke har udtalt sig om spørgsmålet. I den meget omtalte sag vedrørende overførsel af passagerdata til USA, hvilket nu (indtil videre) er gjort pligtigt, blev spørgsmålet bedømt ud fra, at det ikke var et tilstrækkeligt grundlag for overførslen, at der foreligger et retskrav efter amerikansk ret, jfr. også herved Datatilsynets afgørelse af 10.6.2003 vedrørende SAS.³⁶ I en høringsudtalelse (2003-19-0041) vedrørende en ILO-konvention om identifikationspapirer for søfarende lægger Datatilsynet dog til grund, at en overførsel kan begrundes i de søfarendes retskrav mod udenlandske myndigheder. Datatilsynets praksis er overvejende vendt imod, at

34. På dansk angiver artikel 26(1)d, at overførsel kan ske når »videregivelsen er nødvendig eller følger af lov eller bestemmelser fastsat med hjemmel i lov for at beskytte en vigtig samfundsinteresse eller for, at et retskrav kan fastlægges, gøres gældende eller forsvares«. Reglen indgår uændret i POL § 27. På engelsk fastsætter direktivreglen, at overførsel kan ske når »the transfer is necessary or legally required on important public interest grounds or for the establishment, exercise or defense of legal claims«. Der kan være forskel på hvad der forstås ved »lov« og ved »legally«.

35. Jfr. Betænkning 1345/1997 p.288. Se ligeledes FT 1999-2000 p.4067 vedrørende begrebet »retlig forpligtelse« i § 6(1 nr.3). – I modsat fald ville eksportør og importør på denne måde kunne etablere en hjemmel til overførsel.

36. Grundlaget for kravet er US Aviation and Transportation Security Act of 19.11.2001. Se om denne sags problemstillinger Peter Blume, Ugeskrift for Retsvæsen 2004 p.410-13.

12. De specifikke undtagelser

retskravet kan støttes på udenlandsk ret,³⁷ men der er dog undtagelser fra dette udgangspunkt.

De ovenfor angivne retskilder skal i overensstemmelse med sædvanlig juridisk metode tages i betragtning i den nationale retsanvendelse,³⁸ men dette er ikke nødvendigvis tilfældet i et tredjeland eller internationalt, hvor horisonten er bredere. Det kan her være i modstrid med reglens formål, at eksempelvis en virksomhed, der i Rusland konfronteres med et krav baseret på russisk ret, ikke kan overføre de personoplysninger, der er nødvendige for at forholde sig til dette krav. Afskæring af overførslen vil kunne medføre et retstab for virksomheden. Det bør derfor ikke anses for udelukket, at der kan ske overførsel på grundlag af udenlandsk ret, når det er klart, at en sådan overførsel er nødvendig for, at den dataansvarlige kan gøre sin retsposition gældende.

Spørgsmålet er dog, hvorledes det sikres, at der faktisk foreligger et retskrav. Dette er i princippet et selvstændigt spørgsmål, men det har dog nær sammenhæng med hovedspørgsmålet. Det kan overvejes om dette problem kan løses ved at foreskrive, at kravets mulige eksistens skal fastslås ved anvendelse af reglerne om retsanmodning, jfr. retsplejelovens §§ 190 og 347. Dette vil indebære, at der først over for en domstol i det pågældende tredjeland fremsættes en begæring, hvorefter denne domstol anmoder om overførsel af de pågældende oplysninger, jfr. for Danmarks vedkommende § 342.

Det kan ikke afvises, at en retsanmodning, hvorom der også er fastsat internationale konventioner, vil kunne løse problemet i nogle tilfælde, men fremgangsmåden passer ikke godt til alle foreliggende tilfælde. Det forekommer på denne baggrund ikke givet, at en sådan mellemstation altid er nødvendig, og det konkluderes derfor her, at det ikke kan udelukkes, at fremmed ret, herunder tredjelandets ret, i sig selv kan udgøre overførselsgrundlaget.³⁹ Som ovenfor nævnt kræver denne form for overførsel i en del tilfælde en tilladelse, og det har derfor betydning, at det i Datatilsynets aktuelle praksis antages, at fremmed ret ikke kan begrunde en overførsel. En tilladelse er dermed ikke sandsynlig i dag. Det vil alt i alt være nyttigt, om pro-

37. Dette er også tilfældet i den tidligere nævnte afgørelse af 19.5.2004. – I WP 114 synes man hovedsageligt at tilslutte sig denne opfattelse. Som et eksempel nævnes dog p.15 den situation, at en multinational virksomhed bliver sagsøgt af en ansat i et virksomhedens selskaber i EU, hvor dette begrundes, at virksomheden i tredjelandet er berettiget til at få overført oplysninger om den ansatte, når dette er nødvendigt for at møde dens retskrav. Artikel 29-gruppen er således ikke helt »fast i kødet« i sin regelforståelse.

38. I domstolsprocessen antages normalt, at fremmed ret henhører under faktum, ikke jus.

39. Herved fraviges den opfattelse, jeg hidtil har tilkendegivet, jfr. Databeskyttelsesret p.253, men man har et standpunkt, til man tager et nyt.

Kapitel 5 Overførsel til tredjelande

blemstillingen blev forelagt EF Domstolen, således at der autoritativt blev taget stilling til den.

Af de øvrige undtagelser fra overførselsforbuddet har alene en enkelt en interesse i forhold til den private sektor.⁴⁰ Oplysninger kan således overføres, når det er nødvendigt »for at beskytte den registreredes vitale interesser« (nr.5). Denne regel giver mulighed for overførsler i situationer, hvor den registrerede ikke selv er i stand til at disponere ved at give et samtykke. Hovedeksemplet er tilfælde, hvor den registrerede er blevet syg eller impliceret i en ulykke, og hvor overførsel af medicinske oplysninger er nødvendigt. Der kan også være tale om situationer, hvor den registrerede er blevet bortført e.lign. Bestemmelsens område er de åbenbare tilfælde, og den kan ikke antages at have kommerciel interesse. Den vitale interesse kan således normalt ikke være finansiel, hvilket fremgår af Betragtning 31 i direktivets præambel, hvorefter formålet skal være »at beskytte et hensyn af fundamental betydning for den registreredes liv«.

13. Tilladelse

Der er således muligheder for at foretage konkrete overførsler til lande, der skønnes at have et tilstrækkeligt beskyttelsesniveau, og der er ligeledes fastsat en række regler, hvorefter der kan ske overførsel til lande, der ikke har et sådant niveau. Det er som udgangspunkt den dataansvarlige, som udøver skønnet over, hvorvidt en overførsel, der som fremhævet tidligere også forudsætter, at behandlingen nationalt er lovlig, jfr. præambel Betragtning nr.60, kan finde sted. Dette er ikke altid et nemt skøn at udøve og der er derfor i dansk ret med hjemmel i direktivets artikel 20 fastsat regler hvorefter Datatilsynets tilladelse skal indhentes i tilfælde, hvor der foreligger særlige integritetskrænkelserisici.

Den i personoplysningsloven fastsatte ordning, der ikke på alle punkter er helt let at gennemskue,⁴¹ fremgår af § 50(2), som fastsætter, at når en behandling er omfattet af § 50(1), skal tilsynets tilladelse til overførslen indhentes, når den sker til et land med et tilstrækkeligt beskyttelsesniveau (§ 27(1)), og

40. Af en vis interesse kan muligvis også være reglen i nr.6, hvorefter der kan overføres oplysninger fra registre, der er offentligt tilgængelige eller er tilgængelige for en nærmere i lovgivningen afgrænset kreds. Ifølge præambelens betragtning 58 bør overførslen »ikke omfatte alle oplysninger eller hele kategorier af oplysninger«. I denne bestemmelse stilles der ikke krav om nødvendighed. Dens virkeområde er ikke afklaret.

41. Som det vil fremgå af det følgende, er dette et understatement.

ved utilstrækkelige lande, når grundlaget er kontrakt med den registrerede eller i dennes interesse eller er relateret til et retskrav (§ 27(3) nr.2-4). Tilladelsen og den bagvedliggende stillingtagen fra Datatilsynet vedrører alene grundlaget for overførslen og angår dermed ikke den underliggende nationale behandling, idet en stillingtagen til dennes lovlighed principielt ikke vedrører spørgsmålet om tilladelse i forhold til de særlige overførselsregler skal gives. Der stilles ikke krav om tilladelse når grundlaget er den registreredes samtykke, hvilket kan begrundes med hensynet til selvbestemmelsesretten. Der foretages dermed ikke på denne måde nogen vurdering af, om det pågældende samtykke er gyldigt. Tilladelse er ej heller påkrævet, når overførslen skyldes den registreredes vitale interesse, idet sidstnævnte er rent praktisk begrundet, idet sådanne overførsler sædvanligvis skal ske meget hurtigt.⁴²

Det kan umiddelbart virke mærkeligt, at en tilladelse er nødvendig, når der sker overførsel i medfør af § 27(1), idet denne bestemmelse omfatter lande med et tilstrækkeligt beskyttelsesniveau, og hvor der således ikke foreligger en integritetsrisiko, jfr. ovenfor under 4. Direktivet nødvendiggør ikke et sådant krav, og dette er kun fastsat i nogle af medlemsstaterne. Tilladelseskra­vet er begrundet i hensynet til den dataansvarlige, idet denne kan have vanskeligt ved at overskue, om betingelserne konkret er opfyldt.⁴³ Som fremhævet er dette tit et komplekst spørgsmål. Kravet om tilladelse er derfor ment som en art hjælpeforanstaltning.

I Betænkning 1345/1997 blev der ikke foreslået et tilladelseskra­v i relation til § 27(3), idet det blev lagt til grund, at den dataansvarlige her skal vurdere retlige standarder på samme måde som i forhold til national behandling og ikke vurdere tredjelandet, der jo er kategoriseret som utilstrækkeligt.⁴⁴ Der foreligger således ikke i denne situation de ovenfor nævnte vanskeligheder, idet det på ny kan anmærkes, at den nationale behandling forudsættes at være lovlig. Den gældende ordning blev gennemført som følge af et høringssvar fra Registertilsynet,⁴⁵ hvorefter det ikke blev anset betryggende, at den dataansvarlige skal vurdere, om der kan ske overførsel i forhold til behandlinger, der ikke nationalt er omfattet af anmeldelsespligt. Registertilsynet lagde til

42. Ifølge § 12(4) i Østrigs Datenschutzzgesetz 2000 kan overførsel i dette tilfælde kun ske uden kontakt til tilsynet, når den er hastende, og efterfølgende skal der ske anmeldelse.
– En ordning, hvorefter der efterfølgende skal ske anmeldelse, kunne både i denne og andre situationer tjene det formål at tilvejebringe en større viden om foretagne overførsler, men en sådan ordning kendes ikke i dansk ret.

43. Jfr. Betænkning 1345/1997 p.288.

44. Jfr. Betænkning 1345/1997 p.291 og 507.

45. Høringssvar af 3.2.1998, jfr. FT 1999-2000 Tillæg A p.4032.

Kapitel 5 Overførsel til tredjelande

grund, at dette kunne være acceptabelt ved specifikke regler, men altså ikke ved § 27(3 nr.2-4). Det kan diskuteres, om de øvrige regler i § 27(3) er mere specifikke, idet det eksempelvis ikke altid er åbenbart, at et samtykke er gyldigt, og i og for sig synes betænkningens overvejelse velmotiveret, men resultatet blev altså det gældende tilladelseskrav.⁴⁶

Tilladelseskravet gælder som nævnt kun, såfremt behandlingen er omfattet af § 50(1), idet det her først bemærkes, at dette også er tilfældet, selvom behandlingen i øvrigt i medfør af § 49(1) er undtaget fra det selvstændige tilladelseskrav, der fremgår af § 50(1). I denne forbindelse er der på ny grund til at fremhæve, at det er selve overførslen, der efter § 50(2) forudsætter tilladelse, idet det således efter denne bestemmelse principielt er uvedkommende, om behandlingen nationalt forudsætter anmeldelse eller tilladelse, jfr. i øvrigt nedenfor.

§ 50(1) omfatter en række behandlinger, der kategoriseres som særligt integritetsrisikable. For det første er der tale om behandling af følsomme oplysninger som omfattet af §§ 7(1) og 8(4). Det er i og for sig naturligt, at der må være en særlig sikkerhed for, at sådanne oplysninger, som er specielt integritetsrisikable, ikke overføres til et land, hvor der er risiko for, at de bliver misbrugt, jfr. herved præambelens betragtning nr. 60, der netop særlig fremhæver oplysninger, som er omfattet af artikel 8. En dataansvarlig må således være opmærksom på, om der er tale om oplysninger af denne karakter, og herefter over for tilsynet kunne begrunde hvorfor en overførsel er nødvendig.

For det andet er der efter nr.2 tale om en behandling, hvis formål er at advare andre mod at gøre forretninger med nogen eller ansætte bestemte personer. Der er her tale om det, som traditionelt er blevet betegnet advarselsregistre, og det er værd at være opmærksom på, at disse kan omfatte både persondata og virksomhedsdata, jfr. § 1(3). Selvom der som nævnt sædvanligvis er tale om egentlige registre, og det normalt antages, at enkeltstående (»tilfældige«) videregivelser ikke er omfattet af tilladelseskravet i stk.1, er det dog nærliggende at lægge til grund, at også enkeltstående overførsler med dette formål forudsætter en tilladelse efter stk.2. Udformningen af bestemmelsen i nr.2, »behandlingen af«, taler med en vis styrke for denne fortolkning. Imod står, at der i lovforarbejderne (FT 1999-2000 Tillæg A p.4099) bruges betegnelsen »advarselsregistervirksomhed«, og at der i ældre ret, lov om private registre § 3(6), tales om advarselsregistre.⁴⁷ Direktivet er ikke til

46. Det kan anmærkes, at Registertilsynets ovenfor nævnte synspunkt i og for sig ikke helt er tilgodeset eftersom overførsel i forhold til behandlinger, der ikke kræver tilladelse efter § 50(1), kan ske uden tilladelse, selvom der ikke i øvrigt kræves anmeldelse.

47. Korfits Nielsen og Waaben p.406-07 forudsætter, at der er tale om registre.

megen hjælp, da det ikke specifikt omhandler denne form for behandling. Lovteksten taler dog i hvert fald for, at foretager en dataansvarlig flere behandlinger af denne karakter, må der indhentes en tilladelse, idet formålet bag bestemmelsen også taler herfor. Spørgsmålet er uafklaret, idet der ikke ses at foreligge tilsynspraksis herom.

For det tredje er videregivelse af kreditoplysninger omfattet. Den, der ønsker at drive virksomhed med dette formål, skal nationalt indhente tilladelse hertil, jfr. § 19, der henviser til § 50(1). I disse tilfælde sker der en systematisk videregivelse med dette formål, og da bestemmelsen taler om »erhvervsmæssig videregivelse«, er det nærliggende at antage, at der skal være tale om mere end en enkeltstående overførsel, for at en tilladelse er påkrævet. Ud fra en formålsfortolkning af § 50(2) kan der argumenteres for, at en tilladelse er påkrævet, når der sker flere videregivelser, men også her savnes belysende praksis. Der er grund til at tilføje, at bestemmelsen kun vedrører kreditoplysning og altså ikke omfatter kreditvurdering, medmindre denne er tæt forbundet med kreditoplysningen. Med en anden formulering tager bestemmelsen sigte på importørens grundlag for kreditbeslutninger og vedrører ikke selve beslutningerne.

For det fjerde er behandling med henblik på erhvervsmæssig bistand til stillingsbesættelser omfattet. Der kan være tale om de såkaldte headhunterbureauer. I en vis forstand kan det også her overvejes, om den ikke systematiske overførsel er omfattet, men eftersom der her på samme måde som ved kreditoplysning entydigt er tænkt på virksomheder, der har denne erhvervsprofil, forekommer det mest nærliggende at lægge til grund, at det alene er overførsel fra disse virksomheder, der forudsætter en tilladelse efter stk.2.

Endelig omfatter § 50(1) behandling, der udelukkende tager sigte på retsinformationssystemer. Et eksempel er indlægning af domme i Ugeskrift for Retsvæsen. Umiddelbart kan det måske virke overraskende, at denne behandlingstype er medtaget og dermed kategoriseret som særlig integritetsrisikabel, men dette skyldes, at den er undtaget fra en række af lovens almindelige regler, jfr. § 9. For så vidt angår overførsler må det antages, at tilladelseskra­vet aktualiseres, når modtageren er et retsinformationssystem, der er placeret i et tredjeland.

§ 50(2) er for så vidt en klar bestemmelse, idet overførsel forudsætter tilladelse i forhold til de her nævnte behandlingstyper, idet dette gælder, selv om der ikke er anmeldelsespligt efter § 49(1). I forhold til sidstnævnte må det på ny præciseres, at tilladelseskra­vet alene angår selve overførslen. Det kan dog iagttages, at der ikke i reglen er nogen reference til de behandlinger, der er undtaget fra anmeldelseskra­vet i medfør af bestemmelser udstedt i medfør af § 49(3). Her foreligger bekendtgørelse 534/2000, der har en ganske vidt-

Kapitel 5 Overførsel til tredjelande

rækkende karakter, idet det især kan fremhæves, at det af § 2(1 nr.2) fremgår at for behandlinger, der ikke er omfattet af lovens § 49(1), skal der ikke ske anmeldelse »medmindre der er tale om et edb-register eller manuelt register omfattet af lovens § 50, stk.1«. Systematisk manuel behandling er ligeledes undtaget (nr.3). Det følger af § 50(3), som § 49(3) refererer til, at der kun kan gøres undtagelse fra § 50(1 nr.1) vedrørende følsomme oplysninger,⁴⁸ idet bestemmelsen også nævner § 50(2), jfr. hertil nedenfor.

Der er ikke i bekendtgørelsens regel angivet nogen reservation i forhold til § 50(2), og da § 50(1) alene omfatter anmeldelsespligtige behandlinger, indebærer dette muligvis, hvis sædvanlig juridisk metode benyttes, at det kun for så vidt angår følsomme personoplysninger (§§ 7-8) er ved overførsel af eller fra registre, at der foreligger et tilladelseskrav. Det er en almindelig antagelse, at den teknologiske udvikling har medført, at antallet af registre, der i øvrigt defineres i § 3 nr.3, er reduceret, og at megen persondatabehandling finder sted, uden at denne har sit grundlag i et register. I forbindelse med gennemførelsen af personoplysningsloven var det opfattelsen, at registerbegrebet nu i forhold til ældre ret var henvist til en mere tilbagetrukket position, idet det primært har betydning i forhold til afgrænsningen af, hvilken manuel persondatabehandling der er omfattet af loven. I Datatilsynets praksis antages det vist nok fortsat, at der på samme måde som under registerlovgivningen foreligger et register, såfremt oplysninger behandles systematisk i mere end 30 dage, jfr. herved vejledning nr.37 af 2.4.2001 § 19, men det er lidt svært at finde støtte til et så bredt registerbegreb i direktivet og loven.⁴⁹

Lægges det af Datatilsynet antagne brede registerbegreb til grund, kan det konstateres, at bekendtgørelsen, der for en umiddelbar betragtning nærmest derogerer loven, er knap så vidtgående, som den fremtræder, men man kan desuagtet være lidt i tvivl om, hvorvidt den er fuldt ud gennemtænkt, herunder om det er en lapsus, at der ikke er taget forbehold for § 50(2). Det fremtræder lidt mærkeligt, at overførsel af behandlinger forudsætter tilladelse, selvom behandlingen i øvrigt er undtaget fra anmeldelseskravet efter § 49(1),

48. Jfr. om bekendtgørelsen Korfits Nielsen, Waaben p.403-04.

49. Spørgsmålet er, så vidt det ses, ikke omtalt i forarbejderne. I betænkning 1345/1997 p.51 nævnes 30 dages reglen, men dette sker i afsnittet om dagældende ret med henvisning til ældre registertilsynspraksis. Der findes ikke udtalelser om, hvorvidt denne praksis kan videreføres i forhold til definitionen af et register i direktivets artikel 2 litra c. I denne forbindelse må fremhæves, at registerbegrebet ikke længere har samme fremtrædende betydning som i ældre ret, hvor det i almindelighed tjente til at afgrænse lovens område. – Det bør dog også for en god ordens skyld bemærkes, at det ej heller i folketingsforarbejderne (FT 1999-2000), så vidt det ses, er anført, at det ældre registerbegreb i denne henseende ikke skulle videreføres.

medens dette ikke er tilfældet for de behandlinger, der er omfattet af den nævnte bekendtgørelsesregel og dermed ikke skal anmeldes. Det er ikke åbenbart, at overførsel af følsomme oplysninger, der ikke er baseret på en af de behandlingssituationer, der er medtaget i § 49(1), er mindre integritetsrisikabel end disse behandlinger, blot fordi der ikke foreligger et register. Dette synes dog at være den ordning, bekendtgørelsen angiver.

Det her anførte er ikke nødvendigvis udtryk for gældende ret. Ifølge § 50(3) kan der som nævnt fastsættes undtagelser fra § 50(2), og det er muligt, at der i bekendtgørelsen fastsættes sådanne undtagelser. Det er i dennes § 2(2-3) vedrørende oplysninger om ansatte præciseret, at dette ikke er tilfældet, hvorfor dette med en modsætningsslutning kunne antages at være tilfældet i stk.1(nr.2 og 3). Måske! Den fastsatte ordning er, uanset at bekendtgørelsen bl.a. har hjemmel i § 50(3), der muliggør undtagelser fra § 50(2), i det hele svær at forstå for så vidt angår følsomme persondata. I almindelighed medfører bekendtgørelsen, at en i forvejen svært gennemskuelig ordning yderligere kompliceres. Det er ønskeligt at overveje denne regulering på ny og, når loven en dag skal revideres, at fastsætte en klarere ordning⁵⁰. Dette er muligt, eftersom direktivet kun fastsætter få bindinger for medlemsstaterne i henseende til anmeldelses- og tilladelsesordningen.

I de tilfælde, hvor en overførsel forudsætter en tilladelse, kan Datatilsynet betinge denne af, at bestemte vilkår bliver opfyldt, jfr. § 50(5). Der er i praksis tale om standardvilkår, som tilpasses den konkrete situation. Formålet er at sikre, at overførte data behandles betryggende, og de fastsatte vilkår kan ofte indebære, at den dataansvarlige eksportør skal forpligte importøren til at gennemføre bestemte foranstaltninger. På denne måde kan de betænkeligheder i forhold til anvendelsen af artikel 26(1), som artikel 29-gruppen har tilkendegivet, jfr. foran under 11, til en vis udstrækning imødekommes. Der foretages ved vilkårsfastsættelsen en specifik vurdering, hvor der bl.a. som særligt fremhævet i § 29 i den norske personoplysningslov (nr.31 af 14.4.2000) kan tages hensyn til behandlingens varighed i tredjelandet, jfr. direktivets artikel 25(2). Der kan ligeledes stilles vilkår, som vedrører selve overførslen, idet disse typisk vil have karakter af sikkerhedskrav. Adgangen til at stille vilkår giver mulighed dels for at oparbejde en differentieret praksis, dels for at der, inden en tilladelse gives, kan være en dialog mellem tilsyn

50. Selvom det sikkert fremgår af teksten, kan jeg ikke undlade at bemærke, at denne regulering har givet anledning til meget hovedbrud og mange revisioner af teksten under bogens udarbejdelse. Jeg kan kun håbe, at den nu er udtryk for gældende ret!

Kapitel 5 Overførsel til tredjelande

og eksportør, som kan tilvejebringe et bedre grundlag for overførslen. For tilladelsen betales et gebyr på 1.000 kr., jfr. § 63(2).⁵¹

En tilladelse er en begunstigende forvaltningsakt, og efter sædvanlig retsopfattelse er det ikke muligt at tilbagekalde en sådan. Datatilsynets praksis er tilrettelagt inden for de rammer, der følger af Kommissionens opfattelse af de forskellige tredjelandes status og af, under hvilke betingelser overførsel kan ske. Dette indebærer, at der, efter at en tilladelse er givet, kan blive truffet en EU-afgørelse, som indebærer, at overførslen ikke kan finde sted. På denne baggrund er det i § 58(2) fastsat, at tilsynet kan tilbagekalde en tilladelse, idet dette udelukkende kan ske, »såfremt tilbagekaldelsen er nødvendig for at efterleve Kommissionens afgørelse«. Dette vil være en sjældent forekommende situation, og der findes endnu ikke i praksis eksempler herpå.

14. Behovet for alternativer

Hermed er omtalen af den almindelige regulering af adgangen til at overføre persondata til tredjelande afsluttet. Det er konstateret, at der er tale om en regulering, som tilstræber at forebygge, at der ved overførsler opstår situationer, der underminerer det beskyttelsesniveau, som er fastlagt i EU. Det er konstateret, at denne ordning bliver taget alvorligt i den forstand, at der kun i begrænset omfang indgås kompromiser eller accepteres undtagelser. Denne kurs har undertiden betydet, at reguleringen er blevet angrebet for at etablere et fort Europa og for ikke at være tilstrækkelig lydhør over for de kommercielle behov, som begrunder, at der skal kunne ske dataoverførsler. Reguleringen er blevet karakteriseret som virkelighedsfjern. Kritik af denne karakter peger på et behov for andre retlige grundlag for overførsler end dem, der er beskrevet i dette kapitel. Et behov for supplerende generelle ordninger. Et behov, som ikke er udelukket af direktivet. Regulering, der søger at imødekomme dette behov, er temaet i næste kapitel.

51. Der opkræves ikke gebyr for behandlingen af ansøgningen, og der skal således ikke betales et gebyr, såfremt tilladelse ikke opnås.

KAPITEL 6

Særlige overførselsgrundlag

1. Det økonomiske overførselsbehov

I det moderne internationaliserede informationssamfund foreligger der et betydeligt økonomisk behov for at kunne udveksle personoplysninger på tværs af landegrænser. En retlig ordning, der restriktivt begrænser eller udelukker en sådan udveksling, må under dette perspektiv betragtes som irrationel og uønskelig, idet dette i og for sig også gælder ud fra de registreredes gennemsnitlige interesse samt samfundets interesse i et velfungerende erhvervsliv. Under det erhvervsmæssige perspektiv er det ønskeligt, at der ved overførsler tages hensyn til privatlivsbeskyttelse, eftersom en sådan hensyntagen kan betragtes som en del af moderne corporate governance og yderligere understøtter gode relationer til kunder og ansatte, men det er lige så ønskeligt, at dette hensyn tages på en sådan måde, at almindelig moderne erhvervsmæssig virksomhed kan finde sted. Det er således uønskeligt, at der sker en restriktiv begrænsning af de datastrømme, som udgør et afgørende fundament for den moderne handel. Hensynet til databeskyttelse bør ikke unødigt begrænse den dynamik, som internationaliseringen indebærer.

Under dette perspektiv er det ligeledes uhensigtsmæssigt, såfremt der etableres en retstilstand, der indebærer, at EU på dette område bliver en isoleret ø i forhold til resten af verden. Denne opfattelse er ikke nødvendigvis ensbetydende med en kritik af den gældende EU-retlige regulering. Den kan sagtens betragtes som fremsynet, og den beskyttelse, borgerne gives, kan vurderes som berettiget og fornuftig. Det er snarere reguleringens aktuelle virkninger, der kan give anledning til betænkeligheder under et erhvervsmæssigt perspektiv. Det er problematisk, at der er opstået en global retlig ujævnhed, der ganske vist måske under et langt tidsperspektiv vil forsvinde, jfr. i kapitel 8, men som på nuværende tidspunkt kan medføre en blokering af den

Kapitel 6 Særlige overførselsgrundlag

dataudveksling, der er nødvendig i den internationale handel i bred forstand.¹ Den databeskyttelsesretlige regulering vil kunne bremse den økonomiske vækst og dermed være skadelig også for borgerne i EU's medlemsstater. Der foreligger dermed en overordnet interesse i, at sådanne konsekvenser søges undgået eller i hvert fald begrænset.

Som det fremgår, foreligger der en økonomisk orienteret argumentation, der med styrke taler for, at der må være flere muligheder for dataoverførsler end dem, som umiddelbart følger af den almindelige regulering, der er beskrevet i kapitel 5. Dette er en argumentation af en betydelig tyngde, og den er bakket op af stærke erhvervsmæssige interesser. Hertil kommer, at det ikke i almindelighed er databeskyttelsesrettens intention at blokere legitim international erhvervsmæssig aktivitet. Målet er blot, at denne aktivitet skal være civiliseret. Fra denne side af gærdet er der således en accept af, at der søges udviklet ordninger, som skaber yderligere muligheder for dataoverførsler. Disse muligheder kan dog ikke være ubegrænsede, idet det må fastholdes, at beskyttelsen vedrører borgernes grundlæggende rettigheder, og disse rettigheder må derfor fortsat være i fokus i den samlede regulering. Dette er dog ikke til hinder for, at der kan gennemføres bestemte ordninger, som på dette grundlag forbedrer overførselsmulighederne. I direktivet er der åbnet mulighed for, at sådanne ordninger kan realiseres, jfr. nærmere herom nedenfor.

2. Særlige ordninger

EU har været villig til respondere på det erhvervsbetonede pres og medvirke til at udvikle særlige ordninger, der øger overførselsmulighederne. Når bortses fra en enkelt af disse, Safe Harbor, der repræsenterer en speciel anvendelse af artikel 25(1), jfr. nedenfor under 11, er disse ordninger kommet til verden efter et positivt udviklingsforløb, hvor de interesserede erhvervskredse har haft mulighed for at sætte deres præg på resultaterne. Som det vil fremgå af den nedenfor givne beskrivelse, kan det i en del tilfælde diskuteres, hvor stor en afvigelse fra direktivets almindelige regler disse ordninger egentlig indebærer, idet der i betydeligt omfang snarere er tale om anvendelse af en

1. Forventninger om, at mange lande ville tilpasse deres nationale lovgivning til direktivets niveau, er indtil videre gjort til skamme. Som nævnt i kapitel 5 er kun ganske få lande indtil videre anerkendt som havende et tilstrækkeligt beskyttelsesniveau, jfr. yderligere nedenfor under 3.

2. Særlige ordninger

anden retlig form end et andet retligt indhold, men der er dog ikke tvivl om, at disse ordninger samlet indebærer en vis udvidelse af overførselsmulighederne. Ordningerne er da også i almindelighed blevet positivt modtaget. De tilvejebringer specielt et bedre grundlag for dataoverførsler i kommercielle arm-length transaktioner.

Betragtes de gennemførte ordninger, synes der i hvert fald at foreligge to typer. Inden disse udredes, skal det først erindres, at i alle tilfælde forudsætter overførslen, at der nationalt foreligger en lovlig behandling. Den eksportende virksomhed må lovligt være i besiddelse af de personoplysninger, der ønskes overført, og de hermed korresponderende behandlingsskridt må lovligt kunne foretages. Denne almindelige forudsætning er således ikke fraveget i disse særordninger, og dette må selvsagt tages i betragtning ved den samlede vurdering af den enkelte ordning.

Den første type af generelle ordninger karakteriseres ved, at der for den enkeltstående overførsel etableres en særlig ramme. Hovedeksempler her er kontraktregulering og bindende virksomhedsregler. Anvendelsen af sådanne ordninger kendetegnes ved, at en tilpasset udgave af direktivet trænger ind i et ikke tilstrækkeligt tredjeland, idet der etableres en regulering, hvorefter der et bestemt sted i dette tredjeland, hos den konkrete importør, etableres en retstilstand, der under det EU-retlige perspektiv er acceptabel. I en vis forstand kommer EU-retten herved ind ad bagdøren, og disse ordninger kan dermed også beskrives som en form for retseksport. Dette kan betragtes som et generelt plus ved disse ordninger, eftersom de kan udbrede den opfattelse og erfaring, at en regulering, der i hvert fald minder om direktivets, kan fungere på en hensigtsmæssig måde, og dermed kan disse ordninger på længere sigt understøtte almindelige ændringer af tredjelandets retlige regulering. Der kan i disse lande opstå et forstærket pres i retning af, at der gennemføres ændringer af den almindelige lovgivning, således at virksomhederne ikke skal anvende de ressourcer, som er forbundet med den konkrete etablering af disse ordninger. Om man vil, er der tale om en snedig form for retsimperialisme, jfr. dog nedenfor under 3, hvor det her angivne modificeres. Denne fremgangsmåde er dog ikke i alle henseender problemfri, og som der redegøres for nedenfor, er et hovedspørgsmål at sikre, at importøren faktisk behandler de overførte data i overensstemmelse med den pågældende ordning.

Den anden type, som indtil videre alene repræsenteres af Safe Harbor, karakteriseres ved reelt at være en generel undtagelse fra eller nok snarere modifikation af direktivets ordning. En sådan reguleringsmodel er ikke direkte relateret til specifikke overførsler, men angiver derimod, at en virksomhed omfattet af denne model, kan der ske overførsel på grundlag af de særlige regler, som ikke fuldt ud svarer til direktivets. Der er således her tale om

Kapitel 6 Særlige overførselsgrundlag

ordninger, som kan medføre en almindelig udtynding af direktivet, hvorfor det da heller ikke er sandsynligt, at der vil opstå flere end den ene, der er gennemført. En sådan ordning kan da også opfattes som retsimperialisme vendt mod EU.

3. Direktivets globale virkning

De forskellige ordninger indebærer en smidiggørelse af direktivets almindelige regulering, og som anført indledningsvis foreligger der stærke økonomisk orienterede argumenter for at dette sker. Selvom dette er tilfældet, er der ikke nogen grund til at skjule, at disse ordninger indebærer en begrænsning af de generelle aspirationer, som EU har på dette område. Selvom aspirationen måske aldrig har været helt åbent formuleret, er der ikke tvivl om, at direktivet fra begyndelsen er blevet opfattet som den rigtige måde at beskytte personoplysninger på, og intentionen var således, at direktivet skulle fungere som et forbillede for den øvrige verden. Håbet har været, at mange tredjelande ville ændre deres lovgivning i retning af den regulering, som direktivet angiver, og at dette efterhånden kunne blive den globalt virkende norm. I nogle henseender har dette været et lidt naivt håb, som har overvurderet den rolle, som EU spiller globalt, men direktivet har nogle steder haft denne virkning. I forhold til den private sektor er Canada et godt eksempel på, at direktivet har indvirket på national lovgivning.

Uanset det under 2 anførte kan de generelle ordninger i relation til mange tredjelande reducere sandsynligheden for, at der på et senere tidspunkt sker sådanne reguleringsændringer. Dette skyldes, at en væsentlig årsag til at foretage sådanne ændringer er at der foreligger overførselsproblemer. Det pågældende land føler sig lukket ude og dets regering presses af erhvervslivet, hvis indtjeningsevne trues. Bliver det lettere at foretage overførsler, forsvinder denne motivationsfaktor, og den nationale retskultur kan forblive uantastet. Selvom hovedparten af de ordninger, der beskrives i dette kapitel, må vurderes positivt og ikke alvorligt antaster databeskyttelsesniveauet som determineret i EU, kan de på denne baggrund under et langsigtet perspektiv have en uheldig virkning i forhold til etableringen af en harmoniseret global databeskyttelsesretlig orden, jfr. herved drøftelsen af mulighederne herfor nedenfor i kapitel 8.

4. Virksomhedstyper

Forinden de forskellige modeller nærmere omtales, er det hensigtsmæssigt at karakterisere de typer af virksomheder, som disse ordninger tager sigte på. Der findes som bekendt mange forskellige typer af virksomheder, og principielt kan alle drage nytte af de forskellige ordninger. Det kan ligeledes være forskelligartede formål, som begrunder, at der foreligger et overførselsbehov, som ikke uden videre kan honoreres af de almindelige regler.

På denne baggrund er det hensigtsmæssigt at angive visse kategoriseringer og især foretage en opdeling mellem den enkeltstående virksomhed, enheds-selskabet med filialnet og koncernvirksomheden, idet det tilføjes, at den følgende udbygning af denne opdeling selvsagt er udtryk for gennemsnitsbetragtninger. Denne opdeling kan benyttes på tværs af brancheområder og konkrete overførselsbehov.

Ved en enkeltstående virksomhed forstås her en virksomhed, der ikke har nogen konstant retlig eller organisatorisk forbindelse med den virksomhed, til hvilken der ønskes overført personoplysninger. Behovet opstår i forbindelse med en bestemt erhvervsmæssig aktivitet. Man kan tale om singulære overførsler, der i en vis forstand er de mest krævende, eftersom eksportørens kendskab til importvirksomhedens rutiner kan være lavt, hvorved det kan være vanskeligt at sikre, at aftalte spilleregler bliver overholdt. Virksomheder af denne karakter kan ligeledes have få eller ingen erfaringer med hensyn til internationale relationer, og ligeledes af denne grund kan det være ressourcemæssigt krævende at etablere overførselsgrundlaget. Det kan bl.a. være påkrævet at sikre sig en særlig udbygget dokumentation, der beskriver de fastlagte betingelser for, hvorledes importøren skal behandle de overførte personoplysninger. Det er ligeledes nødvendigt at have stærke instrumenter, der sikrer, at betingelserne faktisk vil blive respekteret.

Et internationalt enhedsselskab er retligt organiseret således, at der er etableret afdelinger eller filialer i mange lande. Disse afdelinger er således ikke selvstændige virksomheder, selvom de i mange tilfælde vil være omfattet af den databeskyttelseslovgivning, der gælder i den medlemsstat de er etableret i, jfr. POL § 4(1).² Overførselsbehovet vil her være relateret til cirkulation af oplysninger mellem de forskellige afdelinger eller til samling af oplysningerne et sted i selskabet. Det er således karakteristisk, at dataoverførslen sker

2. Se foran i kapitel 1. – Som det fremgår senere i kapitlet, tager de beskrevne ordninger sigte på overførsler til tredjelande, men de kan også have betydning for virksomheder, der er spredt i flere EU-lande, jfr. især under 15.

Kapitel 6 Særlige overførselsgrundlag

inden for den retlige enhed, der udgøres af selskabet, og dermed blandt kendte parter, der kan underlægges fælles spilleregler. Der foreligger et praktisk anvendeligt fundament, og der er behov for en retlig mekanisme, som på dette grundlag gør sådanne overførsler mulige.

Det internationale selskab kan også være struktureret som en koncern med den konsekvens, at de enkelte virksomheder nok er forbundne, men formelt, vistnok i de fleste retssystemer, er selvstændige. Her kan der ligeledes foreligge et behov for datacirkulation mellem koncernvirksomhederne eller en samling af data, og situationen minder således om enhedsselskabets.³ De retlige mekanismer, som skal gøre dataoverførslen mulig, er dog grundet den forskelligartede retlige udgangsposition ikke nødvendigvis de samme.

Hverken enhedsselskabet eller koncernen orienterer sig mod landegrænser, men mod funktionelle grænser. Begge virksomhedstyper kan naturligvis på samme måde som det enkeltstående selskab ligeledes have singulære relationer til eksterne virksomheder. Ved vurderingen af den konkrete overførselssituation er det på denne baggrund væsentligt at skelne mellem, om denne skal foregå »inden for« eller uden for virksomheden. Dette er ikke en opdeling, der kan genfindes i direktivet eller personoplysningsloven, men en opdeling, som kan tillægges en vis betydning ved vurderingen af, om en overførsel, der ikke kan hjemles i de almindelige regler, må anses for betryggende. Den har betydning for vurderingen af, om en fastsat ordning kan forventes respekteret i praksis, hvilket svarer til de overvejelser, der er aktuelle ved vurderingen af vilkårfastsættelse i forbindelse med overførsel på grundlag af de almindelige regler, jfr. foran i kapitel 5.

Den nævnte opdeling mellem virksomhedstyper har ligeledes i det hele betydning for, i hvilken udstrækning det er muligt at udforme særlige overførselsgrundlag, som tilstrækkeligt tager hensyn til de relevante virksomhedsbehov, og som derfor konkret kan finde anvendelse.⁴

3. Som det nævnes senere i kapitlet, er koncernbegrebet ikke entydigt under et internationalt perspektiv. Det anvendes både om løse sammenslutninger af virksomheder og om selskaber, der står i en tæt organisatorisk forbindelse. Her er tænkt på sidstnævnte.
4. I denne forbindelse kan fremhæves, at det i forhold til fastsatte forpligtelser har betydning, at importøren har en selvstændig tilværelse og ikke blot er underleverandør i forhold til den egentlige importør.

5. Formål

Overførsels formål kan også spille en vis rolle ved vurderingen af, om et særligt overførselsgrundlag kan anvendes. Denne bog tager primært sigte på overførsler, der har et kommercielt formål, men dette er ikke en helt entydig størrelse, men kan tværtimod dække over mange forskellige situationer. Eksempelvis kan der skelnes mellem formål, som er forbundet med gennemførelsen eller fastholdelsen af en bestemt økonomisk relation, og heroverfor formål, der snarere er relateret til produktudvikling i en ny kontekst. I almindelighed vil der kunne ske overførsel i alle tilfælde, hvor formålet kan betragtes som legitimt og dermed danner grundlaget for en saglig persondatabehandling. Det præcise formål kan have betydning for udformningen af overførselsgrundlaget, idet formålet indikerer hvorledes oplysningerne vil blive anvendt af importøren.

En hensyntagen hertil kan være særlig relevant, såfremt formålet indebærer en bestemt form for persondatabehandling, der er underlagt en speciel databeskyttelsesretlig regulering i eksportlandets ret. Et eksempel kan være overførsel af oplysninger, der indgår i forskningsprojekter med et kommercielt potentiale, hvor der i henseende til følsomme data er fastsat en særregulering vedrørende national behandling i POL § 10. Ved vurderingen af om de særlige overførselsmuligheder kan anvendes, får det i sådanne situationer speciel betydning om behandlingen hos importøren kan modsvare de særlige krav, der stilles i den nationale lovgivning. Dette kan medføre, at Datatilsynet stiller bestemte vilkår for at acceptere overførslen.

6. Oplysningstypen

Der indgår således alt i alt en række parametre når det skal vurderes, om en overførsel kan finde sted på et særligt grundlag. Sidst i denne opregning er det naturligt at nævne, at det spiller en væsentlig rolle, hvilken type personoplysninger der er tale om. Som nævnt i kapitel 5 er Datatilsynet i forhold til de almindelige former for overførsel tillagt en tilladelseskompetence i forhold til følsomme data, og det er naturligt at der ved udøvelse af den tilsvarende kompetence i forhold til særlige ordninger anlægges en forsigtig kurs. Når der foreligger størst risiko for integritetskrænkelser, må der tilsvarende være størst sikkerhed for, at de overførte personoplysninger bliver behandlet betryggende. Dette taler for, at der i særlige ordninger er indbygget regler specielt med henblik på følsomme persondata.

Kapitel 6 Særlige overførselsgrundlag

Selvom der naturligt må være størst fokus på de følsomme persondata, har det i det hele taget, på tværs af lovgivningens kategoriseringer, betydning, hvilke oplysninger der påtænkes overført, og for anvendelsen af de særlige overførselsgrundlag er det nødvendigt, at eksportør og importør indretter sig ud fra, hvilke oplysningstyper der konkret ønskes overført. Dette har betydning for den del af de særlige overførselsgrundlag, der udfyldes af de implicerede parter, jfr. yderligere nedenfor.

7. Særordninger kan tillades

I dansk ret er det formelle udgangspunkt POL § 27(4), der implementerer direktivets artikel 26(2 og 3). Ifølge denne bestemmelse kan Datatilsynet tillade, at der sker en overførsel, »såfremt den dataansvarlige yder tilstrækkelige garantier for beskyttelse af de registreredes rettigheder«. En sådan tilladelse kan ledsages af vilkår, og gives den, skal tilsynet underrette Kommissionen og de øvrige medlemsstater.⁵ Dette giver staterne mulighed for at fremsætte indsigelser, og det giver Kommissionen mulighed for at træffe afgørelse om, at overførslen ikke må ske. Såfremt en sådan beslutning træffes, er der, som også nævnt i kapitel 5, i § 58(2) tilvejebragt hjemmel til, at tilsynet kan tilbagekalde sin tilladelse, selvom der er tale om en begunstigende forvaltningsakt. Der findes endnu ikke eksempler herpå i dansk ret.

Det er ikke i § 27(4) nærmere angivet, hvilke ordninger der kan danne basis for en sådan tilladelse og med forbehold for underretningsforpligtelsen udøver tilsynet således et frit skøn. Underretningsforpligtelsen indebærer som nævnt, at de øvrige medlemsstater vil blive bekendt med anvendelsen af særegne grundlag, hvilket i givet fald sandsynligvis vil danne grundlag for en drøftelse i artikel 29-gruppen. Så vidt vides er der dog ikke eksempler på nationale afvigelser i forhold til de retsformer, der kan begrunde en overførsel.

I almindelighed er det ikke overførslens retlige form, men dens grad af overensstemmelse med loven (direktivet) og dens pålidelighed i henseende til efterlevelse og håndhævelse, der er afgørende for, om der kan gives tilladelse. Det kan yderligere lægges til grund, at det er den dataansvarlige, som skal kunne dokumentere, at det er betryggende set under de registreredes perspek-

5. Underretning kan næppe antages at være påkrævet i de tilfælde, hvor tilladelsen gives på grundlag af en uændret anvendelse af de af Kommissionen godkendte standardkontrakter, jfr. om disse nedenfor under 11-13.

tiv, at der gives en sådan tilladelse. Det skal godtgøres, at der ikke ved overførslen udløses en risiko for integritetskrænkelser. Nogle af de retlige instrumenter, der omtales nedenfor, tager sigte på at lette denne dokumentationsbyrde, der kan være krævende for den dataansvarlige.

8. Adfærdskodekser

Anvendelse af former for selvregulering er velkendt i erhvervslivet. Selvregulering indebærer i almindelighed, at de, som skal være retligt forpligtet, selv fastsætter de regler, som de er forpligtet over for, jfr. yderligere nedenfor. Der kan være tale om regulering, der gælder for en bestemt virksomhed eller gruppe af virksomheder, eller regulering, som omfatter en branche. Selvregulering kan antage mange former, idet der bl.a. kan være tale om adfærdskodekser (»codes of conduct«) eller erklæringer vedrørende databeskyttelse (»privacy statements«). Sådanne tilkendegivelser kan være udformet af den pågældende virksomhed selv, men der kan også være tale om at virksomhed tilslutter sig et selvreguleringsprogram⁶ og af dette bliver certificeret som medlem. Der er i princippet ikke grænser for variationsbredden⁷. Grundlæggende er selvregulering baseret på den opfattelse, at en sådan regulering kan tilpasses de særlige omstændigheder i en virksomhed eller branche, og dermed realisere de retlige mål på en måde, som bedrer stemmer overens med de faktiske forhold end tilfældet er ved en lov, der skal dække mange forskellige brancheområder.

Sandsynligheden for, at de fastsatte bestemmelser bliver overholdt, er som udgangspunkt stor, idet reglerne er fastsat af de forpligtede eller med disses tilslutning, hvorved der foreligger en tilkendegivelse om, at reglerne vil blive respekteret. Der er en formodning for, at sådanne regler vil blive betragtet som fornuftige og praktiske. Umiddelbart kan denne antagelse om regelaccept forekomme overbevisende, men det må anmærkes, at der i praksis ganske hyppigt forekommer tilfælde, hvor reglerne alligevel ikke overholdes. Dette kan skyldes, at de ansatte i en selvreguleret virksomhed ikke er blevet tilstrækkeligt uddannet i disse regler og derfor ikke er tilstrækkelig opmærksomme på disse, men det kan også bero på, at det slet ikke har været intentionen, at reglerne skulle overholdes, idet disse blot er blevet udformet med

6. Eksempler på sådanne programmer særligt relateret til Internettet er Trust.e (startet 1997) og BBB-online (startet 1999). Begge ordninger omfatter mekanismer, hvor de tilsluttede virksomheder accepterer kontrol med at de overholder de fastsatte regler.

7. Se om selvregulering WP 7 af 14.1.1998.

Kapitel 6 Særlige overførselsgrundlag

henblik på at give virksomheden et godt image. Adfærdskodeksen benyttes af virksomheden som en art slør. Der er derfor grund til en vis forsigtighed med at anvende selvregulering som grundlag for databeskyttelse, herunder overførsler, men at sådanne tilfælde foreligger, indebærer dog ikke, at dette er udelukket, og en sådan regulering kan i nogle situationer være den bedst egnede.

Adfærdskodekser kan i nogle tilfælde være velegnet instrument i databeskyttelsesretten. I forhold til overførsler er det dog et problem, at mange kodekser er nationale og ikke har det fornødne internationale præg, således at både eksportør og importør med sikkerhed er omfattet. Selvregulering kan desuagtet danne basis for tilladelser efter § 27(4), hvilket er i god overensstemmelse med princippet i § 27(2), hvorefter alle former for regulering skal tages i betragtning, når det vurderes, hvorvidt en overførsel er betryggende. Afgørende for, om en tilladelse kan gives, er dels kodeksens indhold set i forhold til direktivet, dels dens gennemskuelighed. De fastsatte mekanismer til konflikthåndtering tillægges ligeledes væsentlig betydning, idet sanktioneringen af regelbrud ofte er et svagt punkt i forbindelse med selvregulering. Det er svært at sikre sig, at den enkelte dataansvarlige faktisk håndhæver disse regler og så at sige ikke overlader de registrerede til at klare sig selv.

Ved siden af de opdelinger, der er foretaget ovenfor, kan der skelnes mellem selvregulering, der er fritstående i den forstand, at der ikke findes anden databeskyttelsesretlig regulering, og heroverfor selvregulering, som supplerer eller udfylder en allerede foreliggende regulering og derved har til formål at præcisere dennes retlige standarder i forhold til et bestemt erhvervsområde. I medlemsstaterne har selvreguleringen den sidstnævnte karakter. Disse typer af kodekser har et støttepunkt i artikel 27, der er implementeret i POL § 74, hvorefter der i samarbejde med Datatilsynet kan udarbejdes »adfærdskodekser, der skal bidrage til en korrekt anvendelse af reglerne i denne lov«. Intentionen er først og fremmest, at tilsynet skal sikre, at der ikke i en kodeks indgår regler, som strider imod loven, herunder princippet om god skik. Der findes endnu ikke kodekser udarbejdet efter proceduren i § 74, men der er ikke tvivl om, at sådanne ville kunne udgøre et særligt sikkert grundlag for tilladelser til overførsler.⁸ Andre kodekser kan dog også udgøre dette grundlag, og i praksis er der givet enkelte tilladelser.

8. På europæisk niveau findes for tiden to adfærdskodekser. IATA har fastsat regler vedrørende håndtering af persondata i international luftfart, jfr. hertil WP 49/2001, og FEDMA har udformet en kodeks, der tager sigte på brug af persondata til markedsføringsformål, jfr. hertil WP 77/2003. Tilslutning til kodekser af denne karakter udgør et positivt moment i henseende til vurderingen af, om en dataoverførsel skal tillades.

Som nævnt foreligger der usikkerhedsmomenter, hvorfor det ud over selvreguleringens indhold spiller en rolle om der er tilstrækkelig tillid til at eksportøren kan og vil sikre, at de fastsatte regler overholdes. Det har herved betydning, om eksportøren er en kendt aktør på markedet. Formodningen for, at reglerne faktisk vil fungere bestyrkes som ovenfor fremhævet, såfremt der er tale om en international kodeks, som også importøren har tilsluttet sig. En yderligere sikkerhed kan som nævnt opnås ved, at overførslen ud over at være i overensstemmelse med kodeksen skal opfylde særlige vilkår, herunder at ændres kodeksen, må der ikke ske overførsler, inden en fornyet tilladelse er givet. Vilkår fastsat af Datatilsynet kan dermed bevirke, at kodeksen bliver et egnet overførselsgrundlag.

Sammenfattende kan selvregulering i form af kodekser mm. danne grundlag for overførsler, men denne metode er krævende både for den dataansvarlige og for Datatilsynet, der skal foretage en individuel bedømmelse, som kan være ganske vanskelig, bl.a. fordi den forudsætter kendskab til bestemte brancheforhold. Der kan være tale om en besværlig og langsommelig proces, hvilket forklarer, hvorfor især singulære kodekser sjældent bliver anvendt, jfr. om en tilsvarende problemstilling under 15. Dette er ligeledes årsagen til, at mere generelle ordninger er søgt tilvejebragt.

9. Kontrakt

I erhvervsmæssige sammenhænge er den mest anvendte retlige reguleringsform kontrakt. I mange forskellige forhold benyttes kontrakter og andre aftaler til at regulere forholdet til ansatte, kunder og andre virksomheder. Kontrakter anvendes såvel nationalt som internationalt. Der er tale om en gammel retlig model, der er velindarbejdet på basis af en lang retlig praksis, og som dermed er velkendt af dem, som arbejder i erhvervslivet. Der er dermed tale om en form for regulering, der opleves som tryk, og der er en almindelig tillid til at forpligtelser fastsat via kontrakt sædvanligvis bliver indfriet. Som omtalt i kapitel 5 kan kontrakter, hvor den registrerede er kontrahent eller som tilvejebragt i dennes interesse, danne grundlag for overførsler. Det er en nærliggende tanke, at kontrakt, der som nævnt nyder erhvervsmæssig tillid, i videre omfang skulle kunne danne grundlaget for dataoverførsler. Herved vil der foreligge et retskildemæssigt fornuftsægteskab, idet en privatretlig reguleringsform bliver benyttet som middel at sikre overholdelse af offentligretlige forpligtelser.

Anvendelse af kontrakt har været på den retspolitiske dagsorden, stort set siden den første internationale databeskyttelsesretlige regulering så dagens

Kapitel 6 Særlige overførselsgrundlag

lys.⁹ Den grundlæggende overvejelse har været, at en kontrakt indgået mellem en virksomhed/dataansvarlig i eksportlandet og en virksomhed i importlandet skulle udgøre den regulering, der medfører, at dataoverførslen er betryggende. Kontrakten skal skabe sikkerhed for, at eksportøren og importøren overholder de databeskyttelsesretlige forpligtelser, der i kontrakten tilpasses, således at de modsvarer den konkrete overførsel. Der er tale om særlig form for *lex mercatoria*. I modsætning til branchekodekser omfatter en sådan kontrakt en eller flere specifikke overførsler mellem identificerede parter, og kontraktens styrke er, at den er udformet med henblik på dette formål.

I forhold til denne model er det væsentligste spørgsmål, om det under et databeskyttelsesmæssigt perspektiv er acceptabelt, at den registrerede ikke har kontrahentstatus i kontrakten. Det er almindeligt anerkendt, at det i en kontrakt er muligt retligt forpligtende at tillægge udenforstående rettigheder. Et gaveløfte, der er relateret til tredjemand, er et simpelt eksempel herpå. Denne opfattelse af kontraktens relativitet (*»privity of contract«*) betyder, at det ikke er udelukket, at der i en kontrakt mellem to dataansvarlige fastsættes regler, som medfører rettigheder for de registrerede, selvom disse ikke indgår i kontrakten. Problemet er herefter, dels hvorledes det sikres, at disse rettigheder er tilstrækkelige, dels hvorledes den registrerede kan have mulighed for at håndhæve sin ret, såfremt der sker misligholdelse. Det er især det sidstnævnte spørgsmål, der oprindeligt blokerede for anvendelsen af kontraktmodellen.

I forhold til det førstnævnte spørgsmål er svaret, at en overførselskontrakt først får virkning, såfremt den godkendes af Datatilsynet. Beføjelsen i POL § 27(4) danner således grundlaget for, at det kan sikres, at kontrakten indholdsmæssigt er acceptabel. Svaret på det andet spørgsmål er, at der i kontrakten må indbygges regler, som giver den registrerede adgang til at håndhæve sine rettigheder. I kontrakten kan der afgives et såkaldt tredjemandsløfte, som forpligter de to kontrahenter til at acceptere, at den registrerede gør sine kontraktsbestemte rettigheder gældende, jfr. yderligere nedenfor. Det kan lægges til grund, at der i EU-medlemsstaterne ikke findes national lovgivning, som hindrer afgivelsen af et sådant løfte.¹⁰ Om dette er tilfældet i alle

9. Om tidlig brug af kontrakt i EU se A.C.M. Nugter: *Transborder flow of personal data within the EC* (Deventer 1990) p.306-07. – I Europarådet blev der i 1992 udformet en modelkontrakt, der samme år blev udformet i en revideret udgave af *International Chamber of Commerce*. – Se i øvrigt Registertilsynets Årsberetning 1991 p.32-34, hvor Registerrådet fremhæver, at kontrakter er et supplement, ikke et alternativ til lovgivning.

10. Jfr. WP 74 p.12 med note 11.

10. Standardkontrakt

tredjelande, må her henstå som usikkert, men skulle der i importørens nationale ret være hindringer herfor, vil dette indebære, at en sådan konstruktion ikke kan anvendes således at det besværlige alternativ, der består i indgåelse af en selvstændig kontrakt med de registrerede, må benyttes. På grundlag af den almindelige grundsætning om aftalefrihed er det sædvanligvis muligt at benytte et tredjemandsløfte, og på dette grundlag er vejen banet for, at sådanne kontrakter kan udgøre et muligt overførselsgrundlag.

En yderligere forudsætning herfor er, at der i kontrakten er indsat regler, som skaber en tilstrækkelig sikkerhed for at denne vil blive overholdt (»accountability«). Selvom de registrerede tildeles en position, hvorfra de selvstændigt kan agere, bør dette kun undtagelsesvist være nødvendigt. Kun få registrerede evner i praksis at håndhæve deres retspositioner. Kontrakten bør derfor udformes på en sådan måde, at den i sig selv udgør et tilstrækkeligt incitament til, at de angivne forpligtelser bliver overholdt af kontrahenterne.

10. Standardkontrakt

Enhver kontrakt, der tilfredsstillende besvarer de to ovenfor nævnte spørgsmål, vil kunne opnå godkendelse. Der er således ikke fastsat yderligere begrænsninger i valget af kontrakt, jfr. herved den nedenfor omtalte beslutning om standardkontrakt 2001 præambel betragtning 6. Det er dog ikke enkelt at udforme en sådan kontrakt, der ikke ligner de kontrakter, som de fleste virksomheder sædvanligvis anvender. En sådan kontraktudarbejdelse er både tidskrævende og omkostningskrævende. Det har således formodningen for sig, at alene store virksomheder vil kunne magte denne opgave med den konsekvens, at kontraktmodellen kun vil blive anvendt i begrænset omfang. Mellemstore og små virksomheder må derfor have hjælp.

EU har en almindelig interesse af primært økonomisk karakter i, at der i det videst mulige forsvarlige omfang sker overførsler, og dermed en interesse i, at det juridiske grundlag herfor er til rådighed, således at de databeskyttelsesretlige forudsætninger kan være opfyldt. Dette er baggrunden for, at Kommissionen har truffet beslutninger, der endosserer bestemte standardkontrakter. Disse omtales i det følgende, idet først to kontrakter, der vedrører relationen mellem to eller flere dataansvarlige, behandles, hvorefter en standardkontrakt, der angår overførsel fra en dataansvarlig til en databehandler, beskrives.

De af Kommissionen truffne beslutninger er forpligtende for de nationale datatilsyn i den forstand, at tilsynet som altovervejende hovedregel ikke kan nægte at give tilladelse til en overførsel, der sker på grundlag af en uændret anvendelse af en endosseret standardkontrakt. En tilladelse efter POL § 27(4)

Kapitel 6 Særlige overførselsgrundlag

er dog fortsat påkrævet, og det er i sjældne tilfælde muligt for tilsynet at afslå denne, jfr. beslutning om 2001 kontraktens artikel 4 og præambelens betragtning 15. Dette kan ske i tilfælde, hvor det skønnes ikke at være sandsynligt, at kontrakten vil blive overholdt med alvorlig skadevirkning for de registrerede, eller når importørlandets ret indebærer forpligtelser, der i betydeligt omfang strider mod kontrakten. På samme grundlag kan tilsynet ligeledes på et senere tidspunkt suspendere kontrakten. Det må antages at være sjældent at dette vil ske. Den omstændighed, at en tilladelse efter dansk ret¹¹ er påkrævet indebærer yderligere, at der er mulighed for at stille vilkår, der dog ikke kan indebære nye kontraktvilkår, og som sædvanligvis alene består i at kontrakten ikke kan ændres forinden en ny tilladelse er opnået.

Kravet om tilladelse giver Datatilsynet mulighed for at opnå viden om, i hvilket omfang standardkontrakterne bliver benyttet i praksis, hvilket er en målestok for deres anvendelighed. Det giver ligeledes tilsynet en mulighed for at indgå i en dialog med den dataansvarlige, således at det sikres, at denne forstår de databeskyttelsesretlige forpligtelser, som kontrakten indebærer. Datatilsynet kan i denne forbindelse efterse, at det rent faktisk er en af de endosserede standardkontrakter, som bliver anvendt, og ligeledes blive bekendt med, hvorledes de åbne punkter i kontrakten er blevet udfyldt. I praksis accepteres mindre justeringer, men i almindelighed er det karakteristisk, at der sker en nøje kontrol af det forelagtes overensstemmelse med standardkontrakten og ligeledes med, at de åbne punkter er udfyldt på en fornuftig måde.¹² I denne forbindelse bør fremhæves, at det er muligt for kontrahenterne at inddrage andre spørgsmål end de databeskyttelsesmæssige i kontrakten frem for at skulle lave en separat aftale om disse. Dette kan tit være praktisk, men sådanne emner er selvsagt ikke omfattet af tilsynets tilladelseskompetence.

Det må endelig præciseres, at standardkontrakterne ikke udelukker, at Datatilsynet kan give tilladelse på grundlag af en selvstændigt udarbejdet kontrakt, hvilket efter omstændighederne kan være fordelagtigt da sådanne kontrakter er forhandlet mellem parterne. Anvendelse af standardkontrakter kan have den ulempe, at der ikke forinden deres anvendelse er en tilstrække-

11. Tilsynspraksis er ikke ens i medlemsstaterne. I nogle lande, vist nok eksempelvis England, skal en overførsel baseret på en uændret anvendelse af standardkontrakten ikke godkendes eller forelægges tilsynsmyndigheden. En sådan praksis kan være ressourcemæssigt betinget.

12. Som standardformular anvendes: »Idet Datatilsynet har noteret sig og lægger afgørende vægt på, at den foreliggende overførsel finder sted i overensstemmelse med Kommissionens standardkontraktbestemmelser, meddeler ...«

11. 2001-kontrakt for dataansvarlige

lig dybtgående dialog mellem parterne, hvilket kan bidrage til en klarlægning af de forpligtelser, som kontrakten medfører, men i almindelighed er fordelene større end ulemperne.

Forinden de enkelte kontrakter omtales, kan det være nyttigt at nævne de trufne kommissionsbeslutningers struktur. Disse beslutninger består af en præambel, der udgør motiveringen, nogle få artikler, der fastsætter overordnede regler, herefter kontrakten, som omfatter en tekst¹³ med en række bestemmelser (eller klausuler), samt yderligere et antal bilag, der for en dels vedkommende skal udfyldes af kontrahenterne. Strukturen er i og for sig ganske kompliceret, idet præambelen og artiklerne især har til formål at udgøre en støtte for kontrahenterne og Datatilsynet. En tilsvarende støtte er efterfølgende givet ved Kommissionens svar på ofte stillede spørgsmål (»FAQ«).¹⁴

11. 2001-kontrakt for dataansvarlige

Ved beslutning af 15.juni 2001 godkendte Kommissionen den første standardkontrakt for overførsel fra en dataansvarlig i en medlemsstat til en dataansvarlig i et tredjeland, der ikke har et tilstrækkeligt beskyttelsesniveau.¹⁵ Af artikel 2 samt præambelens betragtning nr.1 fremgår, at det er en forudsætning, at den nationale ret i eksportlandet er overholdt. Denne almindelige forudsætning er således fastholdt som en ubetinget forudsætning. Dette gælder også for de øvrige kontrakter. I det følgende redegøres der for kontraktens hovedpunkter, idet der tages udgangspunkt i de implicerede parter.

13. På dette sted er det påkrævet med en bemærkning om sprog og terminologi.

Som bekendt har EU-retsakter samme retlige gyldighed på de 20 EU-sprog. Dette kan undertiden være en komplikation, da det ikke er alle begreber, der helt ens kan gengives på alle sprog. De i det følgende omtalte dokumenter har ikke indgået i sager bedømt af EF Domstolen, der kan fastsætte en definitiv fortolkning. Her anvendes alene den danske udgave.

Der er endvidere en uheldig forskel mellem terminologien i personoplysningsloven og i EU-retsakterne samt øvrige EU-dokumenter. Især bemærkes, at når der i sidstnævnte tales om registeransvarlige, svarer dette til dansk rets dataansvarlige, og begrebet registerfører svarer til vores databehandler. – Det vil være ønskeligt, om der på et tidspunkt kunne ske en samordning af terminologien, hvor den her i landet forekommer mest dækkende.

14. Disse findes på Kommissionens hjemmeside for databeskyttelse.

15. Beslutningen er optrykt i EFT 2001 L 181/19. Se yderligere WP 38 af 26.1.2001 samt Peter Blume, Ugeskrift for Retsvæsen 2001 p.375-80.

Kapitel 6 Særlige overførselsgrundlag

For så vidt angår de registrerede fastslås i bestemmelse nr.3, at der afgives et tredjepartsløfte, idet kontrahenterne i 6.1. vedgår, at der for den registrerede kan være ret til erstatning ved skader. I nr.7 gives de registrerede adgang til at vælge hvilken form for konfliktløsning de ønsker at anvende, idet der eksempelvis kan være tale om domstolsproces eller mægling. I denne forbindelse kan bemærkes, at det i nr.10 fastslås, at det er eksportlandets ret, der skal anvendes for tolkningen af kontrakten. Det må anses for væsentligt i denne sammenhæng, at det netop ikke er importlandets ret, idet dette ville kunne skabe en uoverskuelig situation for den registrerede.¹⁶ Alt i alt kan det konstateres, at de registrerede gives en ganske fremtrædende position, hvis udnyttelse dog forudsætter en aktivitet af disse. Det forekommer som fremhævet ovenfor ikke givet, at alle registrerede i realiteten vil kunne hævde deres ret, men noget tilsvarende vil kunne anføres i forhold til en retsbeskyttelse, der følger af lovgivningen. I begge tilfælde er der tale om komplekse juridiske dokumenter og et fremmed miljø, men med disse nærmest uundgåelige forbehold er den registreredes interesse varetaget på fornuftig måde.¹⁷ Som tidligere nævnt har brugen af tredjemandsløftet været afgørende for overhovedet at acceptere anvendelsen af denne reguleringsmodel.

Kontrakten tildeler ligeledes Datatilsynet en position. Kontrahenterne påtager sig en samarbejdsforpligtelse, jfr. nr.4d og 5c, idet de skal besvare forespørgsler og meddele ønskede oplysninger. Sker der ændringer i importlandets lovgivning af betydning for kontraktens overholdelse skal importøren efter nr.5a meddele dette til såvel eksportør som tilsyn.¹⁸ Efter nr.8 skal et eksemplar af kontrakten på anmodning deponeres hos tilsynet. Dette har således en vis mulighed for løbende at følge med i, hvorledes kontraktforholdet bliver afviklet.

16. Også for Datatilsynet ville en sådan ordning skabe vanskeligheder og kunne let gøre det umuligt at vurdere om kontrakten etablerer et betryggende grundlag.

I forhold til det i kapitel 5 diskuteret spørgsmål om hvorvidt fremmed ret kan begrunde et retskrav, der nødvendiggør overførsler, kan standardkontrakten tale for, at dette ikke kan være tilfældet. Den giver således en vis om end ikke afgørende støtte til det modsatte synspunkt end det, der er advokeret i kapitel 5.

17. I artikel 29-gruppens tidlige overvejelser, WP 9 af 22.4.1998, blev i stedet for tredjemandsløftet nævnt den mulighed, at eksportøren ved siden af overførselskontrakten kunne indgå en selvstændig kontrakt med den registrerede. Dette ville have været en for kompleks ordning, jfr. herved ovenfor under 9.

18. I almindelighed accepteres kun sådanne begrænsninger i importlandets ret, der er begrundet i de samme hensyn, der efter artikel 13 kan begrunde afvigelser fra direktivet. Dette gælder også i forhold til de øvrige kontrakter, der omtales i de kommende afsnit.

11. 2001-kontrakt for dataansvarlige

I kontraktperioden er det særligt afgørende, at importøren faktisk overholder de databeskyttelsesretlige forpligtelser, som følger af kontrakten. I almindelighed er det antaget, at gennemførelse af inspektioner er et virksomt middel i denne forbindelse, jfr. POL § 62(3). I nr.5d reguleres dette spørgsmål, idet importøren skal lade sine faciliteter inspicere enten af eksportøren eller af et af denne udpeget organ, der besidder den fornødne sagkundskab. I sidstnævnte tilfælde skal udpegningen aftales med Datatilsynet, som er i stand til at bedømme organets troværdighed og kompetence. Der er således ikke fastsat en ordning, hvorefter det er eksportlandets datatilsyn, som kan foretage inspektion. Ud over at det kan være problematisk, at en udenlandsk myndighed agerer i en fremmed jurisdiktion, ville en sådan ordning også let kunne være en for stor belastning af tilsynets personaleressourcer, ligesom sproglige forhold vil kunne være en barriere for en forsvarlig gennemførelse af en inspektion.

Alt i alt må det konstateres, at kontrakten giver Datatilsynet muligheder for at overvåge, at overførte data behandles forsvarligt, idet det kan tilføjes, at det i nr.11 fastslås, at parterne ikke ensidigt kan ændre kontrakten. Som tidligere nævnt forudsætter overførsler på grundlag af en ændret kontrakt, at der opnås en ny tilladelse efter POL § 27(4).

Eksportørens forpligtelser er beskrevet i nr.4, hvor det først på ny fastslås, at national ret i det hele skal overholdes. Skal der ske overførsel af følsomme oplysninger, fastsættes en pligt til enten før eller snarest efter overførslen at give de registrerede information om denne. Selvom overførslen ikke var bekendt ved oplysningernes indsamling, jfr. POL §§ 28 og 29 samt foran i kapitel 4, indebærer denne bestemmelse således en oplysningspligt. På denne måde søges sikret, at anvendelsen af kontrakt ikke fører til en manglende transparens, men den fastsatte informationsforpligtelse er byrdefuld i de tilfælde, hvor der overføres oplysninger om mange registrerede. Det kan ikke afvises, at denne forpligtelse kan virke som en begrænsning af kontraktens anvendelighed. Den udvidede informationsforpligtelse kan i øvrigt sammenholdes med den af artikel 29-gruppen tilkendegivne opfattelse (WP 114), hvorefter overførsler med basis i artikel 26(2) er mere betryggende end overførsler efter artikel 26(1), hvor informationsforpligtelsen ikke er udvidet.

Transparens søges endvidere opnået ved, at eksportøren på anmodning er forpligtet til at udlevere de aftalte standardbestemmelser til den registrerede. Det er sandsynligt, at anvendelse af kontrakt i forhold til mange registrerede kan medføre en reduceret transparens, fordi der lægges et yderligere juridisk lag oven på loven. Uanset at en registreret vil kunne få bistand fra Datatilsynet, vil han alligevel ofte befinde sig på »Herrens mark«. Det kunne derfor i og for sig overvejes, om eksportøren skulle være pålagt en videregående

Kapitel 6 Særlige overførselsgrundlag

informationsforpligtelse, men ressourcemæssige hensyn taler med styrke imod en sådan ordning. I tillæg hertil kan fremhæves, at der bør tages hensyn til, at kontraktforhold traditionelt omgives af en vis fortrolighed.

Størst interesse knytter sig til importørens forpligtelser, eftersom disse er afgørende for den databeskyttelsesmæssigt betryggende behandling af de overførte oplysninger. De indholdsmæssige forpligtelser fremgår af nr.5b, der åbner for, at kontrahenterne ved udformningen af den konkrete kontrakt kan vælge mellem to muligheder. For det første kan importøren påtage sig at overholde de forpligtelser, der fremgår af kontraktens tillæg 2. Heri er med en lidt anden ordlyd opregnet direktivets grundprincipper og de registreredes rettigheder, idet det særligt kan bemærkes, at det ved behandling af følsomme oplysninger foreskrives, at der ved overførsel og brug skal anvendes stærk kryptering, jfr. herom i kapitel 2. Endvidere er der fastsat regler om yderligere overførsel til et utilstrækkeligt tredjeland, idet dette for følsomme oplysningers vedkommende forudsætter et samtykke fra den registrerede, der i andre tilfældet har en informeret indsigelsesret.¹⁹ For det andet kan importøren vælge at tilslutte sig de forpligtelser, der er nævnt i tillæg 3, samt i tilknytning hertil en af to muligheder, jfr. nedenfor. Tillæg 3 er mere begrænset og nævner kun enkelte principper samt reglen om videre overførsel. Vælges dette alternativ, skal importøren herudover som nævnt tilslutte sig en af to muligheder. Den ene består i at påtage sig at overholde de relevante bestemmelser i eksportlandets ret, hvilket i og for sig forekommer at være det mest vidtgående. Den anden består i en forpligtelse til at overholde de relevante tilkendegivelser, Kommissionen angiver i beslutninger om, hvorvidt et tredjeland er tilstrækkeligt. Det bemærkes, at den sidste mulighed forekommer at være noget upræcis, og den må være svær at gennemskue for kontrahenterne.

Sammenfattende er det, uanset hvilken af de forskellige muligheder der bliver valgt, karakteristisk, at kontrakten pålægger importøren en betydelig databeskyttelsesmæssig forpligtelse, og at det er overholdelsen af denne, som er afgørende for om kontrakten opfylder sit formål. Selvom disse forpligtelser ikke omfatter hele direktivet, er det alligevel på denne måde, at kontrakten fungerer som en eksport af direktivets retsopfattelse, som er gjort til det almindelige udgangspunkt. Det kan tilføjes, at det må afhænge af de konkrete erhvervsmæssige sammenhænge, hvilken af de ovenfor nævnte muligheder

19. Som tidligere nævnt vanskeliggør en sådan regel kontraktens anvendelighed, når denne omfatter mange registrerede. Måske ville det være bedre, om eksportøren, som der argumenteres for i WP 38 af 17.1.2001, i en sådan situation skulle indgå en selvstændig kontrakt med den nye importør, men dette blev altså ikke ordningen.

11. 2001-kontrakt for dataansvarlige

som efter fornøden overvejelse bliver valgt. Det lægges til grund, at det ikke i almindelighed er muligt at angive en præference mellem disse muligheder.

I bestemmelse nr.6 reguleres spørgsmålet om ansvar. Udgangspunktet er, at eksportør og importør i forhold til den registrerede er solidarisk ansvarlige og alene kan fritages for ansvar, såfremt det bevises, at ingen af dem er skyld i, at kontraktbestemmelserne ikke er overholdt (præsumptionsansvar). Det fremgår endvidere, at den registrerede kan vælge at anlægge sag imod en af kontrahenterne eller dem begge. Bliver den ene dømt grundet en overtrædelse begået af den anden, skal denne skadefriholde førstnævnte, idet denne regel dog ikke efter præambelns betragtning 20 er obligatorisk. I præambelns betragtning 18 begrundes det solidariske ansvar med, at dette mindsker de praktiske problemer for de registrerede, idet der er tilvejebragt en stor sandsynlighed for, at et indtrådt tab faktisk bliver kompenseret, jfr. yderligere nedenfor om denne konstruktion.

Det er mest nærliggende, at en registreret vil gøre et krav gældende i eksportlandet, og i tilfælde, hvor kontrakten er anvendt som grundlag for overførsler fra flere medlemsstater, kan det have betydning for importøren, hvilket land der er tale om. Dette skyldes, at de databeskyttelsesretlige sanktioner ikke er harmoniserede, med den følge at der er væsentlig forskel på det erstatningsniveau, der bliver anvendt. Importøren kan dermed i denne sammenhæng være mere eller mindre heldig. Dette emne skal ikke forfølges yderligere ud over at bemærke, at der er tale om et aspekt, som importøren bør være opmærksom på, jfr. i øvrigt i kapitel 7.

Endelig skal bestemmelse nr.9 om kontraktens ophør nævnes. Heri fastslås det vigtige princip, at uanset af hvilken årsag kontrakten ophører, indebærer dette ikke en fritagelse fra at overholde de forpligtelser vedrørende behandling af de overførte oplysninger, der følger af kontrakten. Som bekendt kan information være flere steder, og er persondata først overført, er der ikke nogen garanti for, at behandlingen ikke fortsættes, selvom kontraktforholdet er ophørt. En regel om, at overførte data skal returneres, er dermed ikke tilstrækkelig, idet det reelt ikke vil være muligt at kontrollere at en sådan bestemmelse bliver overholdt. Det er derfor nødvendigt, at forpligtelserne vedvarer, selvom dette ikke udgør nogen absolut garanti for, at de overførte data behandles forsvarligt. Dette skyldes, at der ikke efter kontraktens ophør er en relation mellem eksportør og importør. Man kan dog ikke komme videre, end at forpligtelserne består. Dette er således årsagen til, at kontrakten gives en

Kapitel 6 Særlige overførselsgrundlag

reel levetid, der i forhold til mange andre kontrakter nok kan forekomme usædvanlig.²⁰

Denne kontrakt må alt i alt karakteriseres som ganske finmasket og synes at tilvejebringe en betydelig garanti for en tilfredsstillende databeskyttelse. På den ene side kan det dog konstateres, at kontrakten ikke i større omfang modificerer direktivet og dermed ikke udgør nogen særlig omfattende imødekommelse af den undertiden fremsatte kritik af direktivet for ikke tilstrækkeligt at tage hensyn til erhvervslivets forhold. Kontrakten er i denne henseende snarere en ny form end et nyt indhold. Kontrakten derogerer ikke direktivet. På den anden side kan der være en vis tvivl om, hvor sikker den beskyttelse, der gives, egentlig er. Nok er det nationale datatilsyn med på banen, men dog mest på sidelinien, og det må som anført ovenfor anses for tvivlsomt, om de registrerede faktisk vil gøre brug af de håndhævelsesmuligheder, som de gives i kontrakten. I forhold til den almindelige lovgivning indgives der sikkert færre klager over overtrædelser til Datatilsynet, end der kunne blive, men der er næppe nogen tvivl om, at dette vil være endnu mere udpræget i forhold til misligholdelse af kontrakten. Det skal tilføjes, at der ikke foreligger undersøgelser, der kan belyse denne problemstilling.

12. 2004-kontrakt for dataansvarlige

Billedet er således ikke entydigt, men ud fra den generelle interesse i at fremme overførsler blev standardkontrakten dog i almindelighed modtaget som et fremskridt. Fra erhvervslivets side skete dette dog ikke med ubetinget glæde, og det kan konstateres, at enkelte dele af kontrakten medfører, at den ikke bliver anvendt i det forventede omfang. Først og fremmest har reglen om det solidariske ansvar givet anledning til kritik og er blevet karakteriseret som usædvanlig. Uanset forpligtelsen til at friholde den anden part fra omkostninger fremstår det ikke som rimeligt, at den ene part skal bære tabet for den anden parts misligholdelse i en situation, hvor parten fuldt ud har opfyldt sine egne forpligtelser. En sådan regel fremmer ikke en tillidsfyldt afvikling af kontrakten. Hensynet til den registrerede kan som nævnt ovenfor vel tale herfor, da ordningen fremmer overskuelighed og især betrygger muligheden for, at tab faktisk bliver erstattet, men det er ikke åbenbart, at dette hensyn er

20. Christopher Kuner: *European Data Privacy Law and Online Business* (Oxford 2003) anfører p.156-57, at bliver det tredjeland, som importøren befinder sig, senere godkendt som generelt tilstrækkeligt, bør det være muligt at lade kontrakten bortfalde. En del kunne tale herfor, men der ses ikke at være taget stilling til denne problemstilling.

12. 2004-kontrakt for dataansvarlige

tilstrækkeligt tungtvejende i denne sammenhæng. Under alle omstændigheder medfører denne usædvanlige klausul i praksis, at mange virksomheder ikke ønsker at benytte kontrakten.²¹

Der blev derfor i erhvervskredse igangsat et arbejde med henblik på udformningen af en anden kontrakt og en dialog med Kommissionen blev gennemført. Disse bestræbelser har medført, at Kommissionen i 2004 og med ikrafttræden 1.4.2005 ved en beslutning endosserede en yderligere standardkontrakt.²² Denne beslutning er formuleret noget misvisende, idet den fremtræder som en ændring af 2001-kontrakten. Dette betyder ikke, jfr. præambelens betragtning 2, at denne kontrakt ikke længere kan anvendes, men er blot udtryk for, at denne nye kontrakt svarer til 2001 kontrakten med en række ændringer. Den følgende omtale kan derfor være noget mere kortfattet, idet den hovedsageligt kun tager sigte på de bestemmelser, som er nydannelser.

Først kan det bemærkes, at de to standardkontrakter ikke kan kombineres, jfr. artikel 1 samt præambelens betragtning 3. I betragtning af, at de endosserede standardkontrakter ikke udtømmende angiver de kontrakter, som et datatilsyn kan godkende, må denne bestemmelse forstås således, at en kombination ikke etablerer en kontrakt, som Datatilsynet er forpligtet til at acceptere. Dette skyldes, at der ellers ville kunne opstå en noget uoverskuelig situation for de enkelte tilsyn, idet det herved præciseres, at godkendelse af en sådan kombinatorisk kontrakt eller en helt anden kontrakt ikke kan antages at være udelukket.

I almindelighed kan det som nævnt konstateres, at denne kontrakt for det meste svarer til 2001-kontrakten, idet det først og fremmest er den formelle udformning, som er blevet justeret. Konstruktionen er fortsat, at der afgives et tredjepartsløfte til de registrerede, der kan gøre et ansvar gældende mod eksportør og/eller importør. En sådan sag forudsætter, at den registrerede er bekendt med kontrakten. For så vidt angår dennes udlevering indebærer nr.1e en normalt nok mindre ændring i forhold til 2001-kontrakten, idet fortrolige dele af kontrakten kan tilbageholdes, hvilket kan siges at svare til sædvanlig fremgangsmåde. Udlevering af kontrakten in extenso kan dog pålægges af Datatilsynet, forudsat at den registrerede accepterer at behandle de pågældende dele af kontrakten fortroligt. Med en enkelt, ikke helt gennemskuelig,

21. I WP 9 af 22.4.1998 overvejer artikel 29-gruppen den mulighed, at det ved lov fastslås, at eksportøren er erstatningsansvarlig for skader forvoldt af importøren. En sådan ordning ville have været et dødsstød for kontraktmodellen, jfr. dog yderligere i kapitel 8, hvor en alternativ løsning, der kan minde herom, skitseres.

22. Denne beslutning er optrykt i EUT 2004 L 385/74. Se også Peter Blume, Ugeskrift for Retsvæsen 2005 p.145-50.

Kapitel 6 Særlige overførselsgrundlag

undtagelse er det ligeledes fortsat eksportlandets ret, der finder anvendelse, jfr. bestemmelse nr.4.

Det kan konstateres, at importørens position er noget styrket, idet det særligt kan fremhæves, at denne i forhold til afholdelse af inspektioner har adgang til at fremsætte berettigede indsigelser, jfr. nr.2g. Det kan endvidere bemærkes, at parterne kan aftale, at det er importøren frem for eksportøren, der besvarer forespørgsler fra Datatilsynet, jfr. nr.1d. Skaber importlandets ret problemer i forhold til kontraktens opfyldelse, skal importøren nu ikke orientere Datatilsynet, men derimod eksportøren, der dog er forpligtet til at meddele dette til tilsynet. Bortset fra en forstærket betoning af kontrahentrelationen synes sidstnævnte ikke at indebære nogen egentlig ændring.

For så vidt angår de materielle databeskyttelsesretlige regler, der skal overholdes, er der foretaget enkelte mindre modifikationer. Dette er tilfældet i forhold til retten til indsigt, som nu kan afslås ved konstant gentagne anmodninger (jfr. også POL § 33) eller hvis der foreligger en tilsvarende undtagelse i eksportlandets ret (jfr. POL §§ 30 og 32), jfr. Bilag A nr.5. For så vidt angår muligheden for reeksport fremgår det af nr.2iii, at specificationsgraden af den information, som skal gives til de registrerede som grundlag for en eventuel indsigelse er noget mindre end i 2001-kontrakten. Sidstnævnte kan give anledning til en vis bekymring, men kontrakten synes dog fortsat at yde et effektivt værn imod underminerende reeksport.

I almindelighed må de indtil videre omtalte nye bestemmelser i det store hele betragtes som udelukkende kosmetisk ændrede i forhold til 2001-kontrakten, idet de formodentlig er udformet med henblik på at gøre kontrakten mere »normal« og »spiselig« anskuet under en erhvervsmæssig synsvinkel. Dataoverførsler udgør et særegent område, og derfor har den retlige fremtrædelsesform en vis overtaleseskraft. Det er vigtigt, at kontrakten så vidt muligt ligner alle mulige andre internationale kontrakter.

Derimod er der som allerede antydnet sket en væsentlig nydannelse i forhold til kontrahenternes ansvar, jfr. herved bestemmelse nr.3 sammenholdt med præamblen betragtning nr.5, der angiver, at ansvarsordningen er udformet ud fra et princip om fornøden omhu, jfr. yderligere nedenfor. Der er ikke længere et solidarisk ansvar, idet hver part er ansvarlig for sine handlinger/undladelser. Mellem parterne, men altså ikke i forhold til de registrerede, er ansvaret begrænset til faktiske skader. Det er endvidere fastslået, at pønalt

13. 2001-kontrakt for databehandlere

begrundet erstatningsansvar er udelukket.²³ Kontrahenterne skal for så vidt angår de registrerede acceptere værneting i eksportlandet, hvor der altså kan føres sag mod en af disse. Det kan dog i praksis være vanskeligt for den registrerede at føre sag mod importøren, hvorfor eksportøren er forpligtet til at gøre den registreredes rettigheder gældende over for importøren inden for en rimelig tid (normalt en måned). Herefter kan sag føres mod importøren eller mod eksportøren såfremt denne ikke kan godtgøre at have udvist passende omhu i forhold til sin forpligtelse (såkaldt culpa in eligendo). I modsætning til 2001-kontrakten (bestemmelse 6.1) er der ikke i almindelighed fastsat en regel om ansvarsgrundlaget. Det fremgår dog, at eksportøren er ansvarlig efter »gældende databeskyttelseslovgivning«, hvilket som følge af direktivets artikel 23(2) indebærer et præsuntionsansvar.

Det er særligt dette ændrede ansvarsregime, der forventes at medføre, at denne kontrakt vil blive anvendt i større omfang. Dette skyldes, at denne ordning i almindelighed anses for at være mere fair end det solidariske ansvar. Det er endnu for tidligt til at vurdere, om dette faktisk vil blive tilfældet, og ligeledes må det indtil videre henstå i det uvisse, om de registrerede under denne ansvarsordning har tilstrækkeligt gode muligheder for at få erstatning i forhold til berettigede krav.

13. 2001-kontrakt for databehandlere

I praksis har de dataansvarlige ikke blot behov for at overføre oplysninger til andre dataansvarlige, men tillige til databehandlere, der foretager den tekniske opbevaring og bearbejdning af den dataansvarliges personoplysninger. En almindelig interesse i at få foretaget databehandlingen til en konkurrencedygtig pris kan begrunde sådanne overførsler. Dette kan eksempelvis være hensigtsmæssigt i en koncern, der samler den tekniske bearbejdning af koncernens oplysninger ét sted, jfr. videre herom nedenfor. Overladelse af oplysninger til en databehandler i et tredjeland er en overførsel, jfr. i kapitel 1, og derfor er det også i denne relation ønskeligt at have et særligt instrument, der kan indramme sådanne overførsler, idet det bemærkes, at Datatilsynet efter POL § 27(4) kan acceptere andre ordninger end den i det følgende omtalte.

23. »Punitive damages«: Den situation, hvor erstatningen udmåles til et beløb, der ligger over det faktiske tab, således at erstatningsansvaret minder om et strafansvar. Denne form for ansvar er ikke anerkendt i nordisk ret.

Kapitel 6 Særlige overførselsgrundlag

Kommissionen har truffet beslutning om en standardkontrakt til dette formål.²⁴ Datatilsynet skal acceptere anvendelsen af denne kontrakt, jfr. præambelens betragtning 5, men har dog mulighed for at foretage suspension eller nedlægge forbud, jfr. betragtning 8 og artikel 4, bl.a. såfremt forpligtelser, der er en følge af importlandets ret, kan medføre negative virkninger for de registrerede.

Ved databehandling er situationen den, at den retlige rådighed over de omfattede oplysninger ikke ændres, idet det er den dataansvarlige, der har forpligtelsen til at sikre, at oplysningerne behandles lovmedholdeligt. Data-behandleren har ikke nogen selvstændig kompetence. Ifølge direktivets artikel 17(3), jfr. POL § 42(2), skal dette klarlægges ved, at der indgås en kontrakt mellem ansvarlig og behandler. Eftersom national ret skal opfyldes, fungerer standardkontrakten som en præcisering af den kontraktforpligtelse, der principielt allerede foreligger, jfr. kontraktpræambelens betragtning 7. Det bør herved betones, at overførselskontrakten er en særlig kontrakt, hvis selvstændige formål er at kompensere for det lavere beskyttelsesniveau i importlandet.

Det er først og fremmest i forhold til datasikkerhed, at det er vigtigt, at der er en regulering af databehandlerens opgaver. Det er da også dette spørgsmål, som kontraktens fastlæggelse af eksportørs og importørs forpligtelser er centreret omkring i bestemmelserne 4 og 5, idet der i et tillæg til kontrakten skal ske en nærmere præcisering af, hvad den konkret vedrører. Herudover kan det for så vidt angår eksportøren bemærkes, at denne ved overførsel af følsomme oplysninger enten forinden eller snarest efter skal informere de registrerede om overførslen (4f), hvilket er en forpligtelse, der er videregående end den, der gælder for sådan overladelse i medfør af dansk ret.²⁵ Det er ikke åbenbart, at det er nødvendigt at pålægge en sådan forpligtelse, som, når databehandlingen omfatter mange registrerede, er svær at løfte for den dataansvarlige. Der er ikke sket nogen ændring af dataansvaret, som ville kunne begrunde en sådan forpligtelse.

For så vidt angår importøren pålægges denne underretningsforpligtelser samt en forpligtelse til at lade foretage inspektioner. Sidstnævnte pligt (5f) svarer til den, der er indeholdt i den tidligere omtalte 2001-kontrakt, men herudover er det i bestemmelse 8.2 fastsat, at eksportlandets datatilsyn vil kunne foretage inspektion efter de samme regler som gælder i eksportlandet,

24. Optrøkt i EFT 2002 L 6/52. – Se også artikel 29-gruppens WP 47 af 13.9.2001.

25. Overladelse af persondata til en databehandler er ikke omfattet af informationsforpligtelsen i POL §§ 28 og 29 (artikel 10 og 11), hvilket er naturligt, eftersom den dataansvarlige fortsat har den retlige rådighed over oplysningerne.

13. 2001-kontrakt for databehandlere

jfr. herved også præambelns betragtning 8. Sidstnævnte kompetence kan ikke anses for problematisk, når det tages i betragtning, at det er eksportøren, der udøver den retlige råden. Dens udøvelse er dog ressourcekrævende for Data-tilsynet, og det vil formodentlig være sjældent, at sådanne inspektioner gennemføres.

Som ovenfor nævnt er det den dataansvarlige, der har forpligtelsen til at sikre lovlig behandling, og dette udgangspunkt præger den fastsatte ansvarsordning. På samme måde som i de andre kontrakter er denne ordning baseret på et tredjepartsløfte til de registrerede, som på basis af eksportlandets ret (nr.9) kan gøre ansvar gældende mod eksportøren, jfr. nr. 6.1, der intet angiver om ansvarsgrundlag eller bevisbyrde, som derfor må være som sædvanligt i eksportlandets rets implementering af direktivet. Ifølge 6.3 kan eksportøren blive skadefriholdt af importøren. Kontrakten tager højde for den situation, at eksportøren ikke længere findes eller er insolvent, og fastsætter i 6.2 at i denne situation kan kravet rettes mod importøren, der accepterer at blive betragtet, som om denne var eksportøren.

Denne kontrakt vil som nævnt ovenfor kunne anvendes af virksomheder, f.eks. en koncern, der befinder sig i flere medlemsstater. Det er et erhvervsmæssigt ønske, at databehandleren i en sådan situation kan behandle alle de overførte oplysninger på grundlag af de samme sikkerhedsregler. Dette skaber den mest enkle og overskuelige situation for koncernen. En sådan ordning vil dog kunne betyde, at sikkerhedsniveauet ikke nødvendigvis lever op til kravene i alle de implicerede medlemsstater eftersom der på dette punkt kan være variationer.²⁶ Dette er således et eksempel på, at den manglende harmonisering i EU skaber vanskeligheder, jfr. kapitel 4. En sådan ordning er ikke udelukket, men forudsætter, at de nationale tilsyn giver deres tilladelse.

Afslutningsvis kan det fremhæves, at der er tale om den eneste endosserede standardkontrakt vedrørende denne overførselssituation, som i princippet er forholdsvis enkel. Kontrakten har ikke givet anledning til kritik, og det synes derfor at kunne lægges til grund, at den i det væsentlige på god måde opfylder sit vigtige praktiske formål.

26. I WP 47 af 13.9.2001 udtrykkes p.3 betænkeligheder ved denne ordning, idet det fremhæves, at det må være eksportlandets niveau, der er gældende. – Se om problemstillingen Christopher Kuner p.154-55.

14. Er kontrakt egnet?

I almindelighed kan det på grundlag af ovenstående overvejes, om kontrakt er en velegnet reguleringsmodel. For en positiv besvarelse af dette spørgsmål taler, at det i en kontrakt er muligt at angive en meget specifik regulering af den konkrete overførsel, samtidig med at det kan sikres, at der er en tilstrækkelig myndighedskontrol, og at de registrerede har rettighedspositioner, som de kan gøre gældende. Det er ligeledes positivt, at sandsynligheden for, at denne regulering i en kommerciel sammenhæng bliver overholdt som følge af tillid til kontraktformen og som følge af, at der er tale om en form for selvregulering, forekommer at være ganske stor, selvom den selvfølgelig ikke er 100%. I den modsatte retning kunne det anføres, at der kan være en risiko for at de databeskyttelsesretlige forpligtelser bliver udtyndede, samtidig med at kontrakten kan etablere et forholdsvis lukket overførselsforløb, som kan være uigennemskueligt for tilsynsmyndigheden, og især at de registrerede uanset tredjemandsløftet vil have svært ved at gøre deres rettigheder gældende. Disse betænkeligheder er udtryk for et caveat, men indebærer ikke, at kontrakt ikke bør anvendes.

Alt i alt er der tale om en velegnet model, i hvis anvendelse erhvervslivet har en positiv egen interesse, selvom de foreliggende standardkontrakter undertiden karakteriseres som komplicerede, og en simplificering efterspørges. Kontrakterne kan især virke tunge i de tilfælde, hvor en eksportør skal relatere sig til et større antal importører. Uanset sådanne vanskeligheder er kontraktmodellen i almindelighed velset i erhvervslivet. Hertil kommer, at kontraktmodellen som tidligere nævnt kan medvirke til en større udbredelse af den europæiske opfattelse af databeskyttelse, og selvom den modsatte virkning også kan indtræde, vil kontrakterne nok på sigt medføre, at flere tredjelande gennemfører en regulering, der gør det muligt at anerkende dem som tilstrækkelige lande. Dette bør fortsat være det langsigtede mål.

15. Bindende virksomhedsregler

Den positive bedømmelse af kontrakt som reguleringsmodel er ikke ensbetydende med, at der ikke kan og bør oparbejdes andre ordninger, som enten alene eller i kombination med kontrakt kan udgøre et grundlag for dataoverførsler. Dette kan være begrundet i, at kontrakt i den specifikke erhvervsmæssige sammenhæng ikke er et anvendeligt eller hensigtsmæssigt instrument. Behovet for et alternativ er særlig aktuelt i forhold til internationale enhedsselskaber som eksempelvis Visa, idet det ikke er muligt at kontrahere

15. Bindende virksomhedsregler

med sig selv, og for koncerner, hvor kontrakt kan fremtræde disharmonisk i forhold til selskabsstrukturen, idet denne gives et opsplittet og mindre tillidsfuldt præg. I praksis er det vist nok særligt koncerner, der har et behov for et andet instrument, som kan bruges som alternativ til kontrakt, idet der ellers kan opstå situationer, hvor der er behov for et meget stort antal sammenhængende kontrakter, hvilket kan medvirke til at skabe uoverskuelighed og indebære store udgifter til juridisk bistand. Internationale koncerner, hvor der eksempelvis anvendes fælles integrerede edb systemer, benyttes i det følgende som eksempel.

På denne baggrund er der udviklet et nyt instrument, der betegnes bindende virksomhedsregler (BVR – »Binding Corporate Rules«), der har været vurderet i artikel 29-gruppen, hvis overvejelser det følgende er baseret på.²⁷ Denne konstruktion kan minde om en standardkontrakt omfattende mere end to kontrahenter, men er en selvstændig reguleringsform, som formelt ikke er et resultat af en forhandling mellem de implicerede virksomheder. Den grundlæggende ide er, at en koncern kan udarbejde regler for, hvorledes den behandler personoplysninger i alle dele af koncernen, herunder i ikke tilstrækkelige tredjelande, og såfremt disse regler er forpligtende og bindende, kan de danne grundlag for, at et datatilsyn kan tillade, at der sker overførsler inden for hele koncernen. Der er således som udgangspunkt tale om et regelsæt, der er skræddersyet til den pågældende koncern og dennes erhvervsprofil, og denne individualitet indebærer, at det ikke vil være muligt for Kommissionen på samme måde som ved kontraktmodellen at endossere en bestemt standard, idet det blot kan anbefales, at de nationale tilsyn accepterer brug af denne metode. Det er dog muligt, at det på et tidspunkt vil være muligt for Kommissionen at anvise en vejledende model for etableringen af en BVR, ligesom de regelsæt, der er blevet godkendt, vil kunne fungere som paradigmer, såfremt de er offentligt tilgængelige, hvilket de i hvert fald i en vis udstrækning må antages at være.

Der kan konstateres erhvervsmæssig opbakning til brugen af denne model, der som nævnt har den fordel, at den kan tilpasses til en bestemt erhvervsmæssig profil, der således i hvert fald i et vist omfang styrer udfyldningen af de databeskyttelsesretlige normer. Modellen afspejler på denne måde den individuelle koncerns autonomi. BVR eksemplificerer, at tankemønstre fra private virksomheder har fået større betydning i den databeskyttelsesretlige regulering. BVR kan minde lidt om de adfærdskodekser, der kan udstedes i

27. Se hertil artikel 29-gruppens WP 74 af 3.6.2003, og WP 107 og 108 af 14.4.2005. – WP 74 er i praksis styrende for datatilsynenes vurdering af BVR.

Kapitel 6 Særlige overførselsgrundlag

medfør af direktivets artikel 27 og POL § 74, men adskiller sig dog fra disse ved at være mere specifikke og ved ikke at dække et så bredt spektrum, som en adfærdskodeks sædvanligvis gør. BVR tager ikke sigte på en branche, men på en bestemt koncern. Regelsættet skal passe til koncernens corporate governance, og dermed er den unik. Det kan endvidere bemærkes, at udarbejdelse af et sådant regelsæt må betragtes som en krævende opgave, der forudsætter afsætning af en del ressourcer, og i betragtning af, at der ikke foreligger en standard er det forventeligt, at denne model alene er en mulighed for store virksomheder. Det er dog sikkert hovedsageligt alene denne type virksomheder, der vil betragte BVR som en egnet model.

Et første spørgsmål er, for hvilke virksomheder en BVR kan betragtes som egnet.²⁸ Dette spørgsmål er til dels aktualiseret af, at der i de forskellige medlemsstater anvendes varierende koncernbegreber. Dette taler for en præcisering af anvendelsesområdet, således at der alene bør være tale om det, man kan kalde tætte koncerner, hvorved mere løse samarbejdsrelationer udelukkes. Dette skyldes, at det er nødvendigt, at der foreligger en rimelig grad af sikkerhed for, at regelsættet faktisk vil fungere. Det vil være op til Datatilsynet at vurdere, om der foreligger en tilstrækkelig tæt koncern, hvilket som følge af dansk rets koncernbegreb næppe vil give anledning til vanskeligheder.

Et andet spørgsmål i denne sammenhæng er, om reglerne skal gælde for hele koncernen eller mere præcist, om de skal gælde både for koncernselskaber, der befinder sig i EU og dermed er omfattet af direktivet, og for koncernselskaber uden for EU i henholdsvis tilstrækkelige og utilstrækkelige tredjelande. Det synes at være opfattelsen, at hele koncernen skal være dækket, hvilket kan begrundes med, at der herved opstår størst sikkerhed for, at reglerne virker effektivt og ligeledes tilvejebringer den bedste overskuelighed for de registrerede. I forhold til den del af koncernen, som befinder sig i EU, virker en BVR dermed som en præcisering af de retlige standarder, der indgår i direktivet. Som det omtales nedenfor, kan dette indebære et vist pres i forhold til de disharmonier, der foreligger mellem medlemsstaternes regulering, jfr. herved også i kapitel 4.

En koncern er ikke nogen fast forankret størrelse, idet der kan komme nye selskaber til. Her er det opfattelsen, at foreligger der en godkendt BVR, skal proceduren i forhold til de implicerede tilsynsmyndigheder ikke gentages,

28. Et eksempel på behovet for en sammenhængende løsning kan være en koncern, der anvender et call center, som er placeret i et tredjeland, der anvender samme sprog som i koncernen. Dette kan bl.a. forekomme inden for den finansielle sektor.

15. Bindende virksomhedsregler

idet et nyt koncernselskab uden videre kan deltage, hvis dette er forpligtet og bundet af de fastsatte regler. I disse tilfælde bør der blot ske en årlig rapportering til de pågældende datatilsyn, således at disse er klar over, hvem koncernen består af.

Under en retlig synsvinkel er anvendelse af BVR mere kompliceret end kontrakt. Dette skyldes, at den koncern, der udsteder et sådant regelsæt, dermed ensidigt påtager sig en forpligtelse. Dette er tilfældet, uanset at en tilsynstilladelse er nødvendig for, at regelsættet kan anvendes. Problemet er herefter, om denne forpligtelse er retligt virksom i den forstand, at koncernen kan fastholdes på denne i forbindelse med bedømmelsen af en efterfølgende konflikt. Dette er afgørende i forhold til det tredjemandsløfte i forhold til de registrerede, som også denne konstruktion er baseret på. Ud over i forhold til domstolene er dette ligeledes væsentligt i forhold til Datatilsynet, der skal have reel mulighed for at behandle klager fra de registrerede. Hvorvidt en ensidig erklæring er retligt forpligtende, afhænger af national ret, og medens dette må antages at være tilfældet i dansk ret, synes dette ikke at være tilfældet i alle medlemsstaterne. Et tilsvarende spørgsmål kan foreligge i relation til selskaber i tredjelande, hvor der generelt vurderet foreligger usikkerhed i denne henseende, men de nedenfor nævnte bestemmelser om jurisdiktion gør dog dette mindre problematisk. Der kan altså opstå den situation, at BVR, der skal omfatte selskaber i mange medlemsstater, ikke uden videre kan være virksom i alle disse stater. Problemet kan dog løses ved at supplere BVR med kontrakt i forhold til sådanne selskaber, der således på denne måde kan forpligtes. Denne mulighed for at anvende supplerende kontrakter vil i øvrigt ligeledes kunne benyttes i forhold til udenforstående underleverandører, som ønskes inddraget under regelsættet. Den her drøftede problemstilling betyder dermed i sidste instans blot, at en BVR ikke altid vil kunne stå alene.

For at en BVR kan accepteres, må det således være sikkert, at den konstituerer en retlig forpligtelse, men herudover må det forudsættes, at disse regler i praksis er bindende i koncernen. Der må være en styring, således at der med BVR sker en udnyttelse af den hierarkiske struktur i en virksomhed. Det må være sikkert, at man i de forskellige koncernselskaber faktisk overholder reglerne. Dette gælder også for de ansatte i koncernen. Opnåelse af en sådan sikkerhed kan først og fremmest ske via interne foranstaltninger, der består af en kombination af information/uddannelse og instrukser fra ledelsen. Det er ledelsen, der må sørge for, at sådanne foranstaltninger er på plads, idet dette bl.a. vil kunne ske ved, at bestemte personer i koncernen gøres ansvarlige for

Kapitel 6 Særlige overførselsgrundlag

koncernens databeskyttelsespraksis.²⁹ Det er af artikel 29-gruppen forudsat at det i det konkrete tilfælde må være sandsynligt at reglerne på denne måde er bindende og ved at formulere dette krav går man i og for sig videre end tilfældet er ved standardkontrakterne, som primært er baseret på fastsættelsen af række retlige forpligtelser. Denne forskel er dog nok mere formel end reel. En yderligere metode til at kontrollere reglernes overholdelse er interne inspektioner, og det forudsættes derfor at der er etableret et system, hvorefter disse finder sted indenfor rimelige intervaller. Det er endvidere forudsat, at disse inspektioner er tilrettelagt på måde, der af det pågældende datatilsyn vurderes som troværdig.

I denne forbindelse kan det overvejes om det som et vilkår for en tilladelse efter § 27(4) kan fastsættes, at Datatilsynet har adgang til at foretage inspektion. Et sådant vilkår vil kunne gøre den pågældende BVR mere betryggende. Det fremgår ikke af § 27(4) eller dennes forarbejder (FT 1999-2000 A p.4083) hvilke vilkår, der kan fastsættes. I modsætning til ved de endosserede standardkontrakter, hvor Kommissionens beslutning udgør en begrænsning, kan der her fastsættes ethvert lovligt vilkår. I § 62(3) er det angivet, at tilsynet i almindelighed kun kan foretage inspektion når persondatabehandlingen er omfattet af § 50, idet der i forarbejderne (FT 1999-2000 A p.4103) tales om en »begrænset inspektionsbeføjelse«. Spørgsmålet er herefter om denne bestemmelse udelukker, at der kan stilles et vilkår om inspektion efter § 27(4), der især vil have selvstændig betydning i det omfang en BVR omfatter almindelige persondata (§ 6). Når det tages i betragtning, at en tilladelse efter § 27(4) indebærer en undtagelse fra lovens ordinære ordning, er et sådant vilkår efter mit skøn ikke udelukket. Selvom loven og forarbejderne er tavse lægges det derfor her til grund, at en inspektionsbeføjelse kan fastsættes som et vilkår, og at dette sædvanligvis vil være hensigtsmæssigt som en betryggelse af de registrerede.

For så vidt angår de materielle regler vil disse variere efter de konkrete omstændigheder, men skal altid omfatte en præciseret angivelse af de grundlæggende principper i direktivet samt en beskrivelse af de datatyper, der be-

29. I en række lande med Tyskland som det vel nok førende eksempel gælder den ordning, at virksomheder over en vis størrelse skal have udpeget en person, der er ansvarlig for databeskyttelse. En sådan ordning er forudsat i direktivets artikel 20(2) samt præambelens betragtning 54. Den er ikke pligtig, og en sådan ordning er ikke medtaget i personoplysningsloven, selvom det i store virksomheder typisk er en bestemt afdeling, der har ansvaret for, at de databeskyttelsesretlige regler bliver overholdt. – Det falder uden for denne bogs emneområde at drøfte, hvorvidt en ordning som den tyske bør gennemføres her i landet.

15. Bindende virksomhedsregler

handles, samt formålet hermed. Denne indholdsmæssige regulering vil dermed ikke principielt adskille sig fra den, der indgår i standardkontrakterne, der tværtimod udgør inspirationskilden til disse. Der skal ligeledes være medtaget bestemmelser om reeksport med en ret til indsigelse eller samtykke, såfremt der er tale om følsomme data.

I forhold til en koncern, der er spredt over et større antal lande, opstår spørgsmålet om, hvor den registrerede kan gøre et krav gældende. Det er her opfattelsen, at der enten må være jurisdiktion i eksportlandet (i EU) eller i et europæisk hovedkvarter eller, såfremt et sådant ikke findes, i et europæisk land, der er fastlagt i den pågældende BVR. Det er således ikke acceptabelt, såfremt den registrerede er henvist til at gøre sit krav gældende i et tredjeland. Denne ordning øger tilliden til BVR som et egnet retligt instrument og må da også i det hele betragtes som mest betryggende, idet den forebygger, at der opstår retsusikkerhed.³⁰ I sådanne sager bør der efter artikel 29-gruppens opfattelse gælde en regel om omvendt bevisbyrde.

Set under tilsynsmyndighedens perspektiv kan anvendelsen af BVR give anledning til ressourcemæssige betænkeligheder. Modsat ved standardkontrakter, hvor der er et forlæg, skal tilsynet tage stilling til et singulært dokument, der tit vil være meget omfattende. I godkendelsesproceduren er der mange forskellige forhold, som tilsynet skal være opmærksom på, og i hvert fald i Danmark er der ikke mulighed for at opkræve et gebyr, idet bestemmelsen i § 63(2) ikke medtager tilladelser i medfør af § 27(4). Selvom gebyret på 1.000 kr. for tilladelser efter § 50(2) reelt hverken er fugl eller fisk, er det bemærkelsesværdigt, at de tilladelser, som må forventes at være de mest arbejdskrævende, er gebyrfrie.³¹ Det er i det hele taget nærliggende fremover at genoverveje gebyrordningen, jfr. hertil i kapitel 7.

Hertil kommer, at en BVR, der ønskes godkendt, typisk omfatter koncernselskaber placeret i mange medlemsstater og der er derfor flere tilsyn, som skal vurdere det foreslåede regelsæt, hvilket kan være en tidskrævende proces. På denne baggrund er det naturligt, at de forskellige tilsyn samarbejder, jfr. herved også direktivets artikel 28. Artikel 29-gruppen anbefaler derfor en

30. Under en BVR vil personoplysninger cirkulere i koncernen og der vil løbende ske såvel eksport som import. Eksportør og importør kan begge være selskaber placeret i et tredjeland og oplysningerne kan vedrøre personer, der ikke er borgere i et EU land. Artikel 29 gruppen synes ikke at have overvejet denne situation, hvor europæisk jurisdiktion ikke forekommer åbenbart.

31. For en god ordens skyld bemærkes, at det er uden betydning, om den underliggende nationale behandling forudsætter en gebyrbelagt tilladelse. Dette er en anden historie end § 27(4)-tilladelsen.

Kapitel 6 Særlige overførselsgrundlag

ordning, hvorefter det mest nærliggende tilsyn fungerer som indgangssted og »lead authority«, idet ideen er, at denne myndigheds godkendelse kan danne grundlag for en mere forenklet sagsbehandling hos de øvrige tilsyn. Det første tilsyn har foretaget den detaljerede gennemgang af regelsæt, og denne bør være styrende for de øvrige tilsyns behandling. De øvrige tilsyn er dog ikke forpligtet til at træffe den samme afgørelse som det første tilsyn, da direktivet ikke er baseret på en one stop ordning,³² og som fremhævet ovenfor vil denne procedure sætte fokus på de forskelle, der er i medlemsstaternes lovgivning. Dette fokus kan blive anspændt, eftersom det selvsagt er meningen, at en BVR skal have gyldighed i alle de relevante medlemsstater.

Det kan tilføjes, at det ikke alene er i forhold til databeskyttelseslovgivningen, at der kan være forskelle mellem medlemsstaterne. For de enkelte tilsyn må det være en forudsætning, at national ret er overholdt, idet dette i Danmark kan have særlig betydning i relation til reglerne i markedsføringslovens § 6a.

Det kan tilføjes, at når der er opnået godkendelse, skal regelsættet foreligge på alle de implicerede landes sprog, men under processen kan koncernen nøjes med at fremsende reglerne på engelsk og på det sprog, der anvendes i det første tilsyns land. Herved udløses de ofte store udgifter til oversættelse først på det tidspunkt hvor de enkelte tilladelser faktisk er blevet givet.

I det hele taget kan det som nævnt være en krævende opgave at udforme en BVR. I artikel 29-gruppens WP 108 er der opstillet en tjekliste, som koncipister kan henholde sig til. Listen er relativt generelt udformet, men kan dog sikkert være til nogen hjælp, såvel når en BVR skal konciperes som når den skal vurderes af datatilsynene.

Den første BVR, der indtil videre omfatter 8 EU-lande, er blevet godkendt af en række datatilsyn, idet det engelske har fungeret som "Lead authority". Denne BVR, der er udformet af General Electric (GE), blev godkendt af Datarådet (25.1.2006) på grundlag af et omfattende materiale og efter drøftelser mellem tilsynssekretariatet og virksomheden.

Sammenfattende kan bindende virksomhedsregler være et brugbart instrument, der kan danne basis for overførsler. Denne model er et godt, men også krævende, supplement til anvendelsen af kontrakter. Der er tale om en model, som er velkendt i den forstand at det efterhånden er ganske udpræget, at der i større virksomheder med henblik på at sikre en tilstrækkelig styring gennemføres en intern regulering i form af kodekser, best practices, mm. Der er endnu ikke indhøstet de store erfaringer med denne model, men det lægges

32. En godkendelse på EU-niveau kunne være den mest ønskelige ordning.

desuagtet til grund, at den kan understøtte en effektiv databeskyttelse og dermed ikke udsætter de registrerede for nogen særlig risiko for en integritetskrænkende behandling af deres oplysninger. Det kan vel være tvivlsomt, om et sådant regelsæt medfører transparens, men når det tages i betragtning, at det i forvejen ikke er let at kigge ind i en koncern, kan en BVR desuagtet bringe lidt lys i mørket. Måske ikke så meget for de registrerede, men i hvert fald for de enkelte datatilsyn.

16. Safe Harbor

Et særligt grundlag for dataoverførsler er fastsat i Safe Harbor-ordningen, der angår dataeksport til USA. Denne ordning adskiller sig fra de hidtil beskrevne ved at den indebærer, at amerikanske virksomheder, som tilslutter sig ordningen, antages at have et tilstrækkeligt beskyttelsesniveau. Ordningen er dermed baseret på artikel 25(1) og ikke på artikel 26(2). Når Safe Harbor-ordningen desuagtet omtales her og ikke i kapitel 5, skyldes det, at denne ordning reelt fungerer som en særegen model og i realiteten ikke kan sammenlignes med den situation, hvor et tredjeland godkendes som tilstrækkeligt. Selvom det retlige grundlag ikke er det samme som for de ovenfor beskrevne ordninger, er Safe Harbor mere i familie med disse end med artikel 25(1)-landene.³³

Safe Harbor-ordningen har sit grundlag i en beslutning truffet af Kommissionen,³⁴ der er knyttet til en række vedtagelser fra den amerikanske regering ved Department of Commerce, som er medtaget som bilag 1-6. I disse bilag angives dels en række indholdsmæssige krav om databeskyttelse, der skal overholdes, dels er der medtaget 15 jævnlige stillede spørgsmål (FAQ – Frequently Asked Questions), hvori disse krav nærmere uddybes. Det er karakteristisk, at disse krav ikke fuldt ud svarer til direktivets.³⁵ Denne ordning vedrører udelukkende importører i den private sektor, der er omfattet af amerikansk jurisdiktion, jfr. hertil yderligere nedenfor. Den omfatter her dataansvarlige og databehandlere, idet det for sidstnævnte gælder, at det er den

33 Dette ses også af, at Kommissionen ofrer ressourcer på at følge denne ordning, der altså ikke er omgivet af den samme ro som de godkendte tredjelande. Som det fremgår nedenfor, var denne ordnings fødsel da også ganske besværlig.

34. Optrykt i EFT 2000 L 215, der medtager de amerikanske myndigheders afgørelser.

35. Ordningen er baseret på 7 hovedprincipper, der vedrører notice, choice, onward transfer, security, data integrity, access, og enforcement. Se hertil Christopher Kuner p.140-41.

Kapitel 6 Særlige overførselsgrundlag

dataansvarlige i EU, der er forpligtet, jfr. FAQ 10, hvorefter der her antages, at der ved denne eksport ikke kræves tilladelse fra Datatilsynet. I praksis skal der opnås tilladelse efter POL § 50(2), men denne gives kurant.

Safe Harbor-ordningen vil ikke blive detaljeret omtalt i det følgende, hvilket skyldes, at den alene regulerer importørens forhold modsat de ovenfor beskrevne ordninger, der også inddrager eksportøren. Det almindelige udgangspunkt er således, at kan en dansk virksomhed konstatere, at en amerikansk virksomhed er omfattet af Safe Harbor, kan der ske en dataoverførsel, idet eksportvirksomheden ikke i øvrigt behøver at foretage sig yderligere, jfr. dog nedenfor. Denne ordning indebærer således ikke, at eksportøren skal indrette sin persondatabehandling på en bestemt måde, idet de amerikanske virksomheder har et tilstrækkeligt beskyttelsesniveau.

Safe Harbor-modellen, der udelukkende omfatter den private sektor i USA, jfr. artikel 2, kom til verden efter et langt og besværligt forhandlingsforløb.³⁶ Baggrunden er, at det er opfattelsen i USA, at direktivet medfører en uacceptabel begrænsning af den frie handel. Det blev herved antydet, at direktivet strider mod WTO-reguleringen i GATS (General Agreement on Trade in Services) og er udtryk for protektionisme.³⁷ Dette skyldes, at USA ikke havde og i øvrigt ikke har nogen intention om at gennemføre en national lovgivning, som svarer til direktivet. USA er tilhænger af selvregulering i den private sektor, således at det grundlæggende er markedet, der normerer databeskyttelsen. Der er derfor ikke behov for nogen generelt dækkende lovgivning. Der er dog i GATS en særlig undtagelse med hensyn til databeskyttelse³⁸ hvorfor direktivet ikke strider mod denne aftale. Dette gøres vist nok heller ikke længere gældende.

36. Artikel 29-gruppen søgte at følge forhandlingsforløbet tæt og var, uanset at man formelt gav udtryk for tilslutning, ikke tryk ved ordningen og ligeledes frustreret over ikke at blive tilstrækkeligt inddraget. Forløbet kan følges via WP 15 af 26.1.1999, WP 19 af 3.5.1999, WP 21 af 7.6.1999, WP 23 af 7.7.1999, WP 27 af 3.12.1999, WP 31 af 16.3.2000. Se ligeledes WP 62 af 2.7.2002 med en første evaluering af ordningen.

37. Se hertil Joel Reidenberg i Colin Bennett, Rebecca Grant(ed): *Visions of Privacy* (Toronto 1999) p.219-20, Peter P. Swire, Robert L. Litan: *None of your Business* (Washington 1998) p.189-196. Se endvidere Colin Bennett, Charles Raab: *The Governance of Privacy* (Aldershot 2003) p.86-89, hvor det bemærkes, at direktivet også »skader« EU-virksomheder.

38. I artikel XIV fastsættes således, at »subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures necessary to secure compliance with laws and regulations which are not inconsistent with the provisions of the Agree-

16. Safe Harbor

USA fandt som nævnt direktivets konsekvenser uacceptable, og på denne baggrund blev der stillet krav om, at der blev etableret en særlig ordning, således at der ikke opstår de handelsbarrierer, som ellers ville foreligge. Der er ikke nogen tvivl om, at var dette krav blevet fremsat af et hvilket som helst andet land, ville det være blevet afvist, men dels er USA en supermagt dels er amerikanske virksomheder særdeles fremtrædende aktører i den internationale handel med en betydelig position også inden for EU.

Der forelå således en presset situation, der resulterede i denne aftale, som der ikke er nogen planer om at kopiere i relation til andre lande. Safe Harbor kan karakteriseres som en *sui generis* aftale, som grundlæggende indebærer en form for diskrimination i forhold til andre tredjelande. Også betragtet på denne måde er ordningen noget ganske usædvanligt inden for databeskyttelsesretten, og dens almindelige omdømme er for nu at formulere det diplomatisk ikke højt.

Grundlæggende er Safe Harbor-ordningen baseret på en form for styret selvregulering, idet en amerikansk virksomhed kan vælge at tilslutte sig de fastsatte principper og FAQs for databeskyttelse og herefter registrere sig som en safe harbor. Denne registrering, der skal gentages årligt, og som er tilgængelig på en hjemmeside drevet af Federal Trade Commission (FTC),³⁹ indebærer, at der herefter frit kan overføres personoplysninger fra en virksomhed i EU til den pågældende amerikanske virksomhed. En forudsætning for, at dette kan ske, er, at virksomheden er underlagt enten FTC's eller det amerikanske transportministeriums kompetence. Registrering kan også ske ved, at virksomheden deltager i en certificeringsordning (f.eks. Trust.E.), der har tilsluttet sig ordningen, men virksomheden skal fortsat være omfattet af de nævnte myndigheders kompetence, jfr. bilag 1 og 5. I praksis betyder dette især, at finansielle virksomheder ikke kan anvende ordningen, ligesom den indtil videre ej heller gælder for luftfartselskaber, idet sidstnævnte skyldes, at en hjemmel hertil i amerikansk lovgivning ikke er blevet udnyttet.

ment including those relating to the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts». [Min sammenskrivning af reglen]

Om bestemmelsen se Markus Konjewski: *National Regulation and Trade Liberalization in Services* (The Hague 2003) p.157-63.

39. www.export.gov/safeharbor

Kapitel 6 Særlige overførselsgrundlag

Ved fortolkningen af ordningen, herunder de fastsatte principper mm., finder amerikansk ret anvendelse,⁴⁰ og i det hele taget er det de relevante amerikanske myndigheder, især FTC, der spiller hovedrollen med den opgave at sikre, at ordningen faktisk fungerer efter hensigten, jfr. herved også nedenfor. Det har derfor en vis betydning for effektiviteten af disse krav, hvorledes den almindelige politiske holdning til privacy er i den amerikanske regering. Her kan det vistnok konstateres, at den nuværende Bush regering ikke prioriterer dette område højt i forhold til erhvervsvirksomheder. Kontrolintensiteten er aktuelt ikke stor, og vil i øvrigt svinge over tid.

EU søger ligeledes at overvåge ordningen dels via Kommissionen dels på grundlag af samarbejdsregler, der er indbygget i ordningen, dels via et særligt panel af tilsynsmyndigheder etableret på basis af FAQ 5. Panelets opgave er primært at besvare konkrete forespørgsler. Det er Kommissionens vurdering,⁴¹ at ganske vist har der ikke været mange klager, men det er dog usikkert, om ordningen overholdes i et tilfredsstillende omfang, idet det især er bemærket, at mange af virksomhederne ikke, som de skulle efter FAQ 6, har offentliggjort deres politik vedrørende databeskyttelse. Der er således en mangel på transparens, som skaber grundlag for en vis utryghed. Et almindeligt indtryk er, at det er ganske vanskeligt at gennemskue, hvorledes ordningen fungerer i praksis og om der reelt er det databeskyttelsesniveau, som ordningen angiver at repræsentere.⁴² En del kunne tyde på, at den ikke virker særlig effektivt.

Selvom der skal ske eksport til en safe harbor virksomhed, skal der foreligge en tilladelse efter POL § 50(2), der finder anvendelse, fordi ordningen er omfattet af 27(1). Denne er som udgangspunkt kurant, men Datatilsynet kan dog efter artikel 3.1 nægte at give tilladelse, enten fordi den kompetente amerikanske myndighed har tilkendegivet, at ordningen ikke overholdes af den pågældende virksomhed, eller når det konkret er indiceret, at manglende overholdelse er sandsynlig. Sidstnævnte vil sikkert sjældent være aktuelt.

40. Dette indebærer, at amerikanske virksomheder kan fravige deres forpligtelser såfremt dette er påkrævet efter amerikansk ret, idet et eksempel herpå kan være Patriot Act 2001.

41. Se SEK(2002) 196. – Baggrunden herfor er en større undersøgelse, foretaget ved universitetet i Namur, Safe Harbour Decision Implementation Study af 19.4.2004. Det påpeges bl.a. her, at mange amerikanske virksomheder grundet forståelsesproblemer har svært ved at overføre principperne til deres faktiske politik.

42. Det er i og for sig noget overraskende, at artikel 29-gruppen i WP 114 af 25.11.2005 p.6 og 9 tilsyneladende vurderer overførsler på dette grundlag positivt.

Som fremhævet ovenfor er det frivilligt, om en virksomhed tilslutter sig ordningen. Dette er sket i ganske stort omfang,⁴³ men der er dog fortsat et meget betydeligt antal amerikanske virksomheder, herunder meget informationsintensive, som ikke har gjort dette. Dette kan skyldes flere forhold. Blandt disse er en frygt for, at reglerne om indsigt skal give grundlag for mange erstatningssøgsmål især i forhold til indirekte indsamlede oplysninger, idet det her må erindres, at erstatningsniveauet er højt i USA. Et mere generelt problem for disse virksomheder er, at de kan bringe sig i den situation, at de også indenlandsk må give den angivne beskyttelse, der ligger over det sædvanlige amerikanske niveau. I almindelighed er det indtrykket, at mange amerikanske virksomheder finder det svært at anvende og gennemskue Safe Harbor-reglerne. Ordningen er kun en betinget succes. Overførsel til en virksomhed, der ikke har tilsluttet sig, er omfattet af § 27(3) og de øvrige ovenfor nævnte ordninger.⁴⁴

Safe Harbor er som nævnt en enlig, men meget betydningsfuld, svale, der, uanset at databeskyttelsesniveauet ligger over det sædvanlige amerikanske i relation til direktivets niveau især for så vidt angår den anvendte regulerings-teknik, kan opfattes som en form for amerikansk retsimperialisme. Modellen vil ikke danne forbillede for andre løsninger og er først og fremmest en illustration af de store økonomiske interesser, der er forbundet med dataoverførsler.

17. Kombination

Der foreligger således alt i alt en række forskellige ordninger, som tilvejebringer mulighed for dataoverførsler. Som udgangspunkt fungerer hver ordning for sig, men de kan dog gensidigt styrke hinanden i forhold til den bredde, som overførsler kan antage. Dette har særligt betydning for vurderingen af, i hvilken udstrækning der kan ske overførsel uden for den enkelte ordnings rammer. I denne forbindelse er et særligt relevant spørgsmål, om en

43. Den aktuelle status fremgår af listen på www.export.gov/safeharbor. Det kan bemærkes, at listen ikke er særlig overskuelig og er ganske vanskelig at anvende, jfr. Implementation Study p.110.

44. I WP 27 af 3.12.1999, hvor ordningen i øvrigt p.2 karakteriseres »som yderst nyttig« (!), fremhæves som et problem den situation, at en tilsluttet virksomhed fusionerer med en ikke tilsluttet virksomhed. Der er ikke fastsat regler herom, men det er nærliggende at antage, at den fusionerede virksomhed selvstændigt må tilslutte sig for at være omfattet af ordningen.

Kapitel 6 Særlige overførselsgrundlag

importør, der er omfattet af en standardkontrakt eller BVR, uden videre kan foretage reeksport i de tilfælde hvor den nye modtager er omfattet af en af disse ordninger eller af Safe Harbor. Så vidt det kan bedømmes, er det den almindelige opfattelse, at sådanne kombinationer kan finde sted, idet person-databehandlingen hele tiden er underlagt en fungerende regulering.

Det forekommer dog ikke åbenbart, at dette er fuldt ud betryggende for den registrerede. Dette skyldes, at videre eksport på dette grundlag medfører en situation, hvor de registrerede reelt ikke har nogen chance for at vide, hvor deres data behandles og med henblik på hvilke formål dette sker. Dette bestrykes af, at det vist nok er den almindelige opfattelse, at denne form for reeksport kan finde sted uden at opfylde de særlige krav bl.a. til information, der i øvrigt er fastsat i de enkelte ordninger, eftersom der er tale om eksport til en dataansvarlig, som i medfør af en af ordningerne har et tilstrækkeligt beskyttelsesniveau. Det kan være svært i en sådan situation at sikre, at de grundlæggende databeskyttelsesprincipper, f.eks. formålsbestemthed, bliver overholdt. Situationen kan minde lidt om de datafællesskaber, der søges etableret inden for den moderne digitale forvaltning, og som ligeledes kan medføre en reduceret transparens.

Overfor disse betænkeligheder står dog, at alle de overførsler, der i dag kan gennemføres med tilladelse efter POL § 27(4), med et vist forbehold for Safe Harbor (§ 50(2)), lever op til overordnede krav til dataoverførsler, og at det ikke er reguleringens formål at blokere sådanne overførsler. Det kan være unødigt restriktivt at udelukke en kombinatorisk anvendelse af ordningerne. På denne baggrund lægges det her til grund, vist nok i overensstemmelse med gældende ret,⁴⁵ at der kan ske en kombination, der dog ikke må forveksles med en sammenblanding. På denne måde kan de forskellige ordninger udgøre grundlaget for en ganske vidtstrakt anvendelse af betryggende dataoverførsler.

18. Vurdering

I det afsluttende kapitel 8 drøftes, om det er muligt at opbygge et mere sammenhængende alternativ til den eksisterende ordning. Her skal det blot afslutningsvis fastslås, at der, ved siden af Safe Harbor-modellen, i dette kapitel

45. Denne antagelse er ikke sikker, idet der kan argumenteres for, at der efter omstændighederne skal opnås (forny)et tilladelse efter enten § 27(4) eller § 50(2). – Det er muligt, at der er varierende opfattelser af denne situation i medlemsstaterne.

er redegjort for de ordninger, som i dag giver mulighed for dataoverførsler til utilstrækkelige tredjelande uden om de almindelige regler, der er omtalt i kapitel 5. Som det er fremhævet, er disse modeller ikke nødvendigvis sidste ord i denne sag, eftersom tilsynsmyndighederne har mulighed for at godtage andre ordninger og eftersom Kommissionen må forventes at stille sig positivt til nye modeller, der måtte blive foreslået. Der er fortsat plads til retlig kreativitet.

Det kan konstateres, at de eksisterende ordninger tager sigte på overførsler i professionelle sammenhænge, og hovedsageligt i forhold til virksomheder som aktører. Overførsel fra individer, f.eks. ved indsamling via en hjemmeside (C-B handel), falder uden for de beskrevne ordninger. Sådanne situationer kan næppe løses ved ordninger som de beskrevne, allerede fordi deres anvendelse forudsætter en ofte ganske betydelig anvendelse af tid og ressourcer.

Selvom andre årsager end de kommercielle kan begrunde gode muligheder for dataoverførsler, må det lægges til grund, at det først og fremmest er disse hensyn, der er den drivende kraft. Det kan konstateres, at de forskellige ordninger generelt bedømt på en betryggende måde muliggør disse overførsler. Selvom der efterhånden er etableret lidt af en retlig jungle, er det en jungle, der trods alt er til at finde rundt i, og alt i alt et forholdsvis sikkert ståsted for de kommercielt begrundede dataoverførsler.

KAPITEL 7

Håndhævelse

Dataoverførsler finder sted i stort omfang, og de antager mange differentierede former. Der foreligger som udgangspunkt en faktisk praksis, som det er vanskeligt eller måske mere dækkende er umuligt at overskue og vurdere. De hjælpemidler, der kan tages i anvendelse, er mangfoldige, og de er ofte ligeledes sofistikerede som følge af den moderne kommunikationsteknologi. Især Internettet udgør en udfordring, idet overførsler kan ske hurtigt og uden at det altid er muligt at afdække, hvem der har foretaget dem. De efterlader så at sige ingen spor. I det hele taget er den del af nettets filosofi, der fremhæver deling af information, i modstrid med databeskyttelsens idegrundlag. Denne modstrid viser sig med særlig styrke på det internationale niveau, hvor det umiddelbart fremtræder som mere naturligt at overføre end ikke at overføre personoplysninger.

Persondatooverførsler er svære at kontrollere udefra, og måske er der mange overførsler, der falder uden for de rammer, som er beskrevet i de forrige kapitler. Det er under alle omstændigheder et velkendt synspunkt, at de mange regler og ordninger ikke er deres papir værd fordi reglerne ikke overholdes og ikke kan kontrolleres. Det hævdes, at reguleringsopgaven er umulig at løse, og at den nærmest kan sammenlignes med det arbejde, som Sisufos skulle udføre.

1. Betyrrende overførsler?

Det er naturligt at overveje, i hvilken udstrækning det er sandsynligt, at de faktiske foretagne dataoverførsler i et tilfredsstillende omfang lever op til den overordnede fordring om, at der ikke ved overførsler må udløses nogen risiko for privatlivskrænkelser af de personer, der er omfattet af den enkelte overførsel. En overvejelse af denne karakter er naturlig, fordi man som nævnt indledningsvis ofte møder den opfattelse, at det kan være meget godt med en retlig regulering, men i det virkelige liv sker der alligevel et stort antal overførsler uden for denne ramme, og at det er en illusion at tro, at der kan foreta-

Kapitel 7 Håndhævelse

ges en kontrol, som med en tilstrækkelig grad af effektivitet forhindrer, at dette sker.¹ Implicit heri ligger, at det enten er lidt spild af tid at bruge så mange kræfter på at udvikle de retlige ordninger, der er beskrevet i de forrige kapitler, eller at disse skaber en ubegrundet tro på, at der på dette område er en databeskyttelse. Den gældende retlige regulering kan skabe en illusion om, at der foreligger et integritetsværn, og sådanne illusioner kan være farlige. I sin yderste konsekvens indebærer denne opfattelse, at der ikke bør være nogen retlig regulering, idet det er mere realistisk at overlade det til markedet at regulere, hvilke overførsler som er acceptable.

Dette er en indvending, der er baseret på et almindeligt indtryk, idet der vist nok ikke findes empiriske undersøgelser, som dokumenterer, at der i forhold til dataoverførsler findes et specielt stort mørketal, om end det er bemærkelsesværdigt, at det vist nok er en udbredt international erfaring, at der kun yderst sjældent retligt gribes ind over for dataoverførsler. Selvom indvendingen ikke er underbygget, er den dog alligevel alvorlig, fordi den synes at være i god overensstemmelse med common sense i den forstand, at det praktiske behov for dataoverførsler er så naturligt og stort, at det ikke synes at kunne inddæmmes af en retlig regulering.² Indvendingen er alvorlig, selvom nok alle vil være enige i, at der ikke til en bestemt retlig regulering kan stilles den fordring, at de fastsatte regler bliver overholdt fuldt ud. Der findes næppe en eneste retlig regel, som vil kunne honorere en sådan fordring. Dette gælder også for regler, der er præcise og klare. Dette er dog ikke ensbetydende med, at det er ønskeligt at have regler, som i meget stort omfang overtrædes. Der bør være en vis sandsynlighed for, at dette ikke er tilfældet. Det er ligeledes uønskeligt at have regler, der foreskriver en adfærd, der i nogle henseender betragtes som unaturlig eller umulig, da man ikke kan forpligtes af sådanne regler (*impossibilium nulla est obligatio*).

Selvom problemets omfang ikke lader sig indkredse med nogen præcision, er det sandsynligt, at det eksisterer, og allerede af den grund er det nødvendigt at vurdere, på hvilken måde dataoverførselsreglerne bliver kontrolleret og håndhævet, herunder hvilke midler der tages og kan tages i anvendelse i denne forbindelse. Denne vurdering er i det følgende struktureret således, at først behandles de nævnte spørgsmål i relation til overførsler inden for de

1. I WP 101 af 25.11.2004 konstateres p.3, at regeloverholdelsen på databeskyttelsesretens område i almindelighed ikke er god.
2. Christopher Kuner: *European Data Privacy law and Online Business* (Oxford 2003) anfører p.119 i relation til den retstilstand, der beskrives i direktivets artikel 25(1), at »this situation is the opposite of that to which most companies will be used, ie, that data can be transferred unless there is a reason not to do so«.

2. Datatilsynets rolle

retlige rammer således, som de er beskrevet i de forudgående kapitler, og derefter sættes fokus på håndteringen af de overførsler, der finder sted uden for disse rammer.

I denne forbindelse bemærkes, at problemstillingen langt overvejende angår overførsler til ikke tilstrækkelige tredjelande, idet der mellem EU-landene er fri overførsel. Spørgsmålet er således, om det i et tilfredsstillende omfang kan sikres, at overførslen er lovlig, og at de overførte persondata i det omfang, der stilles krav herom, behandles inden for den fastsatte ramme i importlandet. Sidstnævnte kan også være relevant inden for EU, men her medfører forudsætningen om, at behandlingen nationalt skal være lovlig, at problemstillingen uanset den manglende fuldstændige harmonisering har en mindre påtrængende karakter, eftersom direktivet trods alt medfører en ganske høj minimumsstandard. I hvilken udstrækning overholdelsen af eksportlandets nationale ret, der er overførselsspørgsmålets første dimension, faktisk kontrolleres og håndhæves, falder ikke naturligt inden for denne del af fremstillingen, idet der herom henvises til almindelige databeskyttelsesretlige litteratur. Det er sikringen af retmæssige overførsler til tredjelande, som er i fokus i det følgende, idet det dog bemærkes, at nogle af de nedenfor drøftede spørgsmål også er relevante i relation til overførsler inden for EU.

2. Datatilsynets rolle

Som det fremgår af beskrivelsen i kapitel 5 og 6, er der i personoplysningsloven og i de fastsatte overførselsordninger indbygget kontrolmekanismer, som tildeler Datatilsynet en række kompetencer. Der kan i almindelighed skelnes mellem ex ante- og ex post-foranstaltninger, idet det kan konstateres, at der langt overvejende sættes ind, før overførslen er foretaget, jfr. dog nedenfor under 7. De anvendte mekanismer omfatter rapporteringsforpligtelser for de dataansvarlige og først og fremmest krav om tilladelse til visse former for overførsler, jfr. POL §§ 27(4) og 50(2). Der stilles ikke normalt spørgsmålstegn ved det fornuftige i at have et datatilsyn, og det kunne for en umiddelbar betragtning forekomme rigtigt, at tilsynet bredt var bekendt med alle overførsler, der finder sted, frem for som i den gældende ordning alene med bestemte udvalgte typer af overførsler.³ Muligheden for at udøve kontrol ville

3. Undtaget måtte dog fortsat være de tilfælde, hvor hensynet til den registreredes vitale interesse begrundet overførslen, jfr. POL § 27(3 nr.5), men her kunne der eventuelt være en pligt til efterfølgende anmeldelse.

Kapitel 7 Håndhævelse

herved blive styrket. En sådan generel anmeldelsesforpligtelse måtte i givet fald omfatte behandlinger, der nationalt ikke skal anmeldes, hvilket kan begrundes med, at en overførsel aktualiserer særlige integritetsrisici. Den eksisterende tilladelsesordning omfatter i en vis udstrækning behandlinger af denne karakter, men en generel anmeldelsesordning støder dog an på i hvert fald to problemer.

Det første vedrører spørgsmålet om, hvor bureaukratisk den databeskyttelsesretlige regulering bør være. Især i relation til den private sektor har det, også i registerlovens tidsalder, været opfattelsen, at man skal være tilbageholdende med at fastsætte for mange byrder af denne karakter. Dette skyldes dels en hensyntagen til erhvervslivets ressourcer og dets behov for at kunne foretage hurtige dispositioner, dels at en sådan ordning kan give den samlede databeskyttelsesretlige regulering et dårligt ry. Sidstnævnte vil være uheldigt, bl.a. fordi databeskyttelsen grundet dens meget store bredde i sidste instans i betydeligt omfang beror på, at de dataansvarlige frivilligt overholder de fastsatte regler. En forudsætning herfor er, at disse regler gennemgående betragtes som fornuftige og velafbalancerede, og at de dermed mødes med en form for respekt. Det er en illusion at tro at databeskyttelse kan virkeliggøres alene fra oven, og det er ønskeligt at undgå en sådan opfattelse ved den praktiske anvendelse af de databeskyttelsesretlige regler. Det er nødvendigt, at de dataansvarlige aktivt medvirker og oplever databeskyttelsen som noget værdifuldt og positivt. Dette betyder ikke, at reguleringen fuldstændigt skal være udformet på den måde, erhvervslivet ønsker, men »blot« at den ikke må opleves som urimelig bureaukratisk eller virkelighedsfjern. Det kunne heroverfor fremføres, at det i takt med informationssamfundets udbredelse er blevet mere naturligt at have en retlig beskyttelse af personoplysninger, og at der hermed er større grobund for retlig kontrol, men selv ud fra denne iagttagelse må det fortsat lægges til grund, at et stort bureaukratisk apparat lægger gift ud for databeskyttelsesretten.

Herved nærmer vi os det andet problem, der består i, at en generel anmeldelsesordning kun har mening, såfremt tilsynet har tilstrækkelige ressourcer til at behandle de indkomne anmeldelser. Det vil ikke være tilfredsstillende, om de blot bliver registreret som modtagne, og det er da også på andre områder praksis i det danske datatilsyn, at anmeldelser, uanset at der ikke samtidig søges om tilladelse, som overvejende hovedregel bliver underkastet reali-

tetsbehandling.⁴ Der foretages en vis vurdering af, om den anmeldte behandling fremtræder som lovmæssig. Efter loven er denne praksis næppe absolut påkrævet, men desuagtet kan det siges at være forudsat, at tilsynet faktisk læser de anmeldelser, det modtager. I modsat fald kan de indgivne anmeldelser let komme til at virke som en art ansvarsfraskrivelser. Dette er ikke nogen umulig opgave, men det er en omfattende opgave, der forudsætter afsætning af ressourcer. Det er næppe alle medlemsstaternes tilsyn, der administrerer deres anmeldelsesordning på denne måde.

En vis finansiering kan tilvejebringes via gebyrer, som det er tilfældet i den eksisterende tilladelsesordning efter § 50(2), idet det kan bemærkes, at det eksisterende gebyr på 1.000 kr. næppe virker afskrækkende og dermed ikke afholder nogen virksomhed fra at angive ansøgning. Dette gebyr har i dag hovedsageligt en symbolsk karakter og modsvarer næppe i noget tilfælde de faktiske omkostninger ved vurderingen af ansøgninger. Som nævnt i kapitel 6 er tilladelser efter § 27(4) af noget uransagelige grunde ikke selvstændigt gebyrbelagt.⁵

Her i landet har det hidtil været opfattelsen, at der ikke bør anvendes omkostningsbestemte gebyrer, hvilket indebærer, at det er staten, som hovedsageligt må finansiere en udvidet anmeldelsesordning. Det kan dog overvejes, om det er hensigtsmæssigt, at det fulde databeskyttelsesretlige apparat finansieres af staten. Der er en betydelig økonomisk interesse forbundet med de kommercielt betingede dataoverførsler, og især ved brugen af de særlige ordninger, der er beskrevet i kapitel 6, kan et omkostningsbestemt gebyr være velbegrundet. Differentierede gebyrer bør overvejes, idet det tilføjes, at et realistisk gebyr ikke kan antages at medføre, at overførselsordningen i et større omfang end i dag søges omgået.

Det er et almindeligt og måske ubesvarligt spørgsmål, hvor store ressourcer staten bør anvende for at sikre sine borgere en forsvarlig databeskyttelse. Konkret beror svaret på en politisk prioritering i forhold til de mange andre opgaver, staten skal/vil varetage sammenholdt med skattebyrden. Et naturligt udgangspunkt kan være, at der må være en vis realitet i den gældende lovgiv-

4. I forhold til persondatabehandling med henblik på forskning og statistik, jfr. § 10, foretages dog en mindre intensiv prøvelse, hvorved bemærkes, at det største antal anmeldelser vedrører denne form for behandling.

5. Det er ikke efter forarbejderne ganske klart, hvorfor tilladelser i medfør af § 27(4) ikke er medtaget i gebyrreglen i § 63(2). Det nævnes i Betænkning 1345/1997 p.516, at reglen svarer til § 26(2) i lov om private registre, men denne regel nævner (nr.8) specifikt tilladelser efter denne lovs § 21. Der synes at være tale om lidt af en lapsus, specielt når det tages i betragtning, at § 27(4) tilladelserne er de mest krævende for tilsynet.

Kapitel 7 Håndhævelse

ning, og at der foreligger en EU-retlig forpligtelse til at sikre, at der op til et eller andet niveau er den databeskyttelse, som det implementerede direktiv i loven angiver. En mere præcis forudsætning om en bestemt ressourceanvendelse kan ikke udledes af direktivet, og spørgsmålet ses ikke at have været drøftet i artikel 29-gruppen. Som nævnt i kapitel 4 illustreres direktivets tavshed af den varierende ressourceafsætning til datatilsynene i de forskellige medlemsstater.

I forhold til anmeldelsesordningen kan det konstateres, at direktivet (artikel 18-20) overlader betydelige frihedsgrader til medlemsstaterne. Der foreligger således ikke nogen særlig præcis forpligtelse til at lade et bestemt udsnit af persondatabehandlingerne underkaste et anmeldelseskrav, jfr. herved præambelens betragtning 49. Det kan retspolitisk diskuteres, om der i dag fra statens side afsættes tilstrækkelige ressourcer, men selvom det antages, at dette ikke er tilfældet, er det dog nærliggende, at der er andre områder af den databeskyttelsesretlige regulering, hvor en større afsætning af midler vil kunne gøre mere gavn end den, der kan opnås ved en generel anmeldelsesordning for dataoverførsler.

Det konkluderes derfor her, at en udvidet anmeldelsesordning ikke er nogen farbar vej. Spørgsmålet er på denne baggrund, om den nuværende ordning fungerer tilfredsstillende, idet der herved bortses fra spørgsmålet, om den altid bliver brugt eftersom det i første omgang kun er de lovlige overførsler, som drøftes. Det er ikke indtrykket, at ordningen af de dataansvarlige bliver opfattet som særlig byrdefuld, og § 50(2)-gebyret er som tidligere nævnt ikke afskrækkende. Tværtimod giver ordningen ofte en vis betryggelse, fordi den danner udgangspunkt for en dialog, der skaber et sikkert grundlag for dataoverførslen, hvilket især beror på, at overførsler i medfør af § 27(1), uanset de hermed forbundne betænkeligheder, forudsætter en tilladelse, jfr. hertil i kapitel 5. For mange dataansvarlige repræsenterer en dataoverførsel noget retligt uoverskueligt, hvorfor det skaber tryghed, at tilsynsmyndigheden kan konsulteres og sikre, at overførslen er lovlig. Dette skaber en vis sikkerhed imod efterfølgende kritik. Tilsynets proaktive funktion er dermed en væsentlig del af dets virksomhed på dette område.

Det kan i denne forbindelse overvejes, om Datatilsynet kan narres i den forstand, at der under sagsbehandlingen overses kritiske punkter fordi disse er blevet maskeret af den virksomhed, som søger tilladelsen. Sådanne tilfælde kan vel forekomme, men det er dog det almindelige indtryk, at i hvert fald det danske tilsyn foretager en meget omhyggelig sagsbehandling, og at givne tilladelser dermed i almindelighed er velbegrundede, jfr. yderligere under 5. Det er vist nok kun yderst sjældent, at det efterfølgende viser sig, at væsentlige forhold er blevet overset.

3. Selvkontrol

En større anvendelse af de i kapitel 6 omtalte særlige ordninger vil være byrdefuld for tilsynet, og løses dette problem ikke via en indførsel af et realistisk gebyr, vil det kunne være nødvendigt at tilføre tilsynet yderligere ressourcer. Især et større antal ansøgninger om godkendelse af BVR, hvor vurderingen ikke kan støttes på et retningsgivende paradigme, vil kunne udløse en sådan situation. Bortset fra disse mulige ressourceproblemer kan det alt i alt sammenfattende lægges til grund, at den nuværende ordning er velfungerende under alle implicerede parterers perspektiv.

3. Selvkontrol

En anden metode til at sikre, at dataoverførsler finder sted på en regelret måde, udgøres af de registreredes selvkontrol, der bl.a. kan give sig udtryk i klager til Datatilsynet. I de gældende ordninger er der på forskellig måde indbygget regler om information til de registrerede og der er dermed søgt tilvejebragt et grundlag for, at de registrerede kan vogte deres interesser, jfr. lovens rettighedskatalog. Det er ikke realistisk at skabe fuld transparens, men en vis åbenhed foreligger dog. Selvkontrol via klage til tilsynet er dog en metode, som der ikke skal fæstnes for meget tillid til i den forstand, at det er sjældent, at de registrerede tager et sådant initiativ. Det er en international erfaring, at der er meget få klager i relation til dataoverførsler. Dette kan ikke tages som udtryk for, at alt er i sin skønneste orden. Den lave klagefrekvens skyldes ikke, at de registrerede er ligeglade eller altid er tilfredse, men at dataoverførsler er svært gennemskuelige. Hertil kommer, at klagemuligheden næppe er kendt af alle, og at dette at klage opfattes i sig selv som krævende, selvom der ikke er bestemte formaliteter, som skal overholdes i denne sammenhæng.

Det er i realiteten kun ressourcestærke personer, der kan gennemføre en sådan selvkontrol, og i mange tilfælde er det ikke sådanne personer, som har det største behov for at beskytte deres personlige integritet. Der vil således let kunne opstå en slagside, såfremt der lægges for megen vægt på denne mulighed, selvom den selvsagt skal foreligge. I almindelighed kan det som en tilføjelse hertil fremhæves, at den rationalitet, som er indbygget i anerkendelsen af de registreredes informationelle selvbestemmelsesret, i praksis har sine væsentlige begrænsninger.

4. Tilsynssamarbejde

Overførsler omfatter i sagens natur flere lande, og det er i en del tilfælde ikke tilstrækkeligt, at det enkelte nationale tilsyn udøver kontrol. Der er behov for, at myndighederne samarbejder, således at der kan ske håndhævelse på tværs af grænserne.⁶ I forhold til vurdering af dataoverførsler er det på denne baggrund væsentligt, at Datatilsynet indgår i et forholdsvis tæt samarbejde med andre tilsynsmyndigheder, idet dette særligt er tilfældet inden for EU, jfr. direktivets artikel 28, og i Norden. I forbindelse med dette samarbejde kan tilsynet blive opmærksom på overførsler, der bør undersøges nærmere. Dette vil især være tilfældet i forhold til virksomheder, der opererer i flere medlemsstater. Dette samarbejde har ligeledes betydning når tværgående ordninger som BVR konkret skal vurderes, jfr. herom i kapitel 6 samt ovenfor. Den generelle meningsudveksling inden for artikel 29-gruppen kan ligeledes give en vis inspiration. Der er i mange henseender behov for, at samarbejdet løbende holdes ved lige og udbygges. Det er forventeligt, at tværgående koordinering af den databeskyttelsesretlige regulering bliver stadig mere vigtig.

Et vist samarbejde med tilsynsmyndigheder i tredjelande foreligger også, men på et betydeligt mindre intensivt niveau. Hertil kommer, at der i de fleste tredjelande ikke findes en sådan myndighed, jfr. yderligere sidst i kapitlet. Internationale kontakter uden for EU kan dog fortsat medføre, at ulovlige overførsler bliver opdaget.

Det kan overvejes, om samarbejdet mellem tilsynsmyndighederne især inden for EU yderligere kan intensiveres, hvilket bl.a. vil kunne medvirke til at udjævne nogle af de forskelle i tilsynspraksis, der i dag foreligger. En mulighed kunne være udveksling af medarbejdere mellem de forskellige tilsyn. Der vil givet være en lang række praktiske vanskeligheder forbundet med en sådan ordning, men medarbejderudveksling vil også kunne vise sig frugtbar og styrke mulighederne for en bedre synergi både med hensyn til håndhævelse og i forhold til andre aspekter af overførselsproblemet. Selvom man mødes i artikel 29-gruppen og andre fora, vil en medarbejderudveksling kunne være nyttig, og mulighederne herfor bør undersøges nærmere.

6. I OECD vil spørgsmålet om cross border enforcement of privacy være et prioritetsområde i 2006.

5. Er de lovlige overførsler lovlige?

5. Er de lovlige overførsler lovlige?

Det er vanskeligt generelt at bedømme, hvorvidt de dataoverførsler, der sættes i værk inden for de lovbestemte rammer, altid i praksis faktisk er fuldt ud lovlige. I denne sammenhæng er gennemførelse af inspektioner et nyttigt middel for tilsynet. Ifølge POL § 62(3) kan inspektioner gennemføres, når overførslen er omfattet af § 50(2), medens bestemmelsen ikke henviser til § 27(4), idet det dog ved tilladelser efter denne bestemmelse vil være muligt for tilsynet at fastsætte et vilkår herom på samme måde som denne mulighed er indbygget i nogle af de særlige overførselsgrundlag. Inspektioner kan i nogle tilfælde være i eksportvirksomhedens interesse, eftersom det kan understøtte virksomhedens troværdighed, at en udenforstående instans har gennemgået de anvendte fremgangsmåder m.v. Inspektioner er dog tidskrævende, og udgør en belastning af tilsynets ressourcer. De kan derfor ikke anvendes systematisk, men selvom inspektioner har karakter af stikprøver, må de betragtes som et virksomt middel.

Inspektionsadgangen udgør dog ikke nogen garanti for, at overførsler i alle henseender er lovlige, idet det må fremhæves, at Datatilsynet normalt ikke forestår inspektioner i importlandet. Selv i de tilfælde, hvor en sådan inspektion er retligt mulig, vil den sædvanligvis ikke være ressourcemæssigt realistisk. I hvilken udstrækning de overførte oplysninger behandles på lovlig måde, herunder i overensstemmelse med fastsatte vilkår, kan i en del tilfælde kun bero på formodninger, jfr. yderligere om denne problemstilling under 11. Det er dog det generelle indtryk, at den eksisterende ordning er velfungerende og skaber grobund for velordnede og betryggende overførsler. Det kan lægges til grund, at danske virksomheder gennemgående har en intention om at respektere de vilkår, som gælder for den konkrete overførsel. Der er en formodning for, at reguleringen virker effektivt i forhold til de dataansvarlige, som anvender den. Der er derfor i almindelighed grund til at formode, at disse overførsler rent faktisk er lovlige.

6. Ulovlige overførsler

Som nævnt indledningsvis kan det ikke antages, at det er alle dataansvarlige, der følger de fastsatte fremgangsmåder og søger de påkrævede tilladelser. Det må formodes, at der foretages en del overførsler uden om de gældende regler. Nogle gange helt bevidst og andre gange grundet ukendskab til reglerne, som det erfaringsmæssigt er vanskeligt at gøre alment kendte. For internationale virksomheder er det naturligt, at oplysninger kan overføres, og derfor kan det

Kapitel 7 Håndhævelse

overses, at der er fastsat regler herom. En konstant retsinformatisk indsats er utvivlsomt påkrævet, og det må tages i betragtning, at det erfaringsmæssigt tager lang tid, før nye regler (2000!) bliver kendt af alle.

Ulovlige overførsler er naturligvis uønskelige, og spørgsmålet er, hvad der ud over information kan gøres for at undgå, at de finder sted, eller mere realistisk for at reducere deres antal. Der findes ikke noget gyldent svar på dette spørgsmål, men i denne forbindelse er det naturligt at interessere sig for, hvilke konsekvenser for den dataansvarlige der er forbundet med, at en ulovlig dataoverførsel bliver opdaget.

7. Straf

Hovedbestemmelserne om dataoverførsler er strafsanktionerede i POL § 70(1). Dette gælder efter nr.1 for overtrædelse af §§ 27(1) og 50(2), efter nr.2 for ikke at efterkomme afgørelser i medfør af §§ 27(4) og 50(2), samt efter nr.5 for at tilsidesætte vilkår fastsat efter §§ 27(4) og 50(5), idet det således kan bemærkes, at overtrædelse af § 27(3) ikke selvstændigt er strafsanktioneret. Sidstnævnte har især betydning for de dele af bestemmelsen, der ikke er omfattet af tilladelseskravet i § 50(2).⁷ Straffelovens almindelige regler, jfr. især § 264d om uberettiget videregivelse af private oplysninger, finder ligeledes anvendelse og har betydning i forhold til enhver overførsel.

Formelt er overførselsbestemmelserne således taget alvorligt, men selv under hensyntagen til, at strafferegleres præventive betydning ikke må overdrives, er det af betydning, om sanktionsstørrelsen kan gøre indtryk på en dataansvarlig virksomhed. På dette område foreligger der store forskelle mellem EU's medlemsstater, hvor det strengeste niveau vistnok er anlagt i Spanien⁸ med Frankrig og Italien lige efter, medens niveauet her i landet sædvanligvis er forholdsvis lavt, og for mange virksomheder ikke kan fremtræde som særligt afskrækkende. Dette er herved forudsat, at det anvendte niveau ved nationale overtrædelser betragtes som retningsgivende ved sanktioneringen af ulovlige overførsler, idet der så vides ikke i dag findes tilfælde, hvor en ulovlig overførsel har medført straf. Samlet er risikoen for straf ikke af et sådant omfang, at den i sig selv hindrer, at ulovlige overførsler finder sted.

7. Det kan dog bemærkes, at en overtrædelse af § 27(3) i sig selv vil implicere en overtrædelse af § 27(1), da der i så fald sker eksport til et land, der ikke som foreskrevet har et tilstrækkeligt beskyttelsesniveau.

8. Her opereres med et bødeniveau på op til 600.000 euro. Det kan nævnes, at der i Spanien er et stort antal retssager, idet tilsynet får medhold i de fleste af disse.

8. Erstatning

I denne forbindelse er der grund til at fremhæve, at i modsætning til i visse medlemsstater er det ikke Datatilsynet, der udmåler sanktioner, idet tilsynet må henvise sådanne sager til politiet, der ganske vist kan rådføre sig med tilsynet, men som ikke selv er særlig fortrolig med personoplysningsloven. Dette kan medføre en vis afsvækkelse af den intensitet, hvormed sådanne sager bliver gennemført, og det kan diskuteres, om tilsynet burde være tillagt en selvstændig kompetence. Dette er et almindeligt spørgsmål angående databeskyttelsesrettens sanktionering og den måde, det danske retssystem traditionelt struktureres på. Dette spørgsmål vedrører ikke specifikt overførsler, hvorfor problemstillingen ikke skal følges nærmere her. Det skal dog bemærkes, at forskellene i tilsynskompetence på ny illustrerer disharmonierne inden for EU og den fristelse til forumshopping disse kan give anledning til. Det kan for en international koncern eksempelvis fremtræde som mere tillokkende at eksportere data fra Danmark end fra Spanien.

8. Erstatning

Risikoen for at ifalde et erstatningsansvar er ej heller afskrækkende. En registreret kan gøre et erstatningskrav gældende, jfr. herved POL § 69 samt direktivets artikel 23. Det fastsættes her, at der skal betales erstatning for skader forvoldt ved ulovlig databehandling, medmindre den dataansvarlige godtgør, at skaden ikke kunne være afværget (præsumptionsansvar). Det er i praksis en sjældenhed, at en registreret gør et erstatningsansvar gældende. Skulle et sådant krav blive gennemført med succes, er det velkendt, at erstatningsudmålingen i Danmark normalt er placeret på et forholdsvis beskeden niveau, selvom der har været en stigende tendens de senere år. Det har således sandsynligheden imod sig, at et udmålt erstatningsbeløb blot nogenlunde vil modsvare de økonomiske fordele, der kan være forbundet med en dataoverførsel.⁹ Der findes dog ikke nogen retspraksis, der nærmere kan belyse dette.

Det bør hertil føjes at selv små erstatninger kan tjene et fornuftigt formål, fordi de symbolsk over for de registrerede demonstrerer, at der er begået en eller anden fejl, og at retssystemet tager dette alvorligt. Det er ikke nødvendigvis erstatningens størrelse, som er afgørende for de registrerede, men for mange dataansvarlige er dette dog i sagens natur væsentligt.

9. Det kan herved bemærkes, at massesøgsmål, class actions, ikke anvendes i dansk ret.

9. Offentlighed

Det er noget mere uformelle risici, der kan medføre, at en ulovlig dataoverførsel ikke søges gennemført. Denne risiko består i dårlig offentlig omtale som følge af, at overførslen bliver taget op i massemediernes. For at denne risiko skal foreligge og i øvrigt gøre indtryk, må det forudsættes, at den dataansvarlige virksomhed har en vis størrelse og er synlig på markedet. Som det er blevet bemærket, er elefanter på dette område mere sårbare end myg. Er der tale om en synlig virksomhed, kan kritisk omtale have endog store økonomiske konsekvenser, idet et dårligt image kan indebære tab af markedsandele.

Risikoen for et reduceret omdømme har en vis præventiv virkning og medfører sikkert lidt færre ulovlige overførsler, men risikoen er særdeles uberegnelig og aktualiseres nok primært i tilfælde, hvor der er større eller særligt synlige skadevirkninger forbundet med den foretagne overførsel. Dette kan være tilfælde, hvor overførslen omfatter et stort antal registrerede eller angår særlig følsomme persondata. Som det er velkendt, er det umuligt at forudsige, hvilke sager massemediernes fatter interesse for, men netop derfor er der tale om en risiko, som udgør et urovækkende usikkerhedsmoment, som den dataansvarlige derfor må kalkulere med. Årvågne medier kombineret med årvågne borgere er et godt middel imod ulovlige overførsler.

10. Datapoliti

Det har undertiden været foreslået, at der skulle oprettes en art datapoliti med den opgave at efterforske og opspore overtrædelser, herunder ulovlige dataoverførsler. Dette kan ikke anses for noget realiserbart forslag, allerede fordi det vil kræve afsætning af betydelige ressourcer samt kunne medføre usikkerhed om forholdet mellem Datatilsynet og et sådant datapoliti. Ideen om et datapoliti peger dog på, at græsrodsbevægelser (ngo'er) kan spille en rolle på dette område. Dette gælder særligt, hvis de indgår i et internationalt samarbejde, eftersom det ofte vil være hos importøren, at den ulovlige overførsel opdages. Ngo'er, eksempelvis Privacy International, vil kunne iværksætte deres egen form for efterforskning, og vil ofte være besjælet af den tilstrækkelige ildhu til, at den kan medføre resultater, som kan benyttes af de formelle datatilsyn. Der er en vis aktivitet på området, som først og fremmest har karakter af en form for overvågning af bestemte virksomheder, der mistænkes for en uheldig praksis, men der er dog vist nok ikke her i landet eksempler på, at ulovlige overførsler er blevet afsløret på denne måde.

11. I importlandet

Særlige problemer foreligger i henseende til persondatabehandlingen i importlandet, når dette er et utilstrækkeligt tredjeland. Her sker behandlingen uden for Datatilsynets jurisdiktion, fjernt fra de registrerede og ligeledes fjernt fra de hjemlige massemedier. I det omfang sådan dataeksport lovligt finder sted, er der i en vis udstrækning, jfr. kapitel 6, søgt indbygget mekanismer, der skal sikre, at behandlingen sker på et velordnet grundlag. Sikkerhed for regeloverholdelse er ligeledes søgt tilvejebragt i disse tilfælde, medens overførsler på grundlag af § 27(3) må betragtes som noget mere usikre.

Der foreligger dog i alle tilfælde en betydelig usikkerhed, der er særlig stor i de lande, hvor der ikke findes myndigheder, som kan bistå med en vis kontrol, og hvor domstolene er uvante med sager af denne karakter. Personoplysningerne befinder sig meget bogstaveligt i et fremmed land. Hvorvidt persondatabehandlingen gennemføres på en regelret måde, er i sidste instans et spørgsmål om tillid til, at importøren faktisk vil overholde de databeskyttelsesretlige forpligtelser. De retlige instrumenter kan i realiteten ikke fuldt ud sikre dette. I mange tilfælde vil denne tillid sikkert være berettiget, men næppe i alle.

For så vidt angår de ulovlige overførsler må det blot konstateres, at er personoplysningerne først nået frem til et sådant importland, er de uden for kontrol. Ofte vil de uopdaget kunne benyttes til hvad som helst i sådanne data havens, hvorfra de vil kunne blive videregivet til tilsvarende steder. Når integritetskrænkelsen manifesteres, vil det ofte ikke være muligt at gennemføre nogen reaktion. Det er denne situation, som altid har udgjort den internationaliserede databeskyttelsesrets skrækscenario.

12. Vær beredt!

Uanset det foran anførte er der dog ikke grund til at overdrive usikkerheden i forbindelse med kommercielt orienterede dataoverførsler. De fleste virksomheder vil, i det omfang de kender reglerne, bestræbe på at overholde dem og handle lovmæssigt. De har en naturlig interesse i en sådan troværdighed. Under alle omstændigheder kan det konstateres, at der ikke her i landet har været egentlige skandaler i relation til dataoverførsler. Som en art caveat må tilføjes, at de i hvert fald ikke er blevet opdaget.

Intet nyt fra vestfronten betyder dermed ikke, at situationen er problemfri, og det må stadig overvejes, på hvilken måde større efterlevelse af reglerne kan fremmes, uden at dette sker ved opbygningen af et ekstensivt kontrolap-

Kapitel 7 Håndhævelse

parat. Årvågenhed og omhyggelighed kombineret med information om reglerne og deres begrundelse må være kodeordene således at man ikke falder i den grøft, der består i, at der bliver etableret et bureaukrati, som skader databeskyttelsen renomme og dermed på sigt måske ligefrem modvirker den effektivitet, der skulle være målet.

KAPITEL 8

En ny løsning?

1. Det globale problem

Kun et mindre antal lande har under et europæisk perspektiv en tilfredsstillende retlig beskyttelse af personoplysninger. Store og for verdenssamfundet væsentlige lande som eksempelvis Kina, Indien, Brasilien og Rusland er ikke med i denne eksklusive kreds. Under det samme perspektiv er USA på mange måder et databeskyttelsesretligt u-land. Så længe ikke alle eller i hvert et overvejende flertal af lande har en retlig regulering, som i fællesskab anerkendes som udtryk for et tilfredsstillende beskyttelsesniveau, vil der være et overførselsproblem, medmindre principielt nye reguleringsmodeller vinder indpas, jfr. nedenfor især under 7. Der er ikke nogen udsigt til, at overførselsproblemet vil forsvinde af sig selv inden for en overskuelig tidshorisont. Databeskyttelse er i mange lande noget fremmed i forhold til den retlige tradition og kultur, og derfor er der ikke indtil videre nogen grund til at forvente en global opbakning til en sådan beskyttelse; i hvert fald ikke på det høje niveau, hvor denne er placeret i den EU-retlige regulering. Er man sympatisk indstillet over for databeskyttelse, er EU et foregangsområde, men under det globale perspektiv kan det overvejes, om man er kommet for langt foran.

Selvom overførselsproblemet første og tredje dimension, at behandlingen skal være lovlig inden for eksport- og importlandet, til stadighed i sig selv vil kunne give anledning til vanskeligheder og medføre, at den nationale regulering virker som en blokering, er det først og fremmest konsekvenserne i forhold til den anden dimension og dermed den manglende mulighed for at foretage overførsler, der repræsenterer en retlig udfordring i forhold til en aspiration om at tilvejebringe en velfungerende international regulering. En udfordring, som kun i dag i et vist omfang er blevet besvaret. Selvom der i EU i de senere år er udviklet ordninger, der kan medvirke til at reducere overførselsproblemet, er der ingen tvivl om, at dette fortsat er stort.

Kapitel 8 En ny løsning?

Dette skyldes først og fremmest, at behovet for at styrke og udvikle international handel og i denne sammenhæng at fremme globaliseringen møder en barriere i form af de databeskyttelsesretlige krav. Nutidens internationale økonomi beror bl.a. på at der let og smidigt kan ske udveksling og cirkulation af personoplysninger, og under dette perspektiv er det uønskeligt, at der findes snærende retlige bånd.¹ Anvendelse af informationsressourcer er en central del af moderne økonomi, og moderne informationsteknologi nedbryder i sig selv grænsernes betydning.² På denne baggrund er den nuværende retlige situation globalt betragtet ikke tilfredsstillende, og den foreliggende disharmoni mellem økonomi og ret giver bl.a. anledning til den tro, at reguleringen i et vist og måske endda i et stort omfang ikke bliver respekteret i praksis, jfr. herom i kapitel 7. Der er en ikke helt bestemmelig diskrepans mellem virkelighed og ret.

2. Virksomhedsinteresse

Under det erhvervsmæssige perspektiv er det ikke en aspiration, at der skal være en ubegrænset frihed til at behandle persondata, og at der ikke skal være nogen form for databeskyttelsesretlige krav, som skal opfyldes af virksomhederne. Det er i hvert fald ikke tilfældet for den »pæne« del af erhvervslivet. I den nutidige forståelse af corporate governance, der dog ikke kan antages at have en ensartet global udbredelse, er der en anerkendelse af, at virksomheder har et ansvar, der rækker ud over den profitmaksimering, som fortsat er den egentlige målsætning. Bredt beskrevet er der en accept af, at erhvervsvirksomheder har et samfundsmæssigt ansvar, og at dette betyder, at de skal forfølge deres kommercielle mål bl.a. med en hensyntagen til de personer, som aktiviteterne berører. Virksomhedens interesse skal i hvert fald i et vist omfang fremmes med respekt for ansattes og kunders integritetsinteresse. Moderne virksomhedskultur er dermed ikke uforenelig med databeskyttelse. I denne kontekst kan en retlig regulering ses som en hjælp til varetagelse af dette mål, selvom der som tidligere fremhævet kan være uenighed om, hvorvidt denne regulering først og fremmest skal komme oppe fra eller have karakter af selvregulering.

1. I APEC Privacy Framework 2005 fremhæves, at man må anerkende »the free flow of information as being essential for both developed and developing market economies to sustain economic and social growth«.
2. Raymond Wacks: *Law, Morality and the Private Domain* (Hong Kong 2000) p.323: »The new information technology disintegrates national borders«.

2. Virksomhedsinteresse

De dataansvarlige virksomheder har en selvstændig interesse i at underlægge sig en vis databeskyttelse. Det kan have positiv betydning for virksomhedens drift, at kunder og ansatte oplever at virksomheden behandler deres data på en forsvarlig måde og især ikke misbruger eller skaber grundlag for misbrug af oplysningerne. Herved sendes der et signal om respekt for personlig integritet. Selvom det er vanskeligt mere præcist at indkredse, hvilken forventning om databeskyttelse der faktisk findes i dag,³ er der næppe nogen tvivl om, at der er en vis forventning herom, og at en imødekommelse af denne kan have økonomisk betydning. Den under denne synsvinkel gode virksomhed vil fremtræde positivt på markedet og af denne grund stå sig bedre i konkurrencen. Disse iagttagelser vedrører virksomheder, der er synlige på markedet og har et omdømme af økonomisk betydning. På internationalt niveau er det mere sandsynligt, at virksomheden har denne karakter, end tilfældet er nationalt, hvor der, som tilfældet er i Danmark, kan være en ur-skov af meget små virksomheder.⁴

En generelt fastsat retlig regulering kan i øvrigt have en yderligere fordel, såfremt den fungerer effektivt, idet den kan betyde, at databeskyttelse ikke bliver et konkurrenceparameter. Dette skyldes, at de udgifter, denne regulering indebærer, på denne måde vil være ens for alle virksomheder, og på denne måde vil konkurrencebetingelserne være lige, idet det herved forudsættes, at der ikke »snydes på vægten«. Betragtet på denne måde er der en interesse i en harmoniseret præcis regulering, som også på andre måder vil kunne medføre en omkostningsbesparelse. Dette gælder ikke mindst i forhold til reguleringen i importlandene, idet en samordning heraf medfører et reduceret behov for anvendelse af bl.a. juridiske ressourcer til at afklare speciel national regulering. En fuldstændig harmonisering er næppe mulig, men man kan dog sikkert komme betydeligt længere, end tilfældet er i dag.

Det lægges dermed til grund, dels at det ikke er modstrid med en erhvervsmæssig interesse, at der er en databeskyttelsesretlig regulering så længe denne ikke er for bureaukratisk og byrdefuld, dels at det erhvervsmæssigt er et attraktivt mål, at der gælder samme regler for virksomheder i alle lande,

3. Der kan spores en vis tendens til, at privathed ikke tillægges helt den samme betydning som tidligere, jfr. hertil Peter Blume: Databeskyttelsesret (2.udg. København 2003) p.318-19, men det er ikke muligt præcist at indkredse denne tendens.

4. På Internettet operer dog også mange små virksomheder, som ikke oplever en interesse i databeskyttelse. Selvom Spam ikke i første række er et databeskyttelsesretligt problem, illustrerer dette fænomen det anarki, som i et vist omfang karakteriserer nettet. En ny retlig regulering vil ikke løse ikke alle problemer, jfr. herved også i kapitel 7.

Kapitel 8 En ny løsning?

herunder at de på ens betingelser kan gennemføre de dataoverførsler, som er nødvendige i den internationale økonomi.

3. Den registreredes interesse

Tages der således udgangspunkt i den dataansvarliges behov, foreligger der en interesse i en løsning af overførselsproblemet. Under individernes, de registreredes, perspektiv er dette i og for sig også tilfældet. Dette skyldes, at internationaliseringen indebærer fordele for borgerne, og at det overordnet ligeledes er i deres interesse, at økonomien er velfungerende. De registrerede er også borgere og forbrugere. Integritetsinteressen er væsentlig og skal tages alvorligt, men den bør i en vist udstrækning afpasses i forhold til interessen i økonomisk vækst og udvikling.

På denne baggrund bør dataoverførsler ganske vist ikke medføre en krænkelse af den enkelte borger, men den regulering, som skal sikre dette, behøver ikke at være rigoristisk. Dette indebærer, at eksempelvis en regulering, hvorefter personoplysninger udelukkende kan overføres, såfremt der foreligger et samtykke, sikkert af de fleste registrerede vil blive opfattet som for usmidig. Samtidig vil en sådan ordning prisgive de registrerede, som ikke kan overskue de konsekvenser, som kan være forbundet med et samtykke. Et ubetinget krav om samtykke vil kunne begrænse overførsler, der reelt er i den registreredes interesse, og ligeledes i realiteten muliggøre overførsler, som er skadelige for den registrerede. Gældende ret er ikke baseret på et sådant absolut samtykkekrav, der sikkert af nogen vil blive betragtet som ideelt, men som fremhævet er en sådan skærpet regulering ikke ønskelig.

Den overordnede interesse for de registrerede er, at personoplysninger er beskyttet imod misbrug med integritetskrænkelser til følge, og at der er en retlig regulering, som effektivt kan sikre dette på det sted, hvor den enkeltes oplysninger faktisk befinder sig. Den registreredes interesse er dermed centreret om importlandet, idet dette ikke nødvendigvis betyder, at reguleringen skal stedsfæstes i dette land. Selvom der som nævnt i kapitel 1 kan argumenteres for en stærkere beskyttelse uden for individets hjemland, medfører internationaliseringen en påvirkning i retning af en større fortrolighed med andre kulturer, hvilket indebærer, at det for de fleste må antages at være tilfredsstillende, at der findes, eller i det mindste er tilstrækkelige garantier for, en tilsvarende beskyttelse, og at en vis transparens ligeledes er etableret. Åbenhed skaber i sig selv tillid.

4. Problemets kerne

På denne baggrund er det muligt at indkredse, hvad overførselsproblemet reelt består i. Kernen repræsenteres af den almindelige opfattelse, at der skal være gensidighed mellem de forskellige landes retlige regulering, således at der foreligger et tilsvarende beskyttelsesniveau. Det skal være muligt at foretage en positiv sammenligning. En løsning af problemet forudsætter således en fundamental tværnational accept af, at personoplysninger bør beskyttes på et bestemt niveau med den konsekvens, at de ikke kan behandles frit. Grundlæggende må der være tilslutning til, at der i en eller anden form må være en retlig regulering, der medfører denne beskyttelse.

Selvom der ovenfor er argumenteret for, at der er en erhvervsmæssig forståelse for dette grundsynspunkt, er dette ikke ensbetydende med, at denne accept er til stede i alle lande. Spørgsmålet om, hvorledes relationen mellem virksomheder og individer skal opfattes, er basalt ideologisk og knyttet til ideer om, hvorledes et samfund bør indrettes. Det er et forholdsvis nyt synspunkt, at denne relation også har en menneskeretlig dimension. Denne indfaldsvinkel refererer således til det forhold, at databeskyttelse vedrører retskultur og dermed traditioner i de enkelte samfund eller stater. Som fremhævet indledningsvis er disse traditioner meget forskellige, og uanset al tale om globalisering er der ikke udsigt til, at forskelle af denne karakter vil blive udlignet eller forsvinde i de nærmeste år. De er meget modstandsdygtige over for forandringer.

En fuldt ud international eller ligefrem global løsning af overførselsproblemet er dermed en meget betydelig opgave, der forståeligt nok af nogle vil blive karakteriseret som utopisk eller i hvert fald meget fjerntliggende. På denne baggrund er det, en lille smule paradoksalt, erhvervslivet, der uanset det ovenfor anførte ofte er skeptisk over for databeskyttelse, som må være den drivende kraft i en sådan proces motiveret af den økonomiske betydning, som dataoverførsler i stigende omfang vil få. Det er behovet for at kunne anvende personoplysninger, som må udgøre den drivende kraft, der fører til forbedrede muligheder for dataoverførsler. Det er grundlæggende persondatas varelignende karakter, der udgør incitamentet.

Hos de interesserede virksomheder må der på dette grundlag oparbejdes en forståelse af, at databeskyttelse udgør en nødvendig pris for at opnå gode muligheder for dataoverførsler, der fremmer profitabilitet. Denne forståelse omfatter en accept af, at der i forbindelse med persondatabehandling er nødvendige ekstra omkostninger. Hvor høj prisen bør være, kan diskuteres, men at der er en pris, bør blot lægges til grund.

5. Tilsvarende niveau

Indtil videre er det styrende princip blevet beskrevet således, at der skal være et tilsvarende beskyttelsesniveau i de forskellige lande. Dette betyder, at de konkrete regler og ligeledes reguleringsmetoder kan være forskellige, idet det er beskyttelsesniveauet, der skal være tilsvarende, jfr. princippet i direktivets artikel 25(2). Så længe niveauet er det samme, er det ikke afgørende set under den registreredes perspektiv, at der bliver benyttet forskellige midler til at sikre dette niveau og på denne måde imødekomme forventningen om privatlivsbeskyttelse. Formelt set ens ret er en umulighed globalt set, og realiseringen af en sådan utopi er ikke nødvendig for at løse overførselsproblemet.

Det kan med en vis ret indvendes, at et princip om tilsvarende niveauer på samme måde, eller endog i større udstrækning end EU-rettens princip om tilstrækkelighed er indholdstomt og ikke angiver noget om, hvilke forpligtelser og rettigheder der skal foreligge. Der er alene tale om et udgangspunkt, som indikerer at der skal være et vist niveau, men det fortæller ikke noget om hvori niveauet består. Formuleringen adskiller sig fra direktivets ved at det mere tydeligt fremhæver sammenlignelighed som det afgørende kriterium. Denne måde at beskrive de retspolitiske aspiration på angiver bedre det mål, som reguleringen efterstræber at opnå: at det for den registrerede er uden betydning, hvor dennes persondata bliver behandlet. Når der lægges vægt på gensidigheden, er konsekvensen, at der startes mere åbent, end når den styrende norm er »tilstrækkelighed«. Dette er ikke nødvendigvis nogen ulempe.

Det vil være en fiktion at tro, at man kan starte oparbejdelsen af en ny regulering med en tabula rasa. Den allerede udviklede retlige regulering skaber naturligt forventninger om en vis form for persondatabeskyttelse. Dette er dog ikke ensbetydende med, at det eksisterende bør udgøre en absolut binding,⁵ jfr. også under 6. Uden at glemme traditionen kan overførselsproblemet betragtes med friske øjne. I denne forbindelse er det et væsentligt retspolitisk spørgsmål, om der i bestræbelserne på at udforme en ny regulering skal tages udgangspunkt i det niveau, der kan udledes af direktiv 95/46. Dette er den aktuelle europæiske position, der, om end det sjældent udtales helt eksplicit, betragter direktivet som den rigtige grundopfattelse og anser størstedelen af verden som uudviklet. Verden bør lære af EU, og alle problemer vil være løst, såfremt dette sker. Den grundlæggende ide om databeskyttelse, der

5. Det er ikke givet, at man som i direktivets præambel betragtning 10 skal lægge til grund, at det nationale beskyttelsesniveau ikke må forringes, når en ny ordning gennemføres. En vurdering heraf beror på, hvor stor vægt dataoverførsler tillægges i den samlede databeskyttelsesretlige regulering.

er koblet til grundrettigheden om privatlivets fred, kan dog konkretiseres og udfyldes på mange måder. Det bør ikke tages for givet, at direktivet repræsenterer den eneste rigtige, selvom det er baseret på den tradition, der stammer fra OECD's retningslinier og Europarådets konvention. Direktivet er blot et stadie på vejen. Hertil kommer, at direktivet fra 1995 efterhånden i lyset af den hastige samfundsudvikling er gammelt, selvom de mere sløve medlemsstater (læs Frankrig) først meget sent (2004) fik det implementeret.

6. En ny start

Tages overførselsproblemet alvorligt, må udfyldningen af den databeskyttelsesmæssige grundtanke betragtes med friske øjne, og det må accepteres, at europæisk retseksport har sine grænser. Dette er lettere skrevet end gjort, eftersom det som også fremhævet ovenfor er svært at løsrive sig fra fortiden/nutiden. Det vil da også være forkert at smide barnet ud med badevandet. Selvom de første ideer om informationel privatlivsbeskyttelse opstår i USA, lang tid før nogen havde tænkt på EU, er der ikke tvivl om, at drivkraften i udviklingen af dette retsområde har været europæisk med Europarådets konvention 1981 og direktivet 1995 som de mest markante fyrtårne.⁶ Det er naturligt at formidle de indvundne erfaringer til den øvrige verden, idet det blot er væsentligt, at den europæiske ret ikke præsenteres som den eneste mulige sandhed, og at den dermed ikke kommer til at virke som en blokering for en global løsning.

Der er blevet tænkt meget, og en række vigtige rettighedspositioner er blevet udviklet. Denne retlige produktion har taget udgangspunkt i borgernes interesse, men det er ikke dækkende at opfatte de opnåede resultater på den måde, at de ensidigt fremmer denne interesse.⁷ En afbalancering er løbende blevet tilstræbt, og der er en vis realisme indbygget i reguleringen. Det er

6. Det er bekendt, at Kommissionen har overvejet at stille forslag om ændringer af direktivet. Tanken er vist nok ikke opgivet, men det er naturligt, at der tøves, idet et sådant forslag vil åbne Pandoras æske og igangsætte en proces, hvis slutresultat er uforudsigeligt. Tiden vil sikkert kunne bruges til noget bedre, og det er ikke givet, at en større direktivrevision er nødvendig for at løse overførselsproblemet.
7. Det er derfor ikke overraskende, at direktivet ikke blot kritiseres for ikke være lydhør over for den kommercielle interesse, men også kritiseres af andre for ikke at give den registrerede en tilstrækkelig beskyttelse og for at lade privatheden i stikken. En retspolitisk konsensus er svær at forestille sig på databeskyttelsesrettens område.

Kapitel 8 En ny løsning?

dermed ikke noget fremmed, at en hensyntagen til den dataansvarliges interesse må indgå i de retspolitiske overvejelser.

Selvom man er kommet langt, er dette ikke ensbetydende med, at man ikke kan gå andre veje og fortsat realisere de grundlæggende ideer. Det er vigtigt at undgå, at den eksisterende regulering og det retlige apparat eller bureaukrati, som omgiver denne, virker konservativt. Bureaukratiet bør ikke blive selvforstærkende og betragte sin eksistens som en værdi i sig selv. Der bør være åbenhed over for, at der er blevet truffet valg, og at disse valg ikke nødvendigvis alle er hensigtsmæssige og under alle omstændigheder til stadighed kan revurderes. På mange områder har den databeskyttelsesretlige regulering været en succes, men netop i forhold til overførsler har succesen været begrænset, hvilket opfordrer til nytænkning. Den retlige regulering bør ikke stivne og blive til en ortodoksi.

Måske lidt skuffende er det ikke tanken her fuldt udfoldet at beskrive en alternativ vej, idet visse muligheder dog skitseres nedenfor. Hovedærindet her er blot at argumentere for, at der bør være en vis frigjorthed fra direktivet, og endvidere at oparbejdelse af en generelt dækkende retlig ramme om dataoverførsler må være baseret på det enkle udgangspunkt, at der i de forskellige lande må være et vist beskyttelsesniveau, der kan anskues som tilsvarende. Udfyldningen af denne norm bør ikke være snævert bundet til den eksisterende udfyldning af direktivets brede regler. Den gamle frygt for overførsler til lande uden nogen form for databeskyttelse er fortsat berettiget, hvorfor der netop må foreligge et vist niveau, eller måske snarere må overførsler forudsætte, at der er sikkerhed for, at overførte oplysninger behandles i overensstemmelse med dette niveau. Hvori dette bør bestå og især, hvorledes dets anvendelse kan sikres, bør vurderes på ny.

Ved overvejelser om udformningen af en alternativ regulering er det på den ovenfor nævnte baggrund en nærliggende mulighed at opsplitte overførselsproblemet i to spørgsmål, der nok er sammenhængende, men hvis besvarelse ikke nødvendigvis er sammenfaldende. Der kan skelnes mellem på den ene side en generel eller almindeligt dækkende ordning, der svarer til den situation, at EU godkender et tredjeland, og på den anden side regulering, der giver mulighed for konkrete overførsler. I det følgende tages udgangspunkt i denne opdeling, idet temaet under 7 er den konkrete overførsel, medens temaet under 8 er de generelt dækkende løsningsmodeller. Ved i højere grad end i gældende ret at adskille disse to momenter er der en mulighed for, at der både på kort og langt sigt kan gøres fremskridt.

7. Forholdet til national ret

I forbindelse med overvejelser om, hvorvidt en revurdering af overførselsmulighederne eventuelt kunne realiseres, er der grund til at tage stilling til, om denne vej er farbar i forhold til den nationale ret. Det er ikke blot direktivet, men også den nationale ret, herunder personoplysningsloven, som fremtræder som indarbejdede kendsgerninger, der er kommet til verden over mange år med investering af betydelige ressourcer. Som tidligere fremhævet er direktivets udfyldning i betydelig udstrækning national, og dermed repræsenterer den nationale ret et selvstændigt startpunkt for de videre overvejelser. Selvom dette lægges til grund, vil en revision af den europæiske opfattelse kunne medføre, at også den nationale lovgivning må ændres, og en sådan revision kan på nogle punkter indebære en reduktion af det foreliggende nationale beskyttelsesniveau. Spørgsmålet er, om dette vil være acceptabelt, eller dette vil være en for høj pris at betale blot for at sikre internationale dataoverførsler, som givet af mange borgere ikke opfattes som noget, der er nærværende i deres dagligdag. Det er sandsynligt, at der på denne baggrund vil være en betydelig modstand at vælge en ny vej.

Et muligt svar ville bestå i en opløsning af sammenhængen mellem to af de dimensioner, der er relateret til overførsler. Med andre ord, at man opgav forudsætningen om, at persondatabehandlingen skal være nationalt lovlig i den forstand, at en overførsel ikke betragtes som en behandling, med den konsekvens at der ikke stilles krav om, at de lande til hvilke data overføres opfylder normen om sammenlignelighed, idet det i stedet blot forudsættes, at behandlingsniveauet i importlandet er tilfredsstillende. Eksportørens nationale behandling, eksempelvis indsamling og registrering, skulle fortsat være i overensstemmelse med eksportlandets personoplysningslov, men overførslen som sådan skulle ikke opfylde dette krav. Konsekvensen heraf er, at eksportlandets ret lades uberørt, og overførselsproblemet løses, uden at det nationale beskyttelsesniveau påvirkes, hvilket i sig selv må betragtes som en væsentlig styrke ved en sådan model. En ny regulering af dataoverførsler bliver realiseret, uden at dette indvirker på de krav, der i andre sammenhænge stilles til persondatabehandling. Bedre overførselsmuligheder nødvendiggør ikke nogen forringelse af det nationale beskyttelsesniveau. Denne løsningsmodel indebærer en adskillelse af det nationale og det internationale niveau, hvilket kan opfattes som noget kunstigt i vor tid, men dette kan betragtes som udtryk for en respekt for det lokale i forhold til det globale, jfr. også under 8.

Løsrivelsen af dataoverførsler fra den nationale regulering behøver ikke at betyde, at der overhovedet ikke er nogen regulering. Selvom overførslen ikke betragtes som en behandling, vil der kunne stilles bestemte krav til eksportør-

Kapitel 8 En ny løsning?

ren, således at der opnås en rimelig grad af sikkerhed for, at overførte oplysninger behandles tilfredsstillende i importlandet. Overførsler vil kunne reguleres, uden at de betragtes som behandlinger. En konsekvens af denne reguleringsmodel er, at der udelukkende sættes fokus på eksportlandets ret i den forstand, at dataoverførsler alene beror på, at eksportøren indestår for og er ansvarlig for, at overførte persondata behandles integritetsmæssigt forsvarligt i importlandet.⁸ Det vil kunne beskrives nærmere, hvad en sådan indeståelse skal omfatte, således at det er klart, hvilken forpligtelse eksportøren påtager sig.⁹ Denne indeståelse vil have karakter af en garanti for, at overførslen ikke udsætter de registrerede for en integritetsmæssig risiko. Det kan overvejes at gøre eksportøren objektivt erstatningsansvarlig herfor.¹⁰ En sådan model indebærer en vis afsvækkelse af den offentligretlige styring, selvom der vedrørende behandlingen i importlandet yderligere kan indbygges en rapporteringsforpligtelse til tilsynsmyndigheden i eksportlandet. Modellen har den fordel, at dataoverførsler vil kunne gennemføres på en mere smidig måde, end tilfældet er i dag.

En regulering af denne karakter medfører en principiel forandring af gældende ret. Den indebærer et vist brud med den opfattelse, at fri overførsel forudsætter national regulering. Der vil være tale om et nyt udgangspunkt. I en vis forstand vil den gordiske knude blive hugget over, men spørgsmålet er, om prisen er for høj. Reguleringsmodellen indebærer, at der ikke gælder nogen forudsætning om gensidighed, således som denne forudsætning normalt forstås, idet eksportørens tilkendegivelse af, at de overførte oplysninger behandles integritetsmæssigt forsvarligt, uden videre lægges til grund. I det retspolitiske laboratorium er et sådant skridt ikke nogen umulighed, men der vil være tale om et brud med den databeskyttelsesretlige tradition og ikke mindst med den erfaring, som er indhøstet gennem mange år. Meget taler for, at der i praksis vil være en utilbøjelighed til, uden basis i særlige overførsels-

8. Denne model antydes i APEC Privacy Framework 2005 princip 26 om »accountability«, idet en overførsel enten kan bero på samtykke eller en sådan indeståelse.

Modellen kan minde lidt om den kritiserede ansvarsmodel i 2001-standardkontrakten for dataansvarlige eller ideen om, at eksportøren ved lov skal gøres generelt erstatningspligtig, jfr. i kapitel 6, men modellen understøttes af argumentationen for disse konstruktioner, idet denne refererer til de registreredes reelle muligheder for at hævde deres rettigheder.

9. Selvom der i kapitel 7 er argumenteret imod en almindeligt dækkende anmeldelsesordning, kunne en sådan komme på tale som en del af den her skitserede ordning.

10. Selvom der vil være tale om et brud med dansk tradition, kunne en yderligere mulighed være at give erstatningsansvaret et pønalt præg for herved at understrege situationens alvor.

8. Folkeretligt instrument

grundlag, at acceptere overførsler, såfremt det modtagende land ikke regulerer nogenlunde, som man selv gør. Det var denne erfaring, der gjorde direktivet nødvendigt i relation til medlemsstaternes indbyrdes forhold.¹¹

Intet bør være helligt, men uanset at den her skitserede model kan være tiltrækkende, er denne vej næppe retspolitisk farbar, og det er muligvis også for risikabelt at bevæge sig ud af denne. En fuldt udfoldet model bør dog sættes på det retspolitiske program. Undlader man at køre i denne retning, må man erkende, at en ny løsning af overførselsproblemet uundgåeligt vil påvirke det beskyttelsesniveau, der fastlægges i forhold til den nationale regulering. Det vil være nødvendigt at genoverveje denne regulerings grundlæggende træk med henblik på at opnå sammenlignelighed, hvilket ligeledes må betragtes som et ganske radikalt skridt. Også denne vej vil være lang, og mange forhindringer vil skulle overvindes, inden målet er nået. Vejen kan dog i sidste instans vise sig at være mere farbar, og er der den fornødne opbakning til at skabe et nyt grundlag for overførsler, må dette betragtes som en realistisk mulighed.

8. Folkeretligt instrument

Skal der i forhold til en generel løsning af overførselsproblemet være et lys for enden af vejen, må dette blive tændt ved hjælp af et folkeretligt instrument. Der findes ikke stærkere retlig regulering, som kan tages i anvendelse på globalt niveau, og der må således benyttes en regulering, som formelt er svagere end direktivet, for slet ikke at nævne en forordning for hvis udstedelse der undertiden er blevet argumenteret, jfr. yderligere under 9. Folkeretlig regulering i form af en konvention behøver dog ikke nødvendigvis at være svag i den forstand, at en sådan konvention kan etablere organer, herunder domstole mm., som kan medvirke til at de fastsatte regler bliver overholdt. Ikke alt behøves overladt til konventionsstaterne. Det er dog klart, at der ikke vil foreligge et apparat, der tåler sammenligning med det, som findes i EU, og at sandsynligheden for regeloverholdelse dermed som udgangspunkt er svagere.

Uanset at sådanne betænkeligheder foreligger, lægges det til grund, at det er ved en folkeretlig konvention, der ratificeres og gennemføres af alle bety-

11. Om det i dag reelt er korrekt, at overførsler til en anden medlemsstat i alle tilfælde er mere betryggende end til et ikke tilstrækkeligt tredjeland, er næppe givet, men det må her blive en anden historie.

Kapitel 8 En ny løsning?

dende lande, at der kan opnås en situation, hvor dataoverførsler kan finde sted frit eller i hvert fald friere end i dag. Det kan herved tilføjes, at der i nyere tid er en tendens, der dog næppe er global, til at folkeretlige forpligtelser tages mere alvorligt, end det engang var tilfældet. Folkeretten behøver ikke at være en *lex imperfecta*.

Det kan overvejes, hvorledes en sådan konvention skulle udformes. Et væsentligt spørgsmål i denne henseende er, hvor præcis den bør være. En mulighed er, at aspirationen er at udforme en global standard for databeskyttelse, som har til formål at understøtte en global kultur, der herefter trænger ind i den nationale ret. En form for »privacy creep«. En sådan konvention vil lægge vægten på principper og retningslinier for persondatabehandling og herefter overlade implementeringen til det nationale niveau og derved muliggøre, at der kan tages hensyn til lokal tradition. Dette vil være i overensstemmelse med en foreliggende tendens til at tage hensyn til skismaet mellem globale rettigheder og lokal kultur.¹² Anlægges dette udgangspunkt, vil der ikke blive institueret globale håndhævelsesorganer. En konvention af denne karakter er på nuværende tidspunkt med de meget forskellige nationale retskulturer en realistisk aspiration, men er udtryk for et mindre ambitiøst mål end det, der betinger den gældende EU-retlige regulering. I denne forbindelse må det endvidere tages i betragtning, at konventionen ikke vil kunne blive helt præcis som følge af selve reguleringsgenstanden, jfr. herved under 9.

8.1. Valg af forum

Et centralt spørgsmål vedrører, på hvilken måde en sådan konvention vil kunne blive etableret. Der må tages stilling til, i hvilket forum drøftelserne skal foregå, idet det herved bemærkes, at det er lagt til grund, at det ikke er realistisk at lade Europarådets konvention 108/81 være grundlaget. Det kan således iagttages, at selvom det er muligt for stater, der ikke er medlemmer af Europarådet, at tilslutte sig konventionen, er dette ikke sket i noget tilfælde. Dette må nok tages som udtryk for, at konventionen selvom den er mere »rundt« formuleret end direktivet, ikke betragtes som attraktiv, ud over at det selvfølgelig for en ikke europæisk stat kan virke noget underligt at tilslutte sig en sådan konvention.

Det er på denne baggrund ønskeligt at anvende et forum, der kan anses for globalt. Det har været nævnt, at WTO kunne være en mulighed, og til støtte herfor kan anføres, at dette er en organisation, som har et godt kendskab til de

12. Jfr. i denne sammenhæng princip 12 i APEC Privacy Framework 2005.

behov, som den internationale handel har.¹³ Ud over at ikke alle betydende lande endnu er medlemmer af WTO, kan det imod at vælge dette forum anføres, at netop denne organisations mission, at fremme den frie handel, kan indebære en fokusering, der hindrer et tilstrækkeligt afbalanceret resultat i forhold til de grundlæggende rettigheder, som databeskyttelsen repræsenterer. Overførselsbehovet kan blive overeksponeret. Selvom konventionen begrænses til alene at angå den private sektor, vil WTO på denne baggrund ikke være et egnet forum.

Det vil derfor være kunne være hensigtsmæssigt at vælge et FN organ som forum. FN er den eneste fuldt ud globale organisation.¹⁴ I den af verdens datatilsyn i Montreux september 2005 vedtagne deklaration er der således medtaget en opfordring til FN om at forberede et bindende juridisk instrument. FN kan være for rettighedsorienteret, hvilket aktualiserer en risiko for ubalance, men organisationens globale natur er en stor styrke. En anden mulighed kunne bestå i at konstruere et helt nyt forum, der eventuelt kunne have sit grundlag i en aftale mellem G8-landene, men det forekommer tvivlsomt, om et sådant forum kan blive tilstrækkeligt globalt.

8.2. Betænkeligheder

Mange, måske de fleste, vil være tøvende over for tanken om at udforme en ny konvention. Al erfaring viser, at dette er tidskrævende proces, der nødvendiggør investering af mange ressourcer. Skulle der blive opnået et tilfredsstillende resultat, går der ligeledes typisk lang tid med implementering. Disse betænkeligheder er reelle, og det er ikke nødvendigvis nogen ideel vej at betræde. Uanset disse naturlige forbehold er det svært at forestille sig et alternativ, idet det må anses for urealistisk at tro, at alle betydende lande blot efterhånden indretter deres lovgivning i overensstemmelse med direktivet. EU er et væsentligt økonomisk område i verden, men har dog ikke nogen dominerende betydning, der kan medføre en sådan retseksport. Erfaringerne med hensyn til forholdet mellem EU og USA taler imod, at direktivet kan få denne virkning. Under alle omstændigheder forekommer det ikke sandsynligt, at en sådan situation vil opstå, i hvert fald ikke i en overskuelig fremtid og nok i en fjernere fremtid end den en ny konvention er underlagt.

13. Jfr. herved Joel Reidenberg, 38 Houston Law Review (2001) p.746-748, der foreslår at der i WTO aftales en General Agreement on Information Privacy (GAIP).

14. FN har tidligere udtalt sig om databeskyttelse, jfr. United Nations guidelines concerning computerized personal data files (adopted by the General Assembly 14.december 1990), men har i øvrigt ikke hidtil været aktiv på dette område.

Kapitel 8 En ny løsning?

En situation, hvor alle betydende lande reelt respekterer de åbne og lidet specifikke krav, der følger af OECD's retningslinier, vil ikke være tilstrækkelig betryggende. Selvom disse retningslinier af artikel 29-gruppen betragtes som en minimumsstandard, vil det være en for stor kamel at sluge, såfremt dataeksport alene på dette grundlag skulle accepteres. Det er sandsynligt, at et nyt internationalt instrument vil modificere direktivet, men dette vil lettere kunne accepteres, når EU selv har været med til at forhandle det pågældende instrument. Den folkeretlige vej må også af denne grund betrædes.

9. Inden for EU

Der er således ikke en sammenhængende løsning lige rundt om hjørnet, og denne konstatering aktualiserer dermed spørgsmålet, om der kan gøres mere på det foreliggende grundlag. Dette kan overvejes både i forhold til overførsler inden for og uden for EU. Forinden dette sker, kan det indskydes, at en yderligere mulighed er at anlægge, hvad man kunne betegne en holistisk indfaldsvinkel, hvor denne opdeling ikke længere benyttes, idet man snarere konkret vurderer den enkelte overførsel. En sådan mulighed bør indgå i de retspolitiske overvejelser.

I kapitel 4 blev det påpeget, at uanset princippet om fri dataoverførsel foreligger der ikke i praksis fuldt ud en sådan frihed mellem medlemsstaterne. Som tidligere nævnt er det svært at gennemføre en reel harmonisering af databeskyttelsesretten, eftersom mange af de fundamentale regler har uskarpe konturer. Denne regulering er på en måde harmoniseringsuegnet, eftersom den er baseret på vage og forholdsvis ubestemmelige grundbegreber. Allerede af denne grund foreligger der ofte noget uigennemskuelige ujævnheder mellem landene, og disse er yderligere forstærkede som følge af de frihedsgrader, som er indbygget i direktivet.

Det har undertiden fra erhvervskredse været fremført, at det ville være bedre at regulere området ved hjælp af en forordning, der kan sikre bedre ensartethed. Det kan dog konstateres, at der ikke hidtil har været tilslutning til en egentlig harmonisering af denne regulering, og det er sandsynligt, at denne modstand stadig foreligger. Samtidig må det tages i betragtning, at databeskyttelse i sig selv som fremhævet ovenfor kun meget vanskeligt lader sig harmonisere. Valg af en anden reguleringsform løser ikke dette problem og kan derfor ikke betragtes som en farbar vej. Specielt kan i denne forbindelse fremhæves, at erfaringerne med direktivet viser, at selvom der er en ensartet lovgivning i medlemsstaterne foreligger der fortolkningsforskelle, der er svært gennemskuelige, og som vanskeliggør dataoverførsler.

10. Tredjelande

Uanset disse vanskeligheder består opgaven for Kommissionen, og eventuelt Domstolen, i at sikre, at direktivet faktisk er implementeret korrekt, og herudover, med bistand af artikel 29-gruppen, at sikre, at der er så få forskelle mellem landene som muligt. Særligt i drøftelserne i gruppen må der lægges vægt på at nå frem til ens fortolkninger af de mange regler, der åbner for flere muligheder. Dette er som fremhævet ikke nogen let opgave, men den bør tiltrække sig større opmærksomhed fremover, idet det er ønskeligt, at denne opgave prioriteres i gruppens årlige arbejdsprogram. Uanset at der er retskulturelle forskelle også inden for EU, må det betragtes som en realistisk mulighed, at der efterhånden kan tilvejebringes en i hvert fald betydeligt større ensartethed i medlemsstaterne, således at fri dataoverførsel, der ikke er omkostningskrævende for eksportører og importører, bliver det sædvanlige. Et indre persondatamarked kan blive en realitet, selvom en fuldt ud harmoniseret databeskyttelsesret er lidt af en utopi.

10. Tredjelande

I forhold til tredjelandene udgør de ordninger, der er beskrevet i kapitel 6, et fremskridt og et godt og nødvendigt supplement til de almindelige regler, men som fremhævet ovenfor er der stadig lang vej at gå. Såvel kontrakt som BVR er svære at anvende, og en simplificering efterlyses ofte. Skal man holde sig på dydens smalle sti, er det særdeles krævende på systematisk måde at gennemføre dataoverførsler, og disse er forbundet med en del omkostninger, som måske ikke alle er strengt nødvendige.

De gennemførte ordninger er i og for sig velgennemtænkte, og selvom flere særlige overførselsgrundlag kan efterlyses, er det vigtigt at undgå, at der bliver etableret et uigennemskueligt juridisk morads, ligesom det bør undgås, at der på dette grundlag opstår et EU-databeskyttelsesretligt bureaukrati, der uvilkårligt vil blive en stopklods i forhold til mere simple ordninger. Som fremhævet ovenfor kan et sådant bureaukrati virke blokerende for udviklingen af hensigtsmæssige folkeretlige instrumenter, der som konsekvens kan have, at disse overførselsgrundlag bliver overflødiggjort.

11. Fantasi

Hovedproblemet er dog de globale ujævnheder, som overordnet må virke som en blokering når det tages i betragtning, at det er grundlæggende rettigheder for borgerne, som er på spil. Det er i almindelighed vigtigt for EU at

Kapitel 8 En ny løsning?

værne sine borgeres grundlæggende rettigheder. Der er kun svage tegn på, at der vil opstå en konvergens mellem landene, og det er ligeledes usikkert, om denne konvergens i givet fald vil medføre et forbedret eller et forringet beskyttelsesniveau. Der er derfor uanset de ovenfor fremhævede betænkigheder behov for flere ordninger og behov for retlig fantasi og kreativitet til at udvikle disse. Alle disse ordninger må have en fornuftig balance og derved tage i betragtning, at dataoverførsler uanset disses store økonomiske betydning grundlæggende må være baseret på respekt for borgernes informationelle privatliv og personlige integritet.

Det er vigtigt for fremtidens udvikling, at dette centrale hensyn fortsat er styrende og bliver taget alvorligt. Det er dog ligeledes vigtigt, at hensynet til databeskyttelse harmoniserer med hensynet til dataoverførsler på en måde, der ikke medfører, at førstnævnte benyttes som et alibi for at begrænse eller udelukke sidstnævnte. For som fremhævet i punkt 19 i det uddybende memorandum til OECD's retningslinier 1980 må det konstateres, at »there is an inherent conflict between the protection and the free transborder flow of personal data. Emphasis may be placed on one or the other, and interests in privacy protection may be difficult to distinguish from other interests relating to trade, culture, national sovereignty, and so forth«.

Litteratur

- Andersen, Mads Bryde: IT-retten (2.udg. København 2005).
- Bennett, Colin, Rebecca Grant (ed): Visions of Privacy (Toronto 1999).
- Bennett, Colin, Charles Raab: The Governance of Privacy (Aldershot 2003).
- Betænkning 1345/1997 om behandling af personoplysninger.
- Blume, Peter: Personregistrering (3.udg. København 1996).
- Blume, Peter: Koncerner i registerretlig belysning, Ugeskrift for Retsvæsen 1993 p.392-98.
- Blume, Peter: Personopplysningsloven (København 2000).
- Blume, Peter: Behandlingsbegrebet i databeskyttelsesretten, Ugeskrift for Retsvæsen 2000 p.425-30.
- Blume, Peter: Eksportaftaler i databeskyttelsesretten, Ugeskrift for Retsvæsen 2001 p.375-80.
- Blume, Peter: Databeskyttelsesret (2.udg. København 2003).
- Blume, Peter: Behandling af persondata (København 2003)
- Blume, Peter: Rejsen til Amerika, Ugeskrift for Retsvæsen 2004 p.407-13.
- Blume, Peter: Eksport af persondata, Ugeskrift for Retsvæsen 2005 p.145-50.
- Carey, Peter: Data Protection (2.ed. Oxford 2004).
- Gomard, Bernhard: Rimelighed og god skik, Juristen 2005 p.191-99.
- Johannsen, Michael Wiik, m.fl.: Personopplysningsloven (Oslo 2001).
- Konjewski, Markus: National Regulation and Trade Liberalization in Services (The Hague 2003).
- Kuner, Christopher: European Data Privacy Law and Online Business (Oxford 2003).
- Nielsen, Kristian Korfits, Henrik Waaben: Lov om handling af personoplysninger (København 2001).
- Nugter, A.C.M.: Transborder flow of personal data within the EC (Deventer 1990).
- Reidenberg, Joel: E-Commerce and Trans-Atlantic Privacy, 38, Houston Law Review p.717-47.
- Swire, Peter P., Robert L. Litan: None of your Business (Washington 1998).
- Wacks, Raymond: Law, Morality and the Private Domain (Hong Kong 2000).
- Öman, Sören, Hans-Olof Lindblom: Personuppgiftslagen (2.udg. Stockholm 2001).

Bilag

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
(uddrag)

Betragtninger:

EUROPA-PARLAMENTET OG RÅDET
FOR DEN EUROPÆISKE UNION HAR -

- under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 100 A,
- under henvisning til forslag fra Kommissionen,
- under henvisning til udtalelse fra Det Økonomiske og Sociale Udvalg,
- i henhold til fremgangsmåden i traktatens artikel 189 B, stk.3, og
- ud fra følgende betragtninger:

- (9) med den ensartede beskyttelse, som vil følge af den indbyrdes tilnærmelse af de nationale lovgivninger, vil medlemsstaterne ikke længere under henvisning til det enkelte menneskes rettigheder og frihedsrettigheder, navnlig retten til privatlivets fred, kunne lægge hindringer i vejen for den frie udveksling af personoplysninger medlemsstaterne imellem; medlemsstaterne vil få en manøvremargin, som erhvervslivet og arbejdsmarkedets parter kan benytte sig af i forbindelse med direktivets gennemførelse; de vil således i

deres nationale lovgivning kunne fastsætte de generelle betingelser for lovlig behandling af personoplysninger; medlemsstaterne skal derved tilsinde en forbedring af den beskyttelse, som deres nuværende lovgivning sikrer; inden for rammerne af denne manøvremargin og i overensstemmelse 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;

- (56) strømmen af personoplysninger på tværs af landegrænserne er nødvendig af hensyn til udbygningen af den internationale samhandel; den beskyttelse, der ved dette direktiv garanteres personer inden for Fællesskabet, er ikke til hinder for, at der videregives personoplysninger til tredjelande, for så vidt disse sikrer et tilstrækkeligt beskyttelsesniveau; vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, skal foretages på grundlag af samtlige de forhold, der har indflydelse på en videregivelse eller en type videregivelse af oplysninger;

Bilag

(57) hvis et tredjeland derimod ikke sikrer et tilstrækkeligt beskyttelsesniveau, skal videregivelse af personoplysninger til det pågældende land forbydes;

(58) der skal dog kunne undtages fra dette forbud under bestemte omstændigheder, hvor den registrerede har meddelt sit samtykke, hvor videregivelsen er nødvendig i forbindelse med en kontrakt eller en retssag, hvor beskyttelsen af væsentlige samfundsinteresser kræver det, f.eks. ved international udveksling af oplysninger mellem skatte- eller toldforvaltninger eller mellem socialsikringsmyndigheder, eller hvor videregivelsen sker fra et register, der er oprettet ved lov, og som offentligheden eller personer med en legitim interesse heri skal kunne konsultere; en sådan videregivelse bør ikke omfatte alle oplysningerne eller hele kategorier af oplysninger i dette register; når et register er beregnet til at blive konsulteret af personer, der har en legitim interesse heri, bør videregivelse kun ske på anmodning af disse personer, eller hvis de selv er modtageren;

(59) der kan træffes særlige foranstaltninger til at afhjælpe et utilstrækkeligt beskyttelsesniveau i et tredjeland, hvis den registeransvarlige stiller de fornødne garantier; endvidere skal der fastsættes bestemmelser om forhandlingsprocedurer mellem Fællesskabet og de pågældende tredjelande;

(60) videregivelse til tredjelande må under alle omstændigheder kun finde sted under fuld overholdelse af de bestemmelser, som medlemsstaterne vedtager i medfør af dette direktiv, særlig artikel 8;

KAPITEL I ALMINDELIGE BESTEMMELSER

Artikel 1

Direktivets formål

1. Medlemsstaterne sikrer i overensstemmelse med dette direktiv beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, i forbindelse med behandling af personoplysninger.

2. Medlemsstaterne må ikke af grunde, der har forbindelse med den i stk. 1 foreskrevne beskyttelse, indskrænke eller forbyde fri udveksling af personoplysninger mellem medlemsstaterne.

Artikel 4

Gældende national ret

1. Medlemsstaterne anvender de nationale bestemmelser, de vedtager til gennemførelse af dette direktiv, på behandling af personoplysninger:

- a) der foretages som led i en virksomheds eller et organs aktiviteter inden for den medlemsstats område, hvor den registeransvarlige er etableret; en registeransvarlig, som er etableret på flere medlemsstats områder, skal træffe de nødvendige foranstaltninger til at sikre, at hver af disse virksomheder eller organer opfylder kravene i den gældende nationale lovgivning
- b) der foretages af en registeransvarlig, der ikke er etableret på den pågældende medlemsstats område, men på et sted, hvor dens nationale lovgivning gælder i henhold til folkeretten
- c) der foretages af en registeransvarlig, der ikke er etableret på Fællesskabets område, og som med henblik på behandling af personoplysninger anvender midler, der er sig elektroniske eller ikke-elektroniske, som befinder sig på den pågældende medlemsstats område, medmindre disse midler kun benyttes med henblik på forsendelse

gennem Det Europæiske Fællesskabs område.

2. I det i stk. 1, litra c), omhandlede tilfælde udpeger den registeransvarlige en repræsentant, der er etableret på den pågældende medlemsstats område, uden at dette i øvrigt berører eventuelle retslige skridt mod den registeransvarlige selv.

KAPITEL IV VIDEREGIVELSE AF PERSONOPLYSNINGER TIL TREDJELANDE

Artikel 25

Principper

1. Medlemsstaterne fastsætter bestemmelser om, at videregivelse til et tredjeland af personoplysninger, der gøres til genstand for behandling, eller som skal gøres til genstand for behandling efter videregivelsen, kun må finde sted, hvis det pågældende tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, og forudsat at de nationale bestemmelser, der vedtages til gennemførelse af direktivets øvrige bestemmelser, overholdes.

2. Vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, sker på grundlag af samtlige de forhold, der har indflydelse på en videregivelse eller en type videregivelse af oplysninger; til grund for vurderingen lægges navnlig oplysningernes art, den eller de påtænkte behandlings formål og varighed, oprindelseslandet og det endelige bestemmelsesland, de retsregler – almindelige regler eller sektorregler – der er i kraft i det pågældende tredjeland, samt de regler for god forretningskik og de sikkerhedsforanstaltninger, der gælder i landet.

3. Medlemsstaterne og Kommissionen underretter gensidigt hinanden, hvis de mener, at et tredjeland ikke sikrer et til-

strækkeligt beskyttelsesniveau i overensstemmelse med stk. 2.

4. Konstaterer Kommissionen efter proceduren i artikel 31, stk. 2, at et tredjeland ikke sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med denne artikels stk. 2, træffer medlemsstaterne de foranstaltninger, der er nødvendige for at hindre enhver videregivelse af oplysninger af samme art til det pågældende tredjeland.

5. Kommissionen indleder på det rette tidspunkt forhandlinger med henblik på at afhjælpe den situation, der opstår som følge af en konstatering efter stk. 4.

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

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

Artikel 26

Undtagelser

1. Som undtagelse fra bestemmelserne i artikel 25, fastsætter medlemsstaterne, medmindre andet er bestemt i deres nationale lovgivning, at videregivelse eller en type videregivelse af personoplysninger til et tredjeland, der ikke sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med artikel 25, stk. 2, kan finde sted, hvis

- a) der ikke hersker tvivl om, at den registrerede har givet sit samtykke, eller
- b) videregivelsen er nødvendig af hensyn til opfyldelsen af en kontrakt mellem den registrerede og den registeran-

Bilag

- svarlige eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en sådan kontrakt, eller
- c) videregivelsen er nødvendig af hensyn til indgåelsen eller udførelsen af en kontrakt, der i den registreredes interesse er indgået mellem den registeransvarlige og tredjemand, eller
 - d) videregivelsen er nødvendig eller følger af lov eller bestemmelser fastsat med hjemmel i lov for at beskytte en vigtig samfundsinteresse eller for, at et retskrav kan fastlægges, gøres gældende eller forsvares, eller
 - e) videregivelsen er nødvendig for at beskytte den registreredes vitale interesser, eller
 - f) videregivelsen finder sted fra et offentligt register, der ifølge love eller administrative bestemmelser er beregnet til at informere offentligheden, og som er tilgængeligt for offentligheden generelt eller for personer, der kan godtgøre at have en legitim interesse heri, i det omfang de ved lov fastsatte betingelser for offentlig tilgængelighed er opfyldt i det specifikke tilfælde.
2. Med forbehold af stk. 1, kan en medlemsstat give tilladelse til videregivelse eller en type videregivelse af personoplysninger til et tredjeland, der ikke sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med artikel 25, stk. 2, hvis den registeransvarlige yder tilstrækkelige garantier for beskyttelse af privatlivets fred, personers grundlæggende rettigheder og frihedsrettigheder samt for udøvelsen af de dertil knyttede rettigheder; sådanne garantier kan især fremgå af passende kontraktbestemmelser.
3. Den pågældende medlemsstat underretter Kommissionen og de øvrige medlemsstater om de tilladelser, den giver i henhold til stk. 2.
- Rejses der indsigelse herimod fra en anden medlemsstat eller Kommissionen, og er denne berettiget ud fra hensynet til beskyttelse af privatlivets fred eller personers grundlæggende rettigheder og frihedsrettigheder, vedtager Kommissionen passende foranstaltninger efter proceduren i artikel 31, stk. 2.
- Medlemsstaterne træffer de foranstaltninger, der er nødvendige for at efterkomme Kommissionens afgørelse.
4. Fastslår Kommissionen efter proceduren i artikel 31, stk. 2, at visse standardkontraktbestemmelser frembyder tilstrækkelige garantier i henhold til stk. 2, træffer medlemsstaterne de foranstaltninger, der er nødvendige for at efterkomme Kommissionens afgørelse.

Lov nr. 429 af 31.05. 2000
om behandling af personoplysninger

Afsnit I
Indledende bestemmelser

Kapitel I
Lovens område

§ 1. Loven gælder for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Stk. 2. Loven gælder tillige for anden ikke- elektronisk systematisk behandling, som udføres for private, og som omfatter oplysninger om personers private eller økonomiske forhold eller i øvrigt oplysninger om personlige forhold, som med rimelighed kan forlanges unddraget offentligheden. Dette gælder dog ikke reglerne i lovens kapitel 8 og 9.

Stk. 3. Loven gælder endvidere for behandling af oplysninger om virksomheder m.v., jf. stk. 1 og 2, hvis denne behandling udføres for kreditoplysningsbureauer. Tilsvarende gælder for så vidt angår behandlinger, som er omfattet af ' 50, stk. 1, nr. 2.

Stk. 4. Kapitel 5 gælder også for behandling af oplysninger om virksomheder m.v., jf. stk. 1.

Stk. 5. Uden for de i stk. 3 nævnte tilfælde kan justitsministeren bestemme, at lovens regler helt eller delvis skal finde anvendelse på behandling af oplysninger om virksomheder m.v., som udføres for private.

Stk. 6. Uden for de i stk. 4 nævnte tilfælde kan vedkommende minister bestemme, at lovens regler helt eller delvis skal

finde anvendelse på behandling af oplysninger om virksomheder m.v., som udføres for den offentlige forvaltning.

§ 2. Regler om behandling af personoplysninger i anden lovgivning, som giver den registrerede en bedre retsstilling, går forud for reglerne i denne lov.

Stk. 2. Loven finder ikke anvendelse, hvis det vil være i strid med informations- og ytringsfriheden, jf. Den Europæiske Menneskerettighedskonventions artikel 10.

Stk. 3. Loven gælder ikke for behandlinger, som en fysisk person foretager med henblik på udøvelse af aktiviteter af rent privat karakter.

Stk. 4. Bestemmelserne i lovens kapitel 8 og 9 og §§ 35-37 og § 39 finder ikke anvendelse på behandlinger, der foretages for domstolene inden for det strafferetlige område. Bestemmelserne i lovens kapitel 8 og §§ 35-37 og § 39 finder heller ikke anvendelse på behandlinger, der foretages for politi og anklagemyndighed inden for det strafferetlige område.

Stk. 5. Loven finder ikke anvendelse på behandling af oplysninger, der foretages for Folketinget og institutioner med tilknytning dertil.

Stk. 6. Loven finder ikke anvendelse på behandlinger, der er omfattet af lov om massemediers informationsdatabaser.

Stk. 7. Loven finder ikke anvendelse på informationsdatabaser, hvori der udelukkende er indlagt allerede offentliggjorte periodiske skrifter eller lyd- og billedprogrammer, der er omfattet af medieansvarslovens § 1, nr. 1 eller 2, eller dele heraf, når indlæggelsen i informationsdatabasen er

Bilag

sket uændret i forhold til offentliggørelsen. Dog gælder bestemmelserne i lovens §§ 41, 42 og 69.

Stk. 8. Loven gælder endvidere ikke for informationsdatabaser, hvori der udelukkende er indlagt allerede offentliggjorte tekster, billeder og lydprogrammer, der omfattes af medieansvarslovens § 1, nr. 3, eller dele heraf, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelsen. Dog gælder bestemmelserne i lovens §§ 41, 42 og 69.

Stk. 9. Loven finder ikke anvendelse på manuelle arkiver over udklip fra offentliggjorte, trykte artikler, som udelukkende behandles i journalistisk øjemed. Dog gælder bestemmelserne i lovens §§ 41, 42 og 69.

Stk. 10. For behandling af oplysninger, som i øvrigt udelukkende finder sted i journalistisk øjemed, gælder alene bestemmelserne i lovens §§ 41, 42 og 69. Det samme gælder for behandling af oplysninger, som udelukkende sker med henblik på kunstnerisk eller litterær virksomhed.

Stk. 11. Loven gælder ikke for behandlinger, der udføres for politiets og forsvarrets efterretningstjenester.

Kapitel 2 Definitioner

§ 3. I denne lov forstås ved:

- 1) Personoplysninger:
Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede).
- 2) Behandling:
Enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for.
- 3) Register med personoplysninger (register):
Enhver struktureret samling af personoplysninger, der er tilgængelige efter bestemte kriterier, hvad enten denne samling er placeret centralt, decentralt

eller er fordelt på et funktionsbestemt eller geografisk grundlag.

- 4) Den dataansvarlige:

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

- 5) Databehandleren:

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

- 6) Tredjemand:

Enhver anden fysisk eller juridisk person, offentlig myndighed, institution eller ethvert andet organ end den registrerede, den dataansvarlige, databehandleren og de personer under den dataansvarliges eller databehandlerens direkte myndighed, der er beføjet til at behandle oplysninger.

- 7) Modtager:

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

- 8) Den registreredes samtykke:

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

- 9) Tredjeland:

En stat, som ikke indgår i Det Europæiske Fællesskab, og som ikke har gennemført aftaler, der er indgået med Det Europæiske Fællesskab, og som indeholder regler svarende til direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbin-

delse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

Kapitel 3 *Lovens geografiske område*

§ 4. Loven gælder for behandling af oplysninger, som udføres for en dataansvarlig, der er etableret i Danmark, hvis aktiviteterne finder sted inden for Det Europæiske Fællesskabs område.

Stk. 2. Loven gælder endvidere for den behandling, som udføres for danske diplomatiske repræsentationer.

Stk. 3. Loven gælder også for en dataansvarlig, som er etableret i et tredjeland, hvis

- 1) behandlingen af oplysninger sker under benyttelse af hjælpemidler, der befinder sig i Danmark, medmindre hjælpemidlerne kun benyttes med henblik på forsendelse af oplysninger gennem Det Europæiske Fællesskabs område eller
- 2) indsamling af oplysninger i Danmark sker med henblik på behandling i et tredjeland.

Stk. 4. Dataansvarlige, som i henhold til stk. 3, nr. 1, er omfattet af denne lov, skal udpege en repræsentant, som er etableret i Danmark. Den registreredes mulighed for at foretage retslige skridt mod vedkommende dataansvarlige berøres ikke heraf.

Stk. 5. Den dataansvarlige skal skriftligt underrette Datatilsynet om, hvem der er udpeget som repræsentant, jf. stk. 4.

Stk. 6. Loven gælder, hvis der for en dataansvarlig, der er etableret i et andet medlemsland, behandles oplysninger i Danmark og behandlingen ikke er omfattet af 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. Loven gælder også, hvis der for en dataansvarlig, der er etableret i en stat,

som har gennemført en aftale med Det Europæiske Fællesskab, der indeholder regler svarende til det i 1. pkt. nævnte direktiv, behandles oplysninger i Danmark og behandlingen ikke er omfattet af de nævnte regler.

Afsnit II Behandlingsregler

Kapitel 4 *Behandling af oplysninger*

§ 5. Oplysninger skal behandles i overensstemmelse med god databehandlingskik.

Stk. 2. Indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål. Senere behandling af oplysninger, der alene sker i historisk, statistisk eller videnskabeligt øjemed, anses ikke for uforenelig med de formål, hvortil oplysningerne er indsamlet.

Stk. 3. Oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

Stk. 4. Behandling af oplysninger skal tilrettelægges således, at der foretages fornøden ajourføring af oplysningerne. Der skal endvidere foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger. Oplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges.

Stk. 5. Indsamlede oplysninger må ikke opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

§ 6. Behandling af oplysninger må kun finde sted, hvis

Bilag

- 1) den registrerede har givet sit udtrykkelige samtykke hertil,
- 2) behandlingen er nødvendig af hensyn til opfyldelsen af en aftale, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelsen af en sådan aftale,
- 3) behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige,
- 4) behandlingen er nødvendig for at beskytte den registreredes vitale interesser,
- 5) behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse,
- 6) behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som den dataansvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt, eller
- 7) behandlingen er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse og hensynet til den registrerede ikke overstiger denne interesse.

Stk. 2. En virksomhed må ikke videregive oplysninger om en forbruger til en anden virksomhed til brug ved markedsføring eller anvende oplysningerne på vegne af en anden virksomhed i dette øjemed, medmindre forbrugeren har givet sit udtrykkelige samtykke hertil. Et samtykke skal indhentes i overensstemmelse med reglerne i markedsføringslovens § 6 a.

Stk. 3. Videregivelse og anvendelse som nævnt i stk. 2 kan dog ske uden samtykke, hvis der er tale om generelle kundeoplysninger, der danner grundlag for inddeling i kundekategorier, og hvis betingelserne i stk. 1, nr. 7, er opfyldt.

Stk. 4. Der kan efter stk. 3 ikke videregives eller anvendes oplysninger som nævnt i §§ 7 og 8. Justitsministeren kan fastsætte yderligere begrænsninger i adgan-

gen til at videregive eller anvende bestemte typer af oplysninger efter stk. 3.

§ 7. Der må ikke behandles oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold.

Stk. 2. Bestemmelsen i stk. 1 finder ikke anvendelse, hvis

- 1) den registrerede har givet sit udtrykkelige samtykke til en sådan behandling,
- 2) behandlingen er nødvendig for at beskytte den registreredes eller en anden persons vitale interesser i tilfælde, hvor den pågældende ikke fysisk eller juridisk er i stand til at give sit samtykke,
- 3) behandlingen vedrører oplysninger, som er blevet offentliggjort af den registrerede, eller
- 4) behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares.

Stk. 3. Behandling af oplysninger om fagforeningsmæssige tilhørsforhold kan endvidere ske, hvis behandlingen er nødvendig for overholdelsen af den dataansvarliges arbejdsretlige forpligtelser eller specifikke rettigheder.

Stk. 4. En stiftelse, en forening eller en anden almennyttig organisation, hvis sigte er af politisk, filosofisk, religiøs eller faglig art, kan inden for rammerne af sin virksomhed foretage behandling af de i stk. 1 nævnte oplysninger om organisationens medlemmer eller personer, der på grund af organisationens formål er i regelmæssig kontakt med denne. Videregivelse af sådanne oplysninger kan dog kun finde sted, hvis den registrerede har meddelt sit udtrykkelige samtykke hertil eller behandlingen er omfattet af stk. 2, nr. 2-4, eller stk. 3.

Stk. 5. Bestemmelsen i stk. 1 finder ikke anvendelse, hvis behandlingen af oplysninger er nødvendig med henblik på fore-

byggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling, eller forvaltning af læge- og sundhedstjenester, og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt.

Stk. 6. Behandling af de i stk. 1 anførte oplysninger kan ske, hvis behandlingen er nødvendig af hensyn til en offentlig myndigheds varetagelse af sine opgaver på det strafferetlige område.

Stk. 7. Undtagelse fra bestemmelsen i stk. 1 kan endvidere gøres, hvis behandlingen af oplysninger sker af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser. Tilsynsmyndigheden giver tilladelse hertil. Der kan fastsættes nærmere vilkår for behandlingen. Hvor tilladelse meddeles, giver tilsynsmyndigheden underretning herom til Europa-Kommissionen.

Stk. 8. For den offentlige forvaltning må der ikke føres edb-registre med oplysninger om politiske forhold, som ikke er offentligt tilgængelige.

§ 8. For den offentlige forvaltning må der ikke behandles oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 7, stk. 1, nævnte, medmindre det er nødvendigt for varetagelsen af myndighedens opgaver.

Stk. 2. De i stk. 1 nævnte oplysninger må ikke videregives. Videregivelse kan dog ske, hvis

- 1) den registrerede har givet sit udtrykkelige samtykke til videregivelsen,
- 2) videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrundes hemmeligholdelse, herunder hensynet til den, oplysningen angår,
- 3) videregivelsen er nødvendig for udførelsen af en myndigheds virksomhed eller påkrævet for en afgørelse, som myndigheden skal træffe, eller

- 4) videregivelsen er nødvendig for udførelsen af en persons eller virksomheds opgaver for det offentlige.

Stk. 3. Forvaltningsmyndigheder, der udfører opgaver inden for det sociale område, må kun videregive de i stk. 1 nævnte oplysninger og de oplysninger, der er nævnt i § 7, stk. 1, hvis betingelserne i stk. 2, nr. 1 eller 2, er opfyldt, eller hvis videregivelsen er et nødvendigt led i sagens behandling eller nødvendig for, at en myndighed kan gennemføre tilsyns- eller kontrolopgaver.

Stk. 4. Private må behandle oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 7, stk. 1, nævnte, hvis den registrerede har givet sit udtrykkelige samtykke hertil. Herudover kan behandling ske, hvis det er nødvendigt til varetagelse af en berettiget interesse og denne interesse klart overstiger hensynet til den registrerede.

Stk. 5. De i stk. 4 nævnte oplysninger må ikke videregives uden den registreredes udtrykkelige samtykke. Videregivelse kan dog ske uden samtykke, når det sker til varetagelse af offentlige eller private interesser, herunder hensynet til den pågældende selv, der klart overstiger hensynet til de interesser, der begrundes hemmeligholdelse.

Stk. 6. Behandling af oplysninger i de tilfælde, der er reguleret i stk. 1, 2, 4 og 5, kan i øvrigt finde sted, hvis betingelserne i § 7 er opfyldt.

Stk. 7. Et fuldstændigt register over straffedomme må kun føres for en offentlig myndighed.

§ 9. Oplysninger som nævnt i § 7, stk. 1, eller § 8 må behandles, hvis dette alene sker med henblik på at føre retsinformationssystemer af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig for førelsen af systemerne.

Stk. 2. De af stk. 1 omfattede oplysninger må ikke senere behandles i andet øjemed. Det samme gælder behandling af an-

Bilag

dre oplysninger, som alene foretages med henblik på at føre retsinformationssystemer, jf. § 6.

Stk. 3. Tilsynsmyndigheden kan meddele nærmere vilkår for de i stk. 1 nævnte behandlinger. Tilsvarende gælder for de i § 6 nævnte oplysninger, som alene behandles i forbindelse med førelsen af retsinformationssystemer.

§ 10. Oplysninger som nævnt i § 7, stk. 1, eller § 8 må behandles, hvis dette alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig for udførelsen af undersøgelserne.

Stk. 2. De af stk. 1 omfattede oplysninger må ikke senere behandles i andet end statistisk eller videnskabeligt øjemed. Det samme gælder behandling af andre oplysninger, som alene foretages i statistisk eller videnskabeligt øjemed, jf. § 6.

Stk. 3. De af stk. 1 og 2 omfattede oplysninger må kun videregives til tredje-mand efter forudgående tilladelse fra tilsynsmyndigheden. Tilsynsmyndigheden kan stille nærmere vilkår for videregivelsen.

§ 11. Offentlige myndigheder kan behandle oplysninger om personnummer med henblik på en entydig identifikation eller som journalnummer.

Stk. 2. Private må behandle oplysninger om personnummer, når

- 1) det følger af lov eller bestemmelser fastsat i henhold til lov,
- 2) den registrerede har givet sit udtrykkelige samtykke hertil eller
- 3) behandlingen alene finder sted til videnskabelige eller statistiske formål, eller hvis der er tale om videregivelse af oplysninger om personnummer, når videregivelsen er et naturligt led i den normale drift af virksomheder m.v. af den pågældende art, og når videregivelsen er af afgørende betydning for

at sikre en entydig identifikation af den registrerede eller videregivelsen kræves af en offentlig myndighed.

Stk. 3. Uanset bestemmelsen i stk. 2, nr. 3, må der ikke ske offentliggørelse af personnummer uden udtrykkeligt samtykke.

§ 12. Dataansvarlige, der med henblik på markedsføring sælger fortegnelser over grupper af personer, eller som for tredje-mand foretager adressering eller udsendelse af meddelelser til sådanne grupper, må kun behandle

- 1) oplysninger om navn, adresse, stilling, erhverv, e-postadresse, telefon- og telefaxnummer,
- 2) oplysninger, der indgår i erhvervsregistre, som i henhold til lov eller bestemmelser fastsat i henhold til lov er beregnet til at informere offentligheden, samt
- 3) andre oplysninger, hvis den registrerede har givet udtrykkeligt samtykke dertil. Et samtykke skal indhentes i overensstemmelse med markedsføringslovens § 6 a.

Stk. 2. Oplysninger som nævnt i § 7, stk. 1, eller § 8, må dog ikke behandles. Justitsministeren kan fastsætte yderligere begrænsninger i adgangen til at behandle bestemte typer af oplysninger.

§ 13. Offentlige myndigheder og private virksomheder m.v. må ikke foretage automatisk registrering af, hvilke telefonnumre der er foretaget opkald til fra deres telefoner. Registrering må dog ske efter forudgående tilladelse fra tilsynsmyndigheden i tilfælde, hvor afgørende hensyn til private eller offentlige interesser taler herfor. Tilsynsmyndigheden kan fastsætte nærmere vilkår for registreringen.

Stk. 2. Bestemmelsen i stk. 1 gælder ikke, hvis andet følger af lov, eller for så vidt angår udbydere af telenet og teletjenesters registrering af, til hvilke telefonnumre

der er foretaget opkald, enten til eget brug eller til brug ved teknisk kontrol.

§ 14. Oplysninger, der er omfattet af denne lov, kan overføres til opbevaring i arkiv efter reglerne i arkivlovgivningen.

Kapitel 5

Videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige

§ 15. Oplysninger om gæld til det offentlige kan efter bestemmelserne i dette kapitel videregives til kreditoplysningsbureauer.

Stk. 2. Oplysninger som nævnt i § 7, stk. 1, eller § 8, stk. 1, må ikke videregives.

Stk. 3. Fortrolige oplysninger videregivet efter reglerne i dette kapitel anses ikke af den grund for offentligt tilgængelige i øvrigt.

§ 16. Oplysninger om gæld til det offentlige kan videregives til et kreditoplysningsbureau, hvis

- 1) det følger af lov eller bestemmelser fastsat i henhold til lov eller
- 2) den samlede gæld er forfalden og overstiger 7.500 kr., idet der dog ikke heri må indgå gældsposter, der er omfattet af en overholdt aftale om henstand eller afdragsvis betaling.

Stk. 2. Det er en betingelse, at den samlede gæld, jf. stk. 1, nr. 2, administreres af samme inddrivelsesmyndighed.

Stk. 3. Det er endvidere en betingelse for videregivelse efter stk. 1, nr. 2, at

- 1) gælden kan inddrives ved udpantning og der er fremsendt 2 rykkere til skyldneren,
- 2) der er foretaget eller forsøgt foretaget udlæg for kravet,
- 3) kravet er fastslået ved endelig dom eller
- 4) det offentlige har erhvervet skyldnerens skriftlige erkendelse af den forfaldne gæld.

§ 17. Myndigheden skal give skyldneren skriftlig meddelelse herom, forinden videregivelse finder sted. Videregivelse må tidligst ske 4 uger efter, at denne meddelelse er givet.

Stk. 2. Den i stk. 1 nævnte meddelelse skal indeholde oplysninger om,

- 1) hvilke oplysninger der vil blive videregivet,
- 2) til hvilket kreditoplysningsbureau videregivelsen vil ske,
- 3) hvornår videregivelse vil finde sted, og
- 4) at videregivelse ikke vil ske, hvis betaling af gælden sker inden videregivelsen eller der indrømmes henstand eller indgås overholdes en aftale om afdragsvis betaling.

§ 18. Vedkommende minister kan fastsætte nærmere regler om fremgangsmåden ved videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige. Det kan i den forbindelse bestemmes, at oplysninger om visse former for gæld til det offentlige ikke må videregives eller kun må videregives, hvis yderligere betingelser end de i § 16 nævnte er opfyldt.

Kapitel 6

Kreditoplysningsbureauer

§ 19. Den, som ønsker at drive virksomhed med behandling af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed med henblik på videregivelse (kreditoplysningsbureau), skal indhente tilladelse hertil fra Datatilsynet, inden behandlingen påbegyndes, jf. § 50, stk. 1, nr. 3.

§ 20. Kreditoplysningsbureauer må kun behandle oplysninger, som efter deres art er af betydning for bedømmelse af økonomisk soliditet og kreditværdighed.

Stk. 2. Oplysninger som nævnt i § 7, stk. 1, og § 8, stk. 4, må ikke behandles.

Stk. 3. Oplysninger om forhold, der taler imod kreditværdighed, og som er mere

Bilag

end 5 år gamle, må ikke behandles, medmindre det i det enkelte tilfælde er åbenbart, at forholdet er af afgørende betydning for bedømmelsen af den pågældendes økonomiske soliditet og kreditværdighed.

§ 21. Kreditoplysningsbureauer skal i overensstemmelse med § 28, stk. 1, eller § 29, stk. 1, meddele de oplysninger, der er nævnt i disse bestemmelser, til den, der behandles oplysninger om.

§ 22. Kreditoplysningsbureauer skal til enhver tid på begæring af den registrerede inden 4 uger på en let forståelig måde meddele denne indholdet af de oplysninger og bedømmelser, som bureauet har videregivet om den pågældende inden for de sidste 6 måneder, samt af de øvrige oplysninger, som bureauet på tidspunktet for begæringens fremsættelse opbevarer om den pågældende i bearbejdet form eller på digitalt medium, herunder foreliggende bedømmelser.

Stk. 2. Er bureauet i besiddelse af yderligere materiale om den registrerede, skal dette samtidig meddeles den pågældende med oplysning om materialets art samt om, at den registrerede kan få adgang til at gennemgå det ved personlig henvendelse til bureauet.

Stk. 3. Bureauet skal endvidere give oplysning om kategorien af modtagere af oplysningerne samt tilgængelig information om, hvorfra de i stk. 1 og 2 nævnte oplysninger stammer.

Stk. 4. Den registrerede kan forlange, at bureauet giver meddelelse som nævnt i stk. 1-3 skriftligt. Justitsministeren fastsætter regler om betaling for skriftlige meddelelser.

§ 23. Oplysninger om økonomisk soliditet og kreditværdighed må kun meddeles skriftligt, jf. dog § 22, stk. 1-3. Bureauet kan dog til abonnenter meddele summariske oplysninger mundtligt eller på lignende måde, såfremt spørgerens navn og

adresse noteres og opbevares i mindst 6 måneder.

Stk. 2. Kreditoplysningsbureauers publikationer må kun indeholde oplysninger i summarisk form og kun udsendes til personer eller virksomheder, der abonnerer på meddelelser fra bureauet. Publikationerne må ikke indeholde oplysninger om de registreredes personnummer.

Stk. 3. Summariske oplysninger om skyldforhold må kun videregives, hvis oplysningerne hidrører fra Statstidende, er indberettet af en offentlig myndighed efter reglerne i kapitel 5, eller hvis oplysningerne vedrører skyldforhold til samme kreditor på mere end 1.000 kr. og kreditor enten har erhvervet den registreredes skriftlige erkendelse af en forfalden gæld, eller hvis der er foretaget retslige skridt mod den pågældende. Oplysninger om endeligt godkendt gældssanering må dog ikke videregives. De i 1. og 2. pkt. nævnte regler gælder tillige for videregivelse af summariske oplysninger om skyldforhold i forbindelse med udarbejdelse af bredere kreditbedømmelser.

Stk. 4. Videregivelse af summariske oplysninger om enkeltpersoners skyldforhold må kun ske på en sådan måde, at oplysningerne ikke kan danne grundlag for vurderingen af økonomisk soliditet og kreditværdighed for andre end de pågældende enkeltpersoner.

§ 24. Oplysninger eller bedømmelser, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges.

§ 25. Er en oplysning eller bedømmelse, der viser sig urigtig eller vildledende, forinden blevet videregivet, skal bureauet straks give skriftlig underretning om berigtigelsen til den registrerede og til alle, der har modtaget oplysningen eller bedømmelsen inden for de sidste 6 måneder, før bureauet er blevet bekendt med forholdet. Den registrerede skal tillige have meddelelse om, hvem der har modtaget under-

retning efter 1. pkt., og hvorfra oplysningen eller bedømmelsen stammer.

§ 26. Henvendelser fra en registreret om sletning, berigtigelse eller blokering af oplysninger eller bedømmelser, der angives at være urigtige eller vildledende, eller om sletning af oplysninger, der ikke må behandles, jf. § 37, stk. 1, skal snarest og inden 4 uger efter modtagelsen besvares skriftligt af bureauet.

Stk. 2. Nægter bureauet at foretage den begærede sletning, berigtigelse eller blokering, kan den registrerede inden 4 uger efter modtagelsen af bureauets svar eller efter udløbet af den i stk. 1 nævnte svarfrist indbringe spørgsmålet for Datatilsynet, der træffer afgørelse om, hvorvidt der skal foretages sletning, berigtigelse eller blokering. Bestemmelsen i § 25 gælder tilsvarende.

Stk. 3. Bureauets svar skal i de i stk. 2 nævnte tilfælde indeholde oplysning om adgangen til at indbringe spørgsmålet for Datatilsynet og om fristen herfor.

Kapitel 7

Overførsel af oplysninger til tredjelande

§ 27. Der må kun overføres oplysninger til et tredjeland, såfremt dette land sikrer et tilstrækkeligt beskyttelsesniveau, jf. dog stk. 3.

Stk. 2. Vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, sker på grundlag af samtlige de forhold, der har indflydelse på en overførsel, herunder navnlig oplysningernes art, behandlingens formål og varighed, oprindelseslandet og det endelige bestemmelsesland, samt de retsregler, regler for god forretningsskik og sikkerhedsforanstaltninger, som gælder i tredjelandet.

Stk. 3. Ud over de i stk. 1 nævnte tilfælde kan der overføres oplysninger til et tredjeland, såfremt

- 1) den registrerede har givet udtrykkeligt samtykke,

- 2) overførsel er nødvendig af hensyn til opfyldelsen af en aftale mellem den registrerede og den dataansvarlige eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en sådan aftale,
- 3) overførsel er nødvendig af hensyn til indgåelsen eller udførelsen af en aftale, der i den registreredes interesse er indgået mellem den dataansvarlige og tredjemand,
- 4) overførsel er nødvendig eller følger af lov eller bestemmelser fastsat i henhold til lov for at beskytte en vigtig samfundsmæssig interesse eller for, at et retskrav kan fastlægges, gøres gældende eller forsvares,
- 5) overførsel er nødvendig for at beskytte den registreredes vitale interesser,
- 6) overførsel finder sted fra et register, der ifølge lov eller bestemmelser fastsat i henhold til lov er tilgængeligt for offentligheden eller for personer, der kan godtgøre at have en berettiget interesse heri, i det omfang de i lovgivningen fastsatte betingelser for offentlig tilgængelighed er opfyldt i det specifikke tilfælde,
- 7) overførsel er nødvendig af hensyn til forebyggelse, efterforskning og forfølgning af strafbare forhold samt straf fuldbyrdelse og beskyttelse af sigtede, vidner eller andre i sager om strafferetlig forfølgning eller
- 8) overførsel er nødvendig af hensyn til den offentlige sikkerhed, rigets forsvar eller statens sikkerhed.

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

Bilag

delser meddelt i henhold til denne bestemmelse.

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

Afsnit III Registreredes rettigheder

Kapitel 8

Oplysningspligt over for den registrerede

§ 28. Ved indsamling af oplysninger hos den registrerede skal den dataansvarlige eller dennes repræsentant give den registrerede meddelelse om følgende:

- 1) Den dataansvarliges og dennes repræsentants identitet.
- 2) Formålene med den behandling, hvortil oplysningerne er bestemt.
- 3) Alle yderligere oplysninger, der under hensyn til de særlige omstændigheder, hvorunder oplysningerne er indsamlet, er nødvendige for, at den registrerede kan varetage sine interesser, som f.eks.:
 - a) Kategorierne af modtagere.
 - b) Om det er obligatorisk eller frivilligt at besvare stillede spørgsmål samt mulige følger af ikke at svare.
 - c) Om reglerne om indsigt i og om berigtigelse af de oplysninger, der vedrører den registrerede.

Stk. 2. Bestemmelsen i stk. 1 gælder ikke, hvis den registrerede allerede er bekendt med de i nr. 1-3 nævnte oplysninger.

§ 29. Hvor oplysninger ikke er indsamlet hos den registrerede, påhviler det den dataansvarlige eller dennes repræsentant ved registreringen, eller hvor de indsamlede oplysninger er bestemt til videregivelse til tredjemand, senest når videregivelsen af oplysningerne finder sted, at give den registrerede meddelelse om følgende:

- 1) Den dataansvarliges og dennes repræsentants identitet.

- 2) Formålene med den behandling, hvortil oplysningerne er bestemt.

- 3) Alle yderligere oplysninger, der under hensyn til de særlige omstændigheder, hvorunder oplysningerne er indsamlet, er nødvendige for, at den registrerede kan varetage sine interesser, som f.eks.:

- a) Hvilken type oplysninger det drejer sig om.
- b) Kategorierne af modtagere.
- c) Om reglerne om indsigt i og om berigtigelse af de oplysninger, der vedrører den registrerede.

Stk. 2. Bestemmelsen i stk. 1 gælder ikke, hvis den registrerede allerede er bekendt med de i nr. 1-3 nævnte oplysninger, eller hvis registreringen eller videregivelsen udtrykkeligt er fastsat ved lov eller bestemmelser fastsat i henhold til lov.

Stk. 3. Bestemmelsen i stk. 1 gælder heller ikke, hvis underretning af den registrerede viser sig umulig eller er uforholdsmæssigt vanskelig.

§ 30. Bestemmelserne i § 28, stk. 1, og § 29, stk. 1, gælder ikke, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv.

Stk. 2. Undtagelse fra bestemmelserne i § 28, stk. 1, og § 29, stk. 1, kan tillige gøres, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til offentlige interesser, herunder navnlig til

- 1) statens sikkerhed,
- 2) forsaret,
- 3) den offentlige sikkerhed,
- 4) forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv,
- 5) væsentlige økonomiske eller finansielle interesser hos en medlemsstat eller Den Europæiske Union, herunder valuta-, budget- og skatteanliggender, og

- 6) kontrol-, tilsyns- eller reguleringsopgaver, herunder opgaver af midlertidig karakter, der er et led i den offentlige myndighedsudøvelse på de i nr. 3-5 nævnte områder.

Kapitel 9

Den registreredes indsigtsret

§ 31. Fremsætter en person begæring herom, skal den dataansvarlige give den pågældende meddelelse om, hvorvidt der behandles oplysninger om vedkommende. Behandles sådanne oplysninger, skal der på en let forståelig måde gives den registrerede meddelelse om,

- 1) hvilke oplysninger der behandles,
- 2) behandlingens formål,
- 3) kategorierne af modtagere af oplysningerne og
- 4) tilgængelig information om, hvorfra disse oplysninger stammer.

Stk. 2. Den dataansvarlige skal snarest besvare begæringer som nævnt i stk. 1. Er begæringen ikke besvaret inden 4 uger efter modtagelsen, skal den dataansvarlige underrette den pågældende om grunden hertil, samt om, hvornår afgørelsen kan forventes at foreligge.

§ 32. Bestemmelserne i § 30 finder tilsvarende anvendelse.

Stk. 2. Oplysninger, der behandles for den offentlige forvaltning som led i administrativ sagsbehandling, kan undtages fra indsigtsretten i samme omfang som efter reglerne i offentlighedslovens § 2 samt §§ 7-11 og 14.

Stk. 3. Der er ikke ret til indsigt i oplysninger, der behandles for domstolene, hvis oplysningerne indgår i tekst, som ikke foreligger i endelig form. Dette gælder dog ikke, hvis oplysningerne er videregivet til en tredjemand. Der er ikke ret til indsigt i voteringsprotokoller og andre referater af domstolenes rådslagning samt materiale udarbejdet af domstolene til brug for rådslagningen.

Stk. 4. Bestemmelsen i § 31, stk. 1, finder ikke anvendelse, hvis oplysningerne udelukkende behandles i videnskabeligt øjemed, eller hvor oplysningerne kun opbevares i form af personoplysninger i det tidsrum, som kræves for at udarbejde statistikker.

Stk. 5. For behandling af oplysninger på det strafferetlige område, der foretages for den offentlige forvaltning, kan justitsministeren fastsætte undtagelser fra retten til at få oplysninger efter § 31, stk. 1, for så vidt bestemmelsen i § 32, stk. 1, jf. herved § 30, må antages at medføre, at begæringer om ret til indsigt i almindelighed må afslås.

§ 33. En registreret person, der har fået meddelelse efter § 31, stk. 1, har ikke krav på ny meddelelse før 6 måneder efter sidste meddelelse, medmindre der godtgøres en særlig interesse heri.

§ 34. Meddelelser i henhold til § 31, stk. 1, skal på begæring gives skriftligt. I tilfælde, hvor hensynet til den registrerede taler derfor, kan meddelelse dog gives i form af en mundtlig underretning om indholdet af oplysningerne.

Stk. 2. Justitsministeren kan fastsætte regler om betaling for meddelelser, som gives skriftligt af private virksomheder m.v.

Kapitel 10

Øvrige rettigheder

§ 35. Den registrerede kan til enhver tid over for den dataansvarlige gøre indsigelse mod, at oplysninger om vedkommende gøres til genstand for behandling.

Stk. 2. Hvis indsigelsen efter stk. 1 er berettiget, må behandlingen ikke længere omfatte de pågældende oplysninger.

§ 36. Fremsætter en forbruger indsigelse herimod, må en virksomhed ikke videregive oplysninger om den pågældende til en anden virksomhed med henblik på markedsføring eller anvende oplysningerne på

Bilag

vegne af en anden virksomhed i dette øjemed.

Stk. 2. Inden virksomheden videregiver oplysninger om en forbruger til en anden virksomhed med henblik på markedsføring eller anvender oplysningerne på vegne af en anden virksomhed i dette øjemed, skal den undersøge i CPR, om forbrugeren har frabedt sig henvendelser i markedsføringsøjemed. Inden oplysninger om en forbruger, der ikke i CPR har frabedt sig sådanne henvendelser, videregives eller anvendes som nævnt i 1. pkt., skal virksomheden tydeligt og på en forståelig måde oplyse om retten til at gøre indsigelse efter stk. 1. Forbrugeren skal samtidig gives adgang til på en nem måde inden for to uger at gøre sådan indsigelse. Oplysningerne må ikke videregives, inden fristen til at gøre indsigelse er udløbet.

Stk. 3. Henvendelse til forbrugeren efter stk. 2 skal i øvrigt ske i overensstemmelse med reglerne i markedsføringslovens § 6 a og regler udstedt i medfør af markedsføringslovens § 6 a, stk. 6.

Stk. 4. Virksomheden kan ikke kræve betaling for behandlingen af en indsigelse.

§ 37. Den dataansvarlige skal berigtige, slette eller blokere oplysninger, der viser sig urigtige eller vildledende eller på lignende måde er behandlet i strid med lov eller bestemmelser udstedt i medfør af lov, hvis en registreret person fremsætter anmodning herom.

Stk. 2. Den dataansvarlige skal underrette den tredjemand, hvortil oplysningerne er videregivet, om, at de videregivne oplysninger er berigtiget, slettet eller blokeret i henhold til stk. 1, hvis en registreret person fremsætter anmodning herom. Dette gælder dog ikke, hvis underretningen viser sig umulig eller er uforholdsmæssigt vanskelig.

§ 38. Den registrerede kan tilbagekalde et samtykke.

§ 39. Fremsætter en registreret person indsigelse herimod, kan den dataansvarlige ikke foranstalte, at den registrerede undergives afgørelser, der har retsvirkninger for eller i øvrigt berører den pågældende i væsentlig grad, og som alene er truffet på grundlag af elektronisk databehandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold.

Stk. 2. Bestemmelsen i stk. 1 gælder ikke, hvis

- 1) den pågældende afgørelse træffes som led i indgåelsen eller opfyldelsen af en aftale, såfremt den registreredes anmodning om indgåelse eller opfyldelse af aftalen er blevet efterkommet eller der findes passende foranstaltninger til at beskytte den registreredes berettigede interesser eller
- 2) den pågældende afgørelse er hjemlet i en lov, der indeholder bestemmelser til beskyttelse af den registreredes berettigede interesser.

Stk. 3. Den registrerede har ret til hos den dataansvarlige snarest muligt og uden ugrundet ophold at få at vide, hvilke beslutningsregler der ligger bag en afgørelse som nævnt i stk. 1. § 30 finder tilsvarende anvendelse.

§ 40. Den registrerede kan klage til vedkommende tilsynsmyndighed over behandling af oplysninger vedrørende den pågældende.

Afsnit IV

Sikkerhed

Kapitel 11

Behandlingssikkerhed

§ 41. Personer, virksomheder m.v., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, må kun behandle disse efter instruks fra den dataansvarlige, medmindre

andet følger af lov eller bestemmelser fastsat i henhold til lov.

Stk. 2. Den i stk. 1 nævnte instruks må ikke begrænse den journalistiske frihed eller være til hinder for tilvejebringelsen af et kunstnerisk eller litterært produkt.

Stk. 3. Den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Stk. 4. For oplysninger, som behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, skal der træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

Stk. 5. Justitsministeren kan fastsætte nærmere regler om de i stk. 3 anførte sikkerhedsforanstaltninger.

§ 42. Når en dataansvarlig overlader en behandling af oplysninger til en databehandler, skal den dataansvarlige sikre sig, at databehandleren kan træffe de i § 41, stk. 3-5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker.

Stk. 2. Gennemførelse af en behandling ved en databehandler skal ske i henhold til en skriftlig aftale parterne imellem. Af aftalen skal det fremgå, at databehandleren alene handler efter instruks fra den dataansvarlige, og at reglerne i § 41, stk. 3-5, ligeledes gælder for behandlingen ved databehandleren. Hvis databehandleren er etableret i en anden medlemsstat, skal det fremgå af aftalen, at de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den medlemsstat, hvor databehandleren er etableret, gælder for denne.

Afsnit V Anmeldelse

Kapitel 12

Anmeldelse af behandlinger, der foretages for den offentlige forvaltning

§ 43. Forinden iværksættelse af en behandling af oplysninger, som foretages for den offentlige forvaltning, skal der af den dataansvarlige eller dennes repræsentant foretages anmeldelse til Datatilsynet, jf. dog § 44. Den dataansvarlige kan bemyndige andre myndigheder eller private til at foretage anmeldelse på dennes vegne.

Stk. 2. Anmeldelsen skal indeholde oplysninger om følgende:

- 1) Navn og adresse på den dataansvarlige, dennes eventuelle repræsentant og på en eventuel databehandler.
- 2) Behandlingens betegnelse og formål.
- 3) En generel beskrivelse af behandlingen.
- 4) En beskrivelse af kategorierne af registrerede og af de typer af oplysninger, der vedrører dem.
- 5) Modtagere eller kategorier af modtagere, som oplysningerne kan overføres til.
- 6) Påtænkte overførsler af oplysninger til tredjelande.
- 7) En generel beskrivelse af de foranstaltninger, der iværksættes af hensyn til behandlingssikkerheden.
- 8) Tidspunktet for påbegyndelsen af behandlingen.
- 9) Tidspunktet for sletning af oplysningerne.

§ 44. Behandling, som ikke omfatter oplysninger af fortrolig karakter, er undtaget fra reglerne i § 43, jf. dog stk. 2. En sådan behandling kan uden anmeldelse endvidere omfatte identifikationsoplysninger, herunder personnummer, og oplysninger om betaling til og fra en offentlig myndighed, medmindre der er tale om en behandling som nævnt i § 45, stk. 1.

Bilag

Stk. 2. Justitsministeren fastsætter nærmere regler om de i stk. 1 nævnte behandlinger.

Stk. 3. Behandlinger, hvis eneste formål er at føre et register, der i henhold til lov eller regler udstedt i medfør af lov er beregnet til at informere offentligheden, og som er tilgængeligt for offentligheden, er ligeledes undtaget fra reglerne i § 43.

Stk. 4. Justitsministeren kan fastsætte regler om, at bestemte typer af behandlinger af oplysninger undtages fra bestemmelsen i § 43. Det gælder dog ikke behandlinger som nævnt i § 45, stk. 1.

§ 45. Forinden behandling, som er omfattet af anmeldelsespligten i § 43, iværksættes, skal Datatilsynets udtalelse indhentes, når

- 1) behandlingen omfatter oplysninger, der er omfattet af § 7, stk. 1, og § 8, stk. 1,
- 2) behandlingen udelukkende finder sted med henblik på at føre retsinformationssystemer,
- 3) behandlingen udelukkende finder sted i videnskabeligt eller statistisk øjemed eller
- 4) behandlingen omfatter sammenstilling eller samkøring af oplysninger i kontroløjemed.

Stk. 2. Justitsministeren kan fastsætte regler om, at tilsynets udtalelse skal indhentes inden iværksættelsen af andre end de i stk. 1 nævnte behandlinger.

§ 46. Ændringer i de i § 43, stk. 2, nævnte oplysninger skal forud for iværksættelsen anmeldes til tilsynet. Ændringer af mindre væsentlig betydning kan anmeldes efterfølgende, dog senest 4 uger efter iværksættelsen.

Stk. 2. Forinden iværksættelse af ændringer i de i § 43, stk. 2, nævnte oplysninger i anmeldelser af behandlinger, som er omfattet af § 45, stk. 1 eller 2, skal tilsynets udtalelse indhentes. Ændringer af mindre væsentlig betydning skal alene anmeldes.

Anmeldelse kan ske efterfølgende, dog senest 4 uger efter iværksættelsen.

§ 47. I tilfælde, hvor dataansvaret er henlagt til en underordnet myndighed og tilsynet ikke kan tiltræde udførelsen af en behandling, forelægges sagen for vedkommende minister, der træffer afgørelse i sagen.

Stk. 2. Kan tilsynet ikke tiltræde udførelsen af en behandling, som foretages for en regional eller kommunal myndighed, forelægges sagen for indenrigs- og sundhedsministeren, der træffer afgørelse i sagen.

Kapitel 13

Anmeldelse af behandlinger, der foretages for en privat dataansvarlig

§ 48. Forinden iværksættelse af en behandling af oplysninger, som foretages for en privat dataansvarlig, skal der af den dataansvarlige eller dennes repræsentant foretages anmeldelse til Datatilsynet, jf. dog § 49.

Stk. 2. Anmeldelsen skal indeholde de oplysninger, som fremgår af § 43, stk. 2.

§ 49. Behandling af oplysninger er, bortset fra de i § 50, stk. 2, angivne tilfælde, undtaget fra reglerne i § 48, når

- 1) behandlingen omfatter oplysninger om ansatte, i det omfang behandlingen ikke omfatter oplysninger som nævnt i § 7, stk. 1, og § 8, stk. 4,
- 2) behandlingen omfatter oplysninger om ansattes helbredsforhold, i det omfang behandlingen af helbredsoplysningerne er nødvendig til opfyldelse af bestemmelser i lov eller forskrifter fastsat i henhold til lov,
- 3) behandlingen omfatter oplysninger om ansatte, hvis registrering er nødvendig som følge af kollektiv overenskomst eller kollektiv aftale på arbejdsmarkedet,
- 4) behandlingen omfatter oplysninger om kunder, leverandører eller andre forret-

ningsforbindelser, i det omfang behandlingen ikke omfatter oplysninger som nævnt i § 7, stk. 1, og § 8, stk. 4, eller i det omfang der ikke er tale om behandlinger som omtalt i § 50, stk. 1, nr. 4,

- 5) behandlingen foretages med henblik på udførelsen af markedsundersøgelser, i det omfang behandlingen ikke omfatter oplysninger som nævnt i § 7, stk. 1, og § 8, stk. 4,
- 6) behandlingen foretages af en forening eller lignende, i det omfang der alene behandles oplysninger om foreningens medlemmer,
- 7) behandlingen foretages af advokater eller revisorer som led i deres virksomhed, i det omfang der alene behandles oplysninger vedrørende klientforhold,
- 8) behandlingen foretages af læger, sygeplejersker, tandlæger, kliniske tandteknikere, apotekere, terapiassistenter, kiropraktorer og lignende personer med autorisation til at udøve virksomhed inden for sundheds- og sygeplejen, i det omfang oplysningerne alene anvendes til brug ved denne virksomhed og behandlingen af oplysningerne ikke sker for et privat sygehus, eller
- 9) behandlingen foretages til brug ved en bedriftssundhedstjeneste.

Stk. 2. Justitsministeren fastsætter nærmere regler om de i stk. 1 nævnte behandlinger.

Stk. 3. Justitsministeren kan fastsætte regler om, at andre typer af behandlinger undtages fra bestemmelsen i § 48. Det gælder dog ikke behandlinger, der er omfattet af § 50, stk. 1, medmindre behandlingerne undtages efter § 50, stk. 3.

§ 50. Forinden iværksættelse af en behandling, som er omfattet af anmeldelsespligten i § 48, skal Datatilsynets tilladelse indhentes, når

- 1) behandlingen omfatter oplysninger som nævnt i § 7, stk. 1, og § 8, stk. 4,
- 2) behandlingen af oplysningerne sker med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret,
- 3) behandlingen sker med henblik på erhvervsmæssig videregivelse af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed,
- 4) behandlingen sker med henblik på erhvervsmæssig bistand ved stillingsbesættelse eller
- 5) behandlingen udelukkende finder sted med henblik på at føre retsinformationssystemer.

Stk. 2. Ved overførsel af oplysninger som nævnt i stk. 1 til tredjelande i medfør af § 27, stk. 1, og stk. 3, nr. 2-4, skal Datatilsynets tilladelse indhentes til overførslen, uanset at behandlingen i øvrigt er undtaget fra anmeldelse i medfør af § 49, stk. 1.

Stk. 3. Justitsministeren kan fastsætte undtagelser fra bestemmelserne i stk. 1, nr. 1, og stk. 2.

Stk. 4. Justitsministeren kan fastsætte regler om, at der forinden iværksættelse af andre anmeldelsespligtige behandlinger end de i stk. 1 eller 2 nævnte skal indhentes tilladelse fra tilsynet.

Stk. 5. Tilsynet kan i forbindelse med meddelelse af tilladelse efter stk. 1, 2 eller 4 fastsætte nærmere vilkår for udførelsen af behandlingerne til beskyttelse af de registreredes privatliv.

§ 51. Ændringer i de i § 48, stk. 2, jf. § 43, stk. 2, nævnte oplysninger skal forud for iværksættelsen anmeldes til tilsynet. Ændringer af mindre væsentlig betydning kan anmeldes efterfølgende, dog senest 4 uger efter iværksættelsen.

Stk. 2. Forinden iværksættelse af ændringer i de i § 48, stk. 2, jf. § 43, stk. 2,

Bilag

nævnte oplysninger i anmeldelser af behandlinger, som er omfattet af § 50, stk. 1, 2 eller 4, skal Datatilsynets tilladelse indhentes. Ændringer af mindre væsentlig betydning skal alene anmeldes. Anmeldelse kan ske efterfølgende, dog senest 4 uger efter iværksættelsen.

Kapitel 14

Anmeldelse af behandlinger, der foretages for domstolene

§ 52. Reglerne i §§ 43-46 gælder for anmeldelse til Domstolsstyrelsen af behandling af oplysninger, der foretages for domstolene.

Kapitel 15

Øvrige bestemmelser

§ 53. Databehandlere, der er etableret i Danmark, og som udøver edb-servicevirksomhed, skal forinden påbegyndelsen af behandlingen foretage anmeldelse til Datatilsynet.

§ 54. Tilsynsmyndigheden skal føre en fortegnelse over de behandlinger, der er anmeldt efter §§ 43, 48 og 52. Fortegnelsen, som mindst skal indeholde de oplysninger, som er anført i § 43, stk. 2, skal være tilgængelig for offentligheden.

Stk. 2. En dataansvarlig skal stille de i § 43, stk. 2, nr. 1, 2 og 4-6, nævnte oplysninger om alle de behandlinger, som udføres for vedkommende, til rådighed for enhver, som anmoder derom.

Stk. 3. Offentlighedens adgang til indsigt i den fortegnelse, der er nævnt i stk. 1, og de oplysninger, der er nævnt i stk. 2, kan begrænses, i det omfang det er nødvendigt til forebyggelse, opklaring og efterforskning af lovovertrædelser eller afgørende hensyn til private interesser gør det påkrævet.

Afsnit VI

Tilsyn og afsluttende bestemmelser

Kapitel 16

Datatilsynet

§ 55. Datatilsynet, der består af et råd og et sekretariat, fører tilsyn med enhver behandling, der omfattes af loven, jf. dog kapitel 17.

Stk. 2. Tilsynets daglige forretninger varetages af sekretariatet, der ledes af en direktør.

Stk. 3. Rådet, der nedsættes af justitsministeren, består af en formand, der er dommer, og af 6 andre medlemmer. Der kan udnævnes stedfortrædere for medlemmerne. Medlemmerne og stedfortræderne for disse udnævnes for 4 år.

Stk. 4. Rådet fastsætter sin forretningsorden og de nærmere regler om arbejdets fordeling mellem råd og sekretariat.

§ 56. Datatilsynet udøver sine funktioner i fuld uafhængighed.

§ 57. Ved udarbejdelse af bekendtgørelser, cirkulærer eller lignende generelle retsfor skrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af oplysninger, skal der indhentes en udtalelse fra Datatilsynet.

§ 58. Datatilsynet påser af egen drift eller efter klage fra en registreret, at behandlingen finder sted i overensstemmelse med loven og regler udstedt i medfør af loven.

Stk. 2. Tilsynet kan til enhver tid tilbagekalde en afgørelse truffet i henhold til § 27, stk. 4, eller § 50, stk. 2, jf. § 27, stk. 1, eller stk. 3, nr. 2-4, såfremt Europa-Kommissionen træffer afgørelse om, at der ikke må ske overførsel af oplysninger til bestemte tredjelande, eller om, at der lovligt kan ske en sådan overførsel. Dette gælder dog kun, såfremt tilbagekaldelsen er

nødvendig for at efterleve Kommissionens afgørelse.

§ 59. Datatilsynet kan påbyde en privat dataansvarlig at ophøre med en behandling, der ikke må finde sted efter denne lov, og at berigtige, slette eller blokere bestemte oplysninger, som er omfattet af en sådan behandling.

Stk. 2. Tilsynet kan forbyde en privat dataansvarlig at anvende en nærmere angiven fremgangsmåde i forbindelse med behandlingen af oplysninger, hvis tilsynet finder, at den pågældende fremgangsmåde medfører en væsentlig risiko for, at der behandles oplysninger i strid med loven.

Stk. 3. Tilsynet kan påbyde en privat dataansvarlig at træffe bestemte tekniske og organisatoriske sikkerhedsforanstaltninger mod, at der behandles oplysninger, som ikke må behandles, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Stk. 4. Tilsynet kan i særlige tilfælde meddele databehandlere påbud eller forbud, jf. stk. 1-3.

§ 60. Datatilsynet træffer over for vedkommende myndighed afgørelse i sager vedrørende § 7, stk. 7, § 9, stk. 3, § 10, stk. 3, § 13, stk. 1, § 27, stk. 4, §§ 28-31, § 32, stk. 1, 2 og 4, §§ 33-37, § 39 samt § 58, stk. 2.

Stk. 2. I andre tilfælde afgiver tilsynet udtalelser over for den dataansvarlige myndighed.

§ 61. Datatilsynets afgørelser efter denne lov kan ikke indbringes for anden administrativ myndighed.

§ 62. Datatilsynet kan kræve enhver oplysning, der er af betydning for dets virksomhed, herunder til afgørelse af, om et forhold falder ind under lovens bestemmelser.

Stk. 2. Tilsynets medlemmer og personale har til enhver tid mod behørig legitimation uden retskendelse adgang til alle lokaler, hvorfra en behandling, som foretages for den offentlige forvaltning, administreres, eller hvorfra der er adgang til de oplysninger, som behandles, samt til lokaler, hvor oplysningerne eller tekniske hjælpemidler opbevares eller anvendes.

Stk. 3. Bestemmelsen i stk. 2 gælder tilsvarende for behandlinger, som foretages for private dataansvarlige, i det omfang behandlingen er omfattet af § 50.

Stk. 4. Bestemmelsen i stk. 2 gælder også, for så vidt angår den behandling, der udføres af databehandlere som nævnt i § 53.

§ 63. Datatilsynet kan bestemme, at anmeldelser og ansøgninger om tilladelse efter denne lov og ændringer heri kan eller skal indgives på nærmere angiven måde.

Stk. 2. For indgivelse af følgende anmeldelser og ansøgninger om tilladelser i henhold til denne lov betales 1.000 kr.:

- 1) Anmeldelse i henhold til § 48.
- 2) Tilladelse i henhold til § 50.
- 3) Anmeldelse i henhold til § 53.

Stk. 3. En anmeldelse som nævnt i stk. 2, nr. 1 og 3, anses først for indgivet, når betaling er sket. Datatilsynet kan bestemme, at en tilladelse som nævnt i stk. 2, nr. 2, ikke meddeles, før betaling er sket.

Stk. 4. Bestemmelserne i stk. 2, nr. 1 og 2, gælder ikke for behandlinger, der udelukkende finder sted i videnskabeligt eller statistisk øjemed.

Stk. 5. Såfremt en behandling både skal anmeldes efter § 48 og tillades efter § 50, betales kun ét gebyr.

§ 64. Datatilsynet kan af egen drift eller efter anmodning fra en anden medlemsstat påse, at en behandling af oplysninger, som finder sted i Danmark, er lovlig, uanset at den pågældende behandling er undergivet en anden medlemsstats lov-

Bilag

givning. Bestemmelserne i §§ 59 og 62 finder tilsvarende anvendelse.

Stk. 2. Datatilsynet kan videregive oplysninger til tilsynsmyndigheder i andre medlemsstater i det omfang, det er nødvendigt for at påse overholdelsen af bestemmelserne i denne lov eller af den pågældende medlemsstats databeskyttelseslovgivning.

§ 65. Datatilsynet afgiver en årlig beretning om sin virksomhed til Folketinget. Beretningen offentliggøres. Tilsynet kan i øvrigt offentliggøre sine udtalelser. Bestemmelsen i § 30 finder tilsvarende anvendelse.

§ 66. Datatilsynet og Domstolsstyrelsen samarbejder, i det omfang det er nødvendigt for at opfylde deres pligter, navnlig ved at udveksle alle relevante oplysninger.

Kapitel 17

Tilsyn med domstolene

§ 67. Domstolsstyrelsen fører tilsyn med behandling af oplysninger, der foretages for domstolene.

Stk. 2. Tilsynet omfatter behandling af oplysninger med hensyn til domstolenes administrative forhold.

Stk. 3. For anden behandling af oplysninger træffes afgørelse af vedkommande ret. Afgørelsen kan kæres til højere ret. For særlige domstole, hvis afgørelser ikke kan indbringes for højere ret, kan den i 1. pkt. nævnte afgørelse kæres til den landsret, i hvis kreds retten er beliggende. Kærefristen er 4 uger fra den dag, afgørelsen er meddelt den pågældende.

§ 68. For Domstolsstyrelsens udøvelse af tilsyn i henhold til § 67 gælder bestemmelserne i §§ 56 og 58, § 62, stk. 1, 2 og 4, § 63, stk. 1, og § 66. Domstolsstyrelsens afgørelser er endelige.

Stk. 2. Ved udarbejdelse af bekendtgørelser eller lignende generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af oplysninger, der foretages for domstolene, skal der indhentes en udtalelse fra Domstolsstyrelsen.

Stk. 3. Domstolsstyrelsen offentliggør en årlig beretning om dens virksomhed.

Kapitel 18

Erstatnings- og strafansvar

§ 69. Den dataansvarlige skal erstatte skade, der er forvoldt ved behandling i strid med bestemmelserne i denne lov, medmindre det godtgøres, at skaden ikke kunne have været afværget ved den agtpågivenhed og omhu, der må kræves i forbindelse med behandling af oplysninger.

§ 70. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 4 måneder den, der i forbindelse med en behandling, som udføres for private,

- 1) overtræder § 4, stk. 5, § 5, stk. 2-5, § 6, § 7, stk. 1, § 8, stk. 4, 5 og 7, § 9, stk. 2, § 10, stk. 2 og 3, 1. pkt., § 11, stk. 2 og 3, § 12, stk. 1 og stk. 2, 1. pkt., § 13, stk. 1, 1. pkt., §§ 20-25, § 26, stk. 1, stk. 2, 2. pkt., og stk. 3, § 27, stk. 1, § 28, stk. 1, § 29, stk. 1, § 31, §§ 33 og 34, § 35, stk. 2, §§ 36 og 37, § 39, stk. 1 og 3, § 41, stk. 1 og 3, § 42, § 48, § 50, stk. 1 og 2, § 51, § 53 eller § 54, stk. 2,
- 2) undlader at efterkomme Datatilsynets afgørelse efter § 5, stk. 1, § 7, stk. 7, § 13, stk. 1, 2. pkt., § 26, stk. 2, 1. pkt., § 27, stk. 4, §§ 28 og 29, § 30, stk. 1, § 31, § 32, stk. 1 og 4, §§ 33-37, § 39, § 50, stk. 2, eller § 58, stk. 2,
- 3) undlader at efterkomme Datatilsynets krav efter § 62, stk. 1,
- 4) hindrer Datatilsynet i at få adgang efter § 62, stk. 3 og 4,

- 5) tilsidesætter vilkår som nævnt i § 7, stk. 7, § 9, stk. 3, § 10, stk. 3, § 13, stk. 1, § 27, stk. 4, § 50, stk. 5, eller en betingelse eller et vilkår for en tilladelse i henhold til regler udstedt i medfør af loven eller
- 6) undlader at efterkomme forbud eller påbud, der er meddelt i henhold til § 59 eller i henhold til regler udstedt i medfør af loven.

Stk. 2. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 4 måneder den, der i forbindelse med en behandling, som udføres for offentlige myndigheder, overtræder § 41, stk. 3, eller § 53 eller tilsidesætter vilkår som nævnt i § 7, stk. 7, § 9, stk. 3, § 10, stk. 3, § 13, stk. 1, § 27, stk. 4, eller en betingelse eller et vilkår for en tilladelse i henhold til regler udstedt i medfør af loven.

Stk. 3. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 4 måneder den, der i forbindelse med en behandling, som er undergivet en anden medlemsstats lovgivning, undlader at efterkomme Datatilsynets afgørelser efter § 59 eller at opfylde Datatilsynets krav efter § 62, stk. 1, eller hindrer Datatilsynet i at få adgang efter § 62, stk. 3 og 4.

Stk. 4. I regler, der udstedes i medfør af loven, kan der fastsættes straf af bøde eller eller fængsel indtil 4 måneder.

Stk. 5. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

§ 71. Den, der driver eller er beskæftiget med virksomhed som nævnt i § 50, stk. 1, nr. 2-5, eller § 53, kan ved dom for strafbart forhold frakendes retten hertil, såfremt det udviste forhold begrunder en nærliggende fare for misbrug. I øvrigt finder straffelovens § 79, stk. 3 og 4, anvendelse.

Kapitel 19

Afsluttende bestemmelser, herunder ikrafttrædelsesbestemmelser m.v.

§ 72. Vedkommende minister kan i særlige tilfælde fastsætte nærmere regler for behandlinger, som udføres for den offentlige forvaltning.

§ 73. Justitsministeren kan fastsætte nærmere regler for bestemte typer af behandlinger, som udføres for private dataansvarlige, herunder at bestemte typer oplysninger ikke må behandles.

§ 74. Brancheforeninger eller andre organer, som repræsenterer andre kategorier af private dataansvarlige, kan i samarbejde med Datatilsynet udarbejde adfærdskodekser, der skal bidrage til en korrekt anvendelse af reglerne i denne lov.

§ 75. Justitsministeren kan fastsætte regler, som er nødvendige for at gennemføre de af Det Europæiske Fællesskab udstedte beslutninger, som træffes med henblik på gennemførelse af direktivet om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, eller regler, som er nødvendige for at anvende de af Fællesskabet udstedte retsakter på direktivets område.

§ 76. Loven træder i kraft den 1. juli 2000.

Stk. 2. Lov om offentlige myndigheders registre, jf. lovbekendtgørelse nr. 654 af 20. september 1991, og lov om private registre m.v., jf. lovbekendtgørelse nr. 622 af 2. oktober 1987, ophæves.

Stk. 3. Registerrådets medlemmer indtræder som medlemmer af Datarådet, indtil justitsministeren har udnævnt Datarådets medlemmer.

Stk. 4. Bekendtgørelse nr. 160 af 20. april 1979 om forretningsorden for registerrådet m.v. gælder for Datatilsynets

Bilag

virksomhed, indtil den ophæves eller erstattes af regler udstedt i medfør af denne lov.

Stk. 5. Anordning nr. 73 af 5. marts 1979 om, at forskrifter for registre m.v., der udfærdiges i medfør af loven om offentlige myndigheders registre, ikke indføres i Lovtidende, ophæves.

Stk. 6. Klage- eller tilsynssager, der er oprettet før den 24. oktober 1998, færdigbehandles efter de hidtil gældende regler. Datatilsynet udøver den kompetence, som efter disse regler tilkommer Registertilsynet.

Stk. 7. Datatilsynet udfører i øvrigt de opgaver, som efter lovgivningen udføres af Registertilsynet.

§ 77. For behandlinger, der foretages for private, og som er iværksat før den 24. oktober 1998, skal reglerne i kapitel 13 være opfyldt senest den 1. oktober 2000.

Stk. 2. For behandlinger, der foretages for offentlige myndigheder, og som er iværksat før den 24. oktober 1998, skal reglerne i kapitel 12 og 14 være opfyldt senest den 1. april 2001.

Stk. 3. Behandlinger, der er iværksat før den 24. oktober 1998, kan fortsætte uden tilladelse i 16 uger efter lovens ikrafttræden, hvis der skal indhentes tilladelse hertil efter reglerne i lovens afsnit II eller bestemmelsen i stk. 7.

Stk. 4. Behandlinger, der er iværksat den 24. oktober 1998 eller senere, men inden lovens ikrafttræden, kan fortsætte uden forudgående anmeldelse, udtalelse eller tilladelse i 16 uger efter lovens ikrafttræden.

Stk. 5. Der skal senest 16 uger efter lovens ikrafttræden foretages anmeldelse efter bestemmelsen i § 53.

Stk. 6. Justitsministeren kan fastsætte regler om, at den i stk. 1 og 2 nævnte frist forlænges.

Stk. 7. Tilsynsmyndigheden kan i ganske særlige tilfælde efter ansøgning bestemme, at behandlinger, der er iværksat

før lovens ikrafttræden, kan fortsætte uanset behandlingsreglerne i afsnit II.

§ 78. Behandlinger, som før lovens ikrafttræden er anmeldt efter § 2, stk. 3, 2. pkt., i lov om private registre m.v., kan fortsætte efter de hidtil gældende regler indtil den 1. oktober 2001. Datatilsynet udøver den kompetence, som efter disse regler tilkommer Registertilsynet.

Stk. 2. Behandlinger som nævnt i stk. 1 skal overholde lovens § 5 og §§ 41 og 42. For disse behandlinger kan den registrerede kræve berigtigelse, sletning eller blokering af oplysninger, der er urigtige eller vildledende, eller som opbevares på en måde, der er uforenelig med de legitime formål, som den dataansvarlige forfølger. Datatilsynet fører tilsyn efter reglerne i lovens kapitel 16.

§ 79. Et samtykke, som er givet i overensstemmelse med de hidtil gældende regler, gælder for behandlinger, der foretages efter lovens ikrafttræden, såfremt samtykket opfylder kravene i denne lovs § 3, nr. 8, sammenholdt med § 6, nr. 1, § 7, stk. 2, nr. 1, § 8, stk. 2-5, § 11, stk. 2, nr. 2, eller stk. 3, eller § 27, stk. 3, nr. 1.

§ 80. I lov nr. 572 af 19. december 1985 om offentlighed i forvaltningen, som senest ændret ved lov nr. 276 af 13. maj 1998, foretages følgende ændring:

1. § 5, stk. 3, affattes således:

»Stk. 3. Vedkommende minister kan fastsætte regler om offentlighedens adgang til at blive gjort bekendt med fortegnelser som nævnt i stk. 2, der ikke er omfattet af lov om behandling af personoplysninger. Der kan herunder fastsættes regler om betaling.«

§ 81. I lov nr. 430 af 1. juni 1994 om massemediers informationsdatabaser foretages følgende ændringer:

1. I § 3, stk. 1 og 3, og § 6, stk. 1, ændres »Registertilsynet« til: »Datatilsynet«.

2. Som ny § 11 a indsættes følgende bestemmelse:

»§ 11 a. Der skal træffes de fornødne sikkerhedsforanstaltninger mod, at informationer i offentligt tilgængelige informationsdatabaser ændres af uvedkommende.«

3. § 16, stk. 1, nr. 1, affattes på følgende måde:

»1) overtræder § 4, § 5, § 7, § 8, stk. 1, § 9, nr. 2 og 3, § 11, stk. 1 og 3, eller § 11 a.«

4. § 17 affattes således:

»§ 17. Et massemedie skal erstatte skade, der er forvoldt ved behandling i strid med bestemmelserne i denne lov, medmindre det godtgøres, at skaden ikke kunne have været afværget ved den agtpågivenhed og omhu, der må kræves i forbindelse med behandling af oplysninger. Lovgivningens almindelige erstatningsregler finder i øvrigt anvendelse.

Stk. 2. Lovgivningens almindelige regler om straf finder anvendelse på sager omfattet af denne lov.

Stk. 3. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.«

§ 82. I tinglysningsloven, jf. lovbe-
kendtgørelse nr. 622 af 15. september
1986, som senest ændret ved § 2 i lov nr.
1019 af 23. december 1998, foretages føl-
gende ændringer:

1. I § 50 d, stk. 1, indsættes i stedet for
»Registertilsynet«: »Domstolsstyrelsen«.

2. § 50 d, stk. 2 og 3, affattes således:

»Stk. 2. Domstolsstyrelsen fører tilsyn
med tinglysningsregistrene. Domstolssty-
relsens afgørelser er endelige.

Stk. 3. Justitsministeren fastsætter nær-
mere regler om dette tilsyn efter forhand-
ling med Domstolsstyrelsen.«

§ 83. Loven gælder ikke for Færøerne,
men kan ved kongelig anordning sættes i
kraft for rigsmyndighedernes behandling af
oplysninger med de afvigelser, som de
særlige færøske forhold tilsiger. Loven
gælder heller ikke for Grønland, men kan
ved kongelig anordning sættes i kraft med
de afvigelser, som de særlige grønlandske
forhold tilsiger.

Stikordsregister

- Adfærdskodekser – se også selvregulering
9, 48, 82, 119, 120, 137, 205
- Almindelige oplysninger 42, 43
- Artikel 29 gruppen 7, 22, 47, 48, 49, 57,
83, 96, 109, 118, 127, 140ff
- Behandling 20
- begrebet 20, 31
 - formål 37, 44, 85, 98, 106
 - hjemmel 45, 72
 - betingelser 53, 82
- Behandlingsformer 32, 33, 36
- Integritetsrisikable 33, 43, 106
- Beskyttelseshensyn 18, 19, 61
- Bindende virksomhedsregler (BVR) 137ff
- Corporate governance 111, 138, 166
- Datatilsynet 22, 28, 36, 46, 47, 49, 71, 72,
76, 99, 102, 133, 139, 153ff
- Dataansvarlig 35ff
- Datakvalitet, se også korrektion 38, 39,
74, 75, 86
- Datapoliti 162
- Databehandler 133ff
- Dataoverførsler 12f, 39f, 49f, 62f, 80f,
110f, 151ff
- økonomiske hensyn 13
 - personlige og ideelle hensyn 13
- Databeskyttelsesretten 19, 21, 22, 26, 31ff
- Data havens 23, 81, 163
- Datakvalitet 38f, 74f, 86
- Databeskyttelsesniveau 53, 114, 146f
- Databeskyttelseslovgivning 52, 115, 133,
142
- Direktiv 95/46 14, 170, 183
- Eksportlandet 25, 27, 31, 51, 52ff, 174
- Eksport af persondata 25, 31, 40, 68
- EMRK 19
- E-mail 24
- Elektronisk signatur 27
- Erstatning 161
- Erhvervshemmelighed 71
- Europarådet 79ff
- EU institutioner 60f
- Europol aftalen 15
- Europarådets konvention 108/81 79, 90,
176
- EØS – komiteen 59, 72, 76
- FAQ 125, 143ff
- Finansielle data 13
- FN 177
- Fortrolige oplysninger 193
- Forumshopping 95, 161
- Formålsbestemthed 37, 86, 148
- Fri overførsel 59f, 70f
- FTC – Federal Trade Commission 145
- Føderale lande 92
- Følsomme oplysninger 19, 43f, 128, 134
- GATS – General Agreement on Trade in
Services 144
- Globalisering 12, 23, 166, 169
- God databehandlingsskik 36, 72f, 97f
- Græsrodsbevægelser (NGO'er) 162
- G8 landene 177
- Harmonisering 62ff, 135, 178
- Hjemmel 41ff, 72
- Hjemmelsprincip 41
- Human resources – oplysninger om ansat-
te 13, 42f, 98, 109
- Håndhævelse 151ff
- Ideelle hensyn 13
- ILO konvention 102

Stikordsregister

- Importlandets ret 53ff, 92
Indsigtsret 73f, 87
Indsigelsesret 45, 75f, 88
Integritetskrænkelser 16, 22, 32, 51, 117f, 168
Internationalisering 23, 111, 168
Internettet 27, 69, 89, 151
Indsigtsanmodning 73
Inspektion 140, 159
Integritetsbeskyttelse 36, 79, 81, 97
- Juridiske personer, oplysninger om 17
- Korrektion, se også datakvalitet 75
Kontrakter 121ff, 136ff
Kontrakt for dataansvarlige 125ff
Kontrakt for databehandlere 133f
Koncern 137ff
Kryptering 27, 39, 128
Krypteringsnøglen 16
Kreditoplysning 92, 107
Kreditvurdering 92, 107
Kundedata 13, 44
- Lex Imperfecta 176
Lex Mercatoria 122
Lindqvist dommen 55, 63
Lovvalg 21f
Lovlige overførsler 156, 159
Luftfartselskaber 145
- Manuelle data 26, 55
Markedsføring 18, 44ff, 88
Menneskerettigheder – se også EMRK 91
- OECD 12, 79, 80, 171, 178, 180
Offentlighed 162
Offentlig sektor 13ff
Offentlighed 162f
Oplysningspligt 70f, 87, 127
Oplysninger om
– ansatte, human resources 13
– juridiske personer 17
– virksomheder 17
– foreninger 17, 44
– myndigheder 17
– IS selskaber 17
Overførsel
– begrebet 15f
– regler 25
– til tredjelande 79ff
– EU lande 178
– behov 14
– problemer 15, 19, 22ff
– til kommercielt behov 28
– til privat formål 28
Overførselsbehov, det økonomiske 111ff
- Persondata 16f
– definition 18
– i digital form 27
Personlige hensyn – se også ideelle hensyn 13
Personnummer 19
Privathed 18f
Privatlivets fred 12, 19, 59, 80, 89, 171
Private interesser 71
Præsumptionsansvar 129, 161
- Reeksport 88, 90, 93, 132, 141, 147f
Registrerede 168
– definition 16
– erstatning 161
Register over overførsler 74
Registertilsynet 105
Retskrav 101ff
Retssikkerhed 15
Registerlove 20, 80, 154
Retskultur 13, 17, 49, 63, 94
Rettigheder 18, 35, 46f, 75
- Retsplejeloven 103
Retseksport 113, 171, 177
- Safe Harbor 93, 112f, 143ff
Samtykke 25, 41ff, 98ff, 168
Sanktioner 89, 129, 160f
Schengen aftalen 15
Sektorlovgivning 43, 68
Selvkontrol, de registreredes 157
Selvregulering 119ff, 136, 144f, 166
Semifølsomme oplysninger 19
Sikkerhed 39ff, 70, 85, 87, 117
Standardkontrakt 123ff
– 2001 for dataansvarlige 125
– 2001 for databehandlere 133

Stikordsregister

- 2004 for dataansvarlige 130
- Spærrelister 42
- Straffeloven 22, 160f
- Straf 160f

- Terror 14
- Tilsyn, se også datatilsynet 46ff, 66, 104, 124ff, 153ff
- Tilsynssamarbejde 158
- Transmission 24f, 39
- Tilladelse 104
 - fra datatilsynet 40

- Tilbagekaldelse 99
 - aftilladelse 110
- Tilstrækkelighedsprincippet 86, 87

- Ulovlige overførsler 158, 159ff
- Ulovlig persondatabehandling 22

- Virksomhedstyper 115f
- Værdispring 42, 43

- WTO 144, 176, 177

- Ytringsfriheden 29