

**Mona Naomi Lintvedt
Christopher J. Helgeby**

**OVERFØRING AV
PERSONOPPLYSNINGER TIL
TREDJELAND**

**KRAVET TIL TILSTREKKELIG BESKYTTELSE ETTER
EU-DIREKTIVET OM PERSONVERN ART. 25**

Henvendelser om denne bok kan gjøres til:

Institutt for rettsinformatikk
Postboks 6706 St. Olavs plass
0130 Oslo
Tlf. 22 85 01 01
www.jus.uio.no/iri/

ISBN 82-7226-056-5
ISSN 0806-1912

unipubskriftserier

Utgitt i samarbeid med Unipub AS
Denne boken går inn i universitets- og høyskolerådets skriftserie
Trykk: GCSM AS
Omslagsdesign Kitty Ensby

Institutt for rettsinformatikks utgivelser i sekriftserien Complex er støttet av:
Advokatfirmaet Selmer DA
Wikborg Rein & Co
Lovdata

INNHOOLD

Forord.....	5
1. Innledning.....	7
1.1 Bakgrunn for emnet og problemstilling.....	7
1.2 Rettskildebildet	9
1.2.1 Personregisterloven og forslag til ny personopplysningslov	9
1.2.2 Internasjonale rettskilder.....	9
1.3 Spesielle metodiske problemer.....	12
1.3.1 Begrepsbruk	12
1.3.2 Bruken av rettskildene.....	12
1.3.3 Andre metodiske forhold.....	14
1.4 Den videre fremstillingen	15
2. Personvern og sentrale begreper.....	17
2.1 Generelt om personvern.....	17
2.2 Personopplysningsbegrepet	19
2.2.1 Informasjonskravet	19
2.2.2 Tilknytningskravet.....	20
2.2.3 Identifikasjonskravet.....	21
2.3 Behandlingsbegrepet	22
3. Overføring til tredjeland	25
3.1 Overføring av personopplysninger.....	25
3.1.1 Hva er en overføring?	26
3.1.2 Overføring via Internett	29
3.1.3 EU-direktivets geografiske virkeområde.....	30
3.2 Tredjeland.....	33
3.2.1 EU-landene.....	33
3.2.2 EFTA-landene.....	34
3.2.3 Kan land utenfor EØS tiltre direktivet?.....	34
3.2.4 Uttrykket stater i personopplysningsloven § 29.....	35
4. Kravet til tilstrekkelig beskyttelse	39
4.1 Oversikt over japansk personvernrett	39
4.1.1 Grunnloven	39
4.1.2 Nasjonal lovgivning.....	40
4.1.3 Lokal lovgivning.....	41

4.1.4	<i>Ulovfestet rett</i>	42
4.1.5	<i>Forarbeider</i>	42
4.1.6	<i>Juridisk teori</i>	43
4.1.7	<i>Offentlig rettledning</i>	43
4.1.8	<i>Metodiske problemer ved bruken av japanske kilder</i>	45
4.2	<i>Vurderingen av tilstrekkelighetsnivået</i>	46
4.2.1	<i>Hva menes med begrepet tilstrekkelig?</i>	47
4.2.2	<i>Hvilke regler skal vurderes?</i>	48
4.2.3	<i>Hvilke krav stilles til mottakerlandets regler?</i>	50
4.2.4	<i>Oppsummering</i>	61
4.3	<i>Kontrollordninger</i>	62
4.3.1	<i>EUs krav til tilsynsmyndighet</i>	63
4.3.2	<i>Kontrollordninger i Japan</i>	64
4.3.3	<i>Sanksjonsmuligheter</i>	71
4.3.4	<i>Oppsummering</i>	74
4.4	<i>Hvem skal foreta beskyttelsesvurderingen?</i>	75
4.4.1	<i>Behandlingsansvarlig</i>	75
4.4.2	<i>Tilsynsmyndigheten</i>	77
4.4.3	<i>Kommisjonen</i>	79
5.	Sammenfatning og vurdering	85
Etterord		89
Norge		89
EU		89
	<i>Status for implementeringen av personverndirektivet</i>	89
	<i>Godkjennelse av tredjelands beskyttelsesnivå</i>	90
	<i>Safe Harbour avtalen</i>	91
	<i>Standardkontrakt</i>	91
Japan		92
Bibliografi		95
Utredninger og uttalelser		98
Lover og retningslinjer m.m.		100
Annet		101
Vedlegg		105
The Act for Protection of Computer-Processed Personal Data Held by Administrative Organs		103
Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector		109

FORORD

Denne avhandlingen ble skrevet høsten 1999 og er preget av rettssituasjonen den gang. For å gi et best mulig bilde av emnet opp til i dag har vi inkludert et etterord som oppsummerer endringer i rettskildebildet siden avhandlingen ble levert.

Avhandlingen ble skrevet av Mona Naomi Lintvedt og Christopher J. Helgeby i samarbeid. I forbindelse med avhandlingen fikk vi stipend fra Sasakawa Young Leadership Foundation som gjorde det mulig å dra til Tokyo for å forske ved Chuo universitetet.

Vi ønsker først og fremst å takke professor Dag Wiese Schartum som har vært vår veileder, både for hans råd og evne til å akseptere vår uenighet. Der nest vil vi rette en stor takk til professor Masao Horibe ved Chuo universitet i Tokyo. Hans engasjement, kunnskaper og gjestfrihet har bidratt sterkt til å gjøre det mulig for oss å skrive om dette temaet. Og til slutt ønsker vi å takke professor Jon Bing som har en helt egen evne til å se mulighetene når vitebe-gjærlige studenter kommer med aparte prosjekter.

Til slutt vil vi takke Christophers trofaste Macintosh Powerbook som har ledet oss gjennom oppgaven uten det minste problemer.

Oslo, 15. august 2002

1. INNLEDNING

1.1 Bakgrunn for emnet og problemstilling

Teknologisk utvikling, endrede kommunikasjonsmønstre og økende internasjonal handel byr på utfordringer for personvernet. Personvernregler i ett land er ikke lenger nok til å sørge for at personvernet holdes i hevd. Den økende muligheten for transport av personopplysninger gjør det enkelt å omgå slike regler, dersom det ikke finnes mekanismer som ivaretar opplysningenes integritet ved overføring. På den annen side kan for strenge regler hindre internasjonalt samarbeid både økonomisk og politisk. Et eksempel på at personopplysninger har blitt nektet overført, er at Tyskland siden sommeren 1996 har nektet å utlevere fingeravtrykk til Norge i forbindelse med kontroll av asylsøkere. Årsaken er at tyske myndigheter ikke anser de norske personvernregler som gode nok.¹

Det følger av legalitetsprinsippet at faktiske handlinger er tillatt så lenge ikke annet er bestemt i lov. Hvilke begrensninger som gjelder for overføring av personopplysninger er dermed opp til lovgiver å bestemme. Hvordan regulering av personopplysninger skal skje vil på mange måter være et dilemma. Overføring av personopplysninger er nødvendig for internasjonal handel og kontakt, men mangel på restriksjoner kan føre til dårligere vern for individet. I et globalt samfunn er behovet for ensartede regler også nødvendig for å hindre omgåelse av nasjonale regler ved å flytte opplysningene til «personvernparadis».²

Overføring av personopplysninger skjer ved de fleste transaksjoner og kontraktsoppfyllelser. Sett at Peder Ås skal på ferie i utlandet. Han bestiller reisen via et reisebyrå, og bestillingen registreres i et felles reservasjonssystem for reiselivsbransjen lokalisert utenfor Norge. Fra denne basen kan både flyselskapet, hotellet og leiebilfirmaet ta ut opplysninger om Peder for å gjennomføre reservasjonen i sine systemer. Når Peder er på reise bruker han sitt kredittkort til betalinger. Denne bruken registreres og sendes til kredittkortselskapet, som igjen sender informasjonen til Peders bank i Norge. En av dagene får Peder et illebefinnende og legges inn på det lokale sykehuset. Legen er usikker på diagnosen, og ber om å få tilsendt Peders sykejournal fra

¹ Johansen, Per Anders «Nektet å utveksle beviser», *Aftenposten (Morgen)* 18. desember 1998:2

² Djønne, Eirik; Grønn, Tove og Hafli, Tor *Personregisterloven med kommentarer*, TANO, Oslo 1987:155

hans lege i Norge. Fra sykehuset sendes informasjon til Peders forsikringsselskap i Norge for å kontrollere at kostnadene dekkes. To år senere ønsker Peder igjen å besøke landet. Han blir avvist på grensen med den begrunnelse at han har en sjelden sykdom. Etter Peders forrige opphold er hans sykejournal blitt tatt vare på, og videregitt til immigrasjonsmyndighetene. Dette scenariet viser at overføring av personopplysninger er svært vanlig. Det viser også at overføring både kan være til gunst og til ulempe for den det gjelder. På den ene siden forventer man at visse tjenester er tilgjengelige og at hjelp ytes når det er nødvendig, men like fullt stiller man strenge krav til hva opplysninger om en selv brukes til.

I denne særavhandlingen vil vi drøfte hvilke krav som stilles når personopplysninger skal overføres over landegrensene. Oppgaven vil fokusere på reglene som gjelder innen den Europeiske Union (EU), og hvilke konsekvenser reglene har for land utenfor Unionen. Hovedvekten vil ligge på EUs direktiv 95/46/EF *om beskyttelse av fysiske personer i forbindelse med behandling af personopplysninger og om fri udveksling af sådanne oplysninger* av 24.oktober 1995 art. 25 som i utgangspunktet stiller et krav om at land utenfor EU – tredjeland – må ha et tilstrekkelig beskyttelsesnivå for behandling av personopplysninger dersom en overføring skal kunne skje. Hovedtemaet i avhandlingen er å kartlegge begrepet *tilstrekkelig beskyttelse*. Vi vil ikke drøfte alle momentene som er gitt i EU-direktivet art. 25 nr. 2, men fokusere på de forutsetningene som må være tilstede for at en overføring skal kunne skje. Avhandlingen avgrenses også mot unntaksbestemmelsene i EU-direktivet art. 26.

For å gjøre problemstillingen mer konkret kommer vil til å benytte oss av Japan som eksempel på tredjeland. Valget av Japan er gjort av flere grunner. Den mest innlysende er at Japan er et land utenfor EU. At landet er demokratisk og industrialisert med en godt utbygget rettslig infrastruktur gjør det enklere å drøfte rettslige problemstillinger. Som verdens nest største økonomi³ er Japan en vesentlig handelspartner for både Norge og EU, og nesten enhver form for handel forutsetter en eller annen form for utveksling av personopplysninger. På den annen side har landet et svært ulikt kulturelt utgangspunkt enn vestlige land, og det påvirker også måten retten fungerer på. Alle disse faktorene gjør Japan til et sentralt og interessant land å knytte eksempler opp mot.

3

Se CIA factbook 1998

<http://www.odci.gov/cia/publications/factbook/ja.html#econ> (16. juli 1999)

1.2 Rettskildebildet

1.2.1 Personregisterloven og forslag til ny personopplysningslov

Det rettslige utgangspunktet for overføring av personopplysninger til andre land er i dag lov av 9. juni 1978 nr. 48 *om personregistre m.m. (personregisterloven)*. Etter personregisterloven § 36 kan konsesjonspliktige personregistre ikke overføres til utlandet uten samtykke av Kongen, men denne myndigheten er delegert til Datatilsynet.⁴ Personregisterloven § 36 tredje ledd gir hjemmel for utarbeidelse av forskrift som kan gjøre unntak fra dette. I forskrift av 21. desember 1979 § 8-1⁵ er plikten til å innhente samtykke erstattet med en meldeplikt til Datatilsynet i forkant av overføringen. Gjennom meldeplikten kan Datatilsynet kontrollere overføringer ut av landet, og gripe inn dersom det anses nødvendig. For overføringer som Norge har plikt til å foreta i henhold til en folkerettslig avtale eller som følge av medlemskap i en internasjonal organisasjon, foreligger det ikke meldeplikt, jf personregisterloven § 36 tredje ledd og forskriften § 8-1 annet ledd.

For tiden pågår det et arbeid med en ny lov som skal avløse personregisterloven. Forslag til denne loven ble lagt fram i juni 1999 ved Ot. prp. nr. 92 (1998-99) *om lov om behandling av personopplysninger (personopplysningsloven)*,⁶ basert på NOU 1997:19 *Et bedre personvern – forslag til lov om behandling av personopplysninger*. Bakgrunnen for denne lovtutviklingen er den utfordring teknologisk og økonomisk utvikling skaper for personvernet, samt EUs vedtagelse av personverndirektivet.⁷ Regelen om overføring av personopplysninger finnes i personopplysningsloven § 29. Her er kravet at en overføring bare kan skje til land som *sikrer en forsvarlig behandling* av opplysningene. Det oppstilles ingen konsesjonsplikt, men all elektronisk behandling av personopplysninger skal meldes i forkant til Datatilsynet, jfr. personopplysningsloven § 31 første ledd litra a.

1.2.2 Internasjonale rettskilder

Av de internasjonale rettskildene er den mest sentrale for denne fremstillingen Europaparlamentets og rådets direktiv 95/46/EF af 24. oktober 1995 *om beskyttelse av fysiske personer i forbindelse med behandling af perso-*

⁴ Se kongelig resolusjon av 21. desember 1979

⁵ Forskrifter i medhold av lov om personregistre m.m., gitt av Justisdepartementet 21. desember 1979 i medhold av kongelig resolusjon av 21. desember 1979.

⁶ Tilråding fra Justis- og politidepartementet av 25. juni 1999, godkjent i statsråd samme dag.

⁷ NOU 1997:19 Et bedre personvern s. 19

nopplysninger og om fri utveksling af sådanne oplysninger – heretter kalt direktivet. Dette direktivet ble vedtatt 24. oktober 1995, og etter en tre års implementeringsperiode trådte det i kraft 24. oktober 1998. Direktivet presiserer og utvider prinsippene i Europarådskonvensjonen om personvern, jf direktivets fortale punkt 11. Bakgrunnen for direktivet var at ulikheter i medlemslandene personvernlovgivning ville være et hinder for den frie flyt av personopplysninger innad i EU, og dermed hemme det økonomiske samarbeidet.⁸ Fri flyt av varer, personer, tjenester og kapital henger nøye sammen med fri flyt av personopplysninger, fordi slike opplysninger vil være aktuelle ved nær sagt all utveksling og kommunikasjon. Utgangspunktet for direktivet er derfor at overføring av personopplysninger skal skje uten restriksjoner innad i EU, jf direktivet art. 1 nr. 2. Dette kan lett komme på kant med personverninteresser, men ved å innføre et høyt beskyttelsesnivå skal individets rettigheter ivaretas. Utveksling av personopplysninger skal derfor ikke utgjøre noen trussel mot det enkelte menneskets grunnleggende rettigheter, jf direktivets fortale punkt 3.

Europarådets konvensjon 28. januar 1981 nr. 108 om personvern i forbindelse med elektronisk databehandling av personopplysninger⁹ har hatt stor betydning for utvikling av personvernreglene i Europa. Konvensjonens formål er å sikre respekt for rettigheter og grunnleggende friheter, og særlig respekt for personvern med hensyn til den økende internasjonale utveksling av personopplysninger, jf konvensjonens fortale. Alle Europarådets medlemmer kan tiltre konvensjonen, jf konvensjonen art. 22 nr.1, og den vil ved tiltredelse være folkerettslig bindende. Også andre land kan tiltre konvensjonen, jf konvensjonen art. 23. nr. 1, men foreløpig har ingen gjort det.¹⁰ Konvensjonens art. 12 regulerer overføring av personopplysninger til land som har tiltrådt konvensjonen, såkalt transborder flows of personal data. Utgangspunktet er at overføring av personopplysninger til et annet tiltredende land ikke kan forbys dersom slikt forbud utelukkende begrunnes i personvern hensyn, jf konvensjonen art. 12 nr. 2. Det er adgang til å gjøre unntak fra denne bestemmelsen etter konvensjonen art. 12 nr. 3 for kategorier av personopplysninger som reguleres særskilt. Overføring av slike opplysninger kan dermed forbys eller gjøres avhengig av betingelser, dersom mottakerlandet ikke har regler som gir lik beskyttelse. Videre i fremstillingen vil ikke

⁸ NOU 1997:19 *Et bedre personvern* s. 38

⁹ Convention for the protection of individuals with regard to automatic processing of personal data 108/81 av 28. januar 1981
<http://www.coe.fr/eng/legaltxt/108e.htm> (15. juli 1999)

¹⁰ Se Europarådets offisielle hjemmeside
<http://www.coe.fr/tablconv/108t.htm> (15. juli 1999)

Europarådskonvensjonen i seg selv bli behandlet, men den kan være et moment i tolkingen av direktivet.

En regulering som har større internasjonal rekkevidde er *Guidelines concerning the protection of privacy and transborder flows of personal data* av 23. september 1980 utarbeidet av Organisasjonen for økonomisk samarbeid og utvikling (OECD).¹¹ Til tross for at retningslinjene ikke er rettslig bindende, er de av stor betydning for utvikling av personvernregler internasjonalt. Blant annet har den japanske lov på området sin opprinnelse i OECD retningslinjene.¹² Bakgrunnen for retningslinjene er medlemsstatenes felles interesse i å beskytte privatlivets fred og individuelle friheter, men også å fjerne hindringer for informasjonsflyt mellom landene for å bidra til økonomisk og sosial utvikling, jf fortalen til retningslinjene. Medlemslandene er ikke forpliktet til å følge retningslinjene, men henstilles å ta hensyn til disse i sin nasjonale lovgivning vedrørende personvern.¹³ Retningslinjene oppstiller åtte grunnleggende prinsipper som bør være basis for regulering av personvern: Begrensning av innsamling, datakvalitet, formålsbestemthet, bruksbegrensning, sikkerhet, åpenhet, individuell deltakelse og ansvarlighet.¹⁴ Når det gjelder overføring av personopplysninger mellom medlemslandene skal denne være så uhindret som mulig. Medlemslandene oppfordres til ikke å innføre restriksjoner på slik overføring, og til å være tilbakeholden med å utvikle praksis og lover som vil skape hindringer for flyt av personopplysninger over landegrensene, jf retningslinjene del 3. De prinsippene som fremgår av retningslinjene ligger til grunn for mesteparten av den personvernregulering vi ser i Japan, og kan være et tolkingsverktøy i drøftelsen av disse.

¹¹ OECD Guidelines concerning the protection of privacy and transborder flows of personal data av 23. september 1980.

<http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM> (9. juli 1999)

¹² Franklin, Charles E. H. (red) *Business guide to privacy and data protection legislation*, Kluwer law international, Den Haag 1996:279

¹³ Rekommandasjon fra OECD Council av 23. september 1980.

¹⁴ Collection limitation, data quality, purpose specification, use limitation, security safeguard, openness, individual participation, accountability.
Del 2 av OECD retningslinjene.

1.3 Spesielle metodiske problemer

1.3.1 Begrepsbruk

Vi kommer til å basere oss på den danske utgaven av EU-direktivet fordi denne ligger nærmest det norske språket. Den danske utgaven benytter begrepet *videregivelse* når den omtaler transport av personopplysninger, jf direktivet art. 25. I den svenske, engelske og franske versjonen av direktivet brukes *överföring*, *transfer* og *le transfert*, og disse skal etter fellesskapsretten anses som synonyme.¹⁵ Vi vil i det følgende bruke den norske oversettelsen *overføring* i stedet for *videregivelse* fordi vi mener det gir bedre assosiasjoner til handlingen.

1.3.2 Bruken av rettskildene

Vår problemstilling er knyttet til overføring av personopplysninger over landegrensene, og etter norsk rett reguleres dette av personregisterloven. I vår fremstilling velger vi imidlertid å se på EU-direktivet som primærkilde, og det krever en forklaring. EU-direktivet representerer en ny tilnærming til problematikken rundt overføring av personopplysninger. Det stilles krav til at mot-takerlandet innehar et *tilstrekkelig beskyttelsesnivå* for behandling av personopplysninger, før overføring kan skje. Dette er regler som er mer nyanserte enn någjeldene norsk lov, og som kommer til å påvirke norsk rett blant annet gjennom forslaget til ny personopplysningslov. EU-direktivet har også betydning for norsk rettstilstand fordi det er tatt inn i EØS-avtalen,¹⁶ og vi er av den grunn folkerettslig forpliktet til å ta hensyn til disse reglene. Drøftelsen av EU-direktivet kan derfor bidra til å gi et bilde av fremtidig norsk rettstilstand.

Når vi har valgt å basere oss på kilder fra fellesskapsretten får dette betydning for drøftelsen. EUs direktiver er bindende for medlemsstatene i unionen, men krever at hvert enkelt land selv gjennomfører dem internrettslig.¹⁷ Direktiver retter seg altså mot medlemsstatene og ikke rettssubjektene, og på den måten ingen plikter for rettssubjektene før de er gjennomført i nasjonal

¹⁵ Kapteyn, P. J. G. og Verloren van Themaat, P. *Introduction to the law of the European Communities – After the coming into force of the Single European act*, (2. utgave) Kluwer law and taxation publishers, Deventer 1989:63-65

¹⁶ EØS-komiteéns beslutning nr. 83/1999 av 25. juni 1999 om endring av EØS-avtalens protokoll 37 og vedlegg XI (Telekommunikasjonstjenester).

¹⁷ Avtale om Det europeiske økonomiske samarbeidsområde (EØS-avtalen) av 2. mai 1992 Konsolideret utgave af Traktaten om oprettelse af det Europæiske Fællesskab av 10. november 1997 (Romatraktaten) art. 249 tredje ledd.

rett.¹⁸ Våre konklusjoner i drøftelsen av direktivet vil derfor ikke ha direkte virkning på noe enkeltlands rettssituasjon. Det vil derimot kunne danne bakteppe for hvordan personvernet skal håndheves innen EU.

Tolking av EU-direktiver skjer på et noe annet grunnlag enn det som er vanlig innen norsk rettskildelære. Siden alle språk innen unionen er offisielle vil også alle språkutgaver av direktivet være like autentiske. Dette gjør at man ikke vektlegger forskjeller i den språklige utformingen av teksten, men den språklige forståelsen vil være relevant for tolkingen av direktivet.¹⁹ En videre tolkning må skje på grunnlag av de rettskildene som brukes innen fellesskapsretten. Romatraktaten²⁰ ligger til grunn for hele fellesskapsretten, som en slags grunnlov, og kan være et moment i tolkingen av direktivet. Europadomstolens praksis er generelt en svært viktig rettskilde, men i spørsmål relatert til personverndirektivet har domstolen ennå ikke avgjort noen saker. Lovforarbeider spiller også mindre rolle. En av grunnene kan være de relativt store forandringer forslagene gjennomgår i prosessen frem mot vedtatt tekst. På den annen side vil fortalen ofte presisere bakgrunnen og de forskjellige formål med direktivet, og vil derfor være et tolkingsmoment. I dette rettskildemessig karrige landskapet vil formålsbetraktninger få større vekt. I EU-direktivet har lovgiver konkretisert formålet, og det må tas i betraktning ved tolkingen. Rettsområdet er svært dynamisk og blir raskt påvirket av ny teknologi, samtidig må hensynet til individets rettigheter ivaretas på best mulig måte. Ved å vektlegge formålsbestemmelser gir man mulighet for en bredere tolking av enkelte bestemmelser. Dette vil særlig være aktuelt ved anvendelse av skjønsmessige og vurderingspregede regler. Direktivets funksjon som rammelov for den enkelte medlemsstat gjør at man ofte må trekke ut mer generelle regler og supplere disse med hva som er formålstjenlig i den enkelte situasjon.²¹ Reelle hensyn vil derfor få en betydning i vurderingen. De tolkingsmomenter vi kommer til å bruke vil av den grunn i stor grad være basert på formålsbetraktninger og reelle hensyn.

Personopplysningsloven slik den foreligger per juli 1999 er regjeringens forslag, og den er ennå ikke vedtatt i Stortinget. Lovforslaget er dermed ikke

¹⁸ Arnesen, Finn; Borgli, Anneke B.; Bull, Henrik; Foyn, Sven; Rognstad, Ole-Andreas og Stemhaug, Helge *Oversikt over EØS-retten*, (1. utgave) Universitetet i Oslo, Oslo 1994:96

¹⁹ Arnesen, Finn; Borgli, Anneke B.; Bull, Henrik; Foyn, Sven; Rognstad, Ole-Andreas og Stemhaug, Helge *Oversikt over EØS-retten*, (1. utgave) Universitetet i Oslo, Oslo 1994:94

²⁰ Konsolideret utgave af Traktaten om oprettelse af det Europæiske Fællesskab av 10. november 1997 (Romatraktaten)

²¹ Arnesen, Finn; Borgli, Anneke B.; Bull, Henrik; Foyn, Stein; Rognstad, Ole-Andreas og Stemhaug, Helge *Oversikt over EØS-retten*, (1. utgave) Universitetet i Oslo, Oslo 1994:103-107

gjeldende rett, men gir indikasjon på hvilken retning personvernlovgivningen tar. Det forventes at ny lov vil bli vedtatt, men lovens endelige form kan bli en annen enn den vi ser i dagens forslag. Vi vil likevel benytte oss av lovforslaget i drøftelsene av overføring av personopplysninger. Ikke som en kilde til norsk rettstilstand, men for å belyse enkelte sider ved direktivets bestemmelser. Personopplysningsloven blir dermed først og fremst brukt som eksempel materiale for problemstillingene. I dette arbeidet vil NOU 1997:19 *Et bedre personvern – forslag til lov om behandling av personopplysninger* og Ot. prp. 92 (1998-99) *om lov om behandling av personopplysninger* bli brukt for å tolke forslaget til personopplysningslov.

Personregisterloven vil bli berørt for å belyse eventuelle forskjeller mellom gjeldende rett og den forventede fremtidige rettstilstand, men vil ikke bli grundigere behandlet. Annen europeisk rett vil bli nevnt for å illustrere former implementeringen av EU-direktivet kan ta.

1.3.3 Andre metodiske forhold

I forbindelse med arbeidet med denne avhandlingen fikk vi muligheten til å reise til Japan for på empirisk grunnlag å få innsikt i japansk personvernrett. Begrenset interesse for fagfeltet fra japansk hold og språkbarrierer, har imidlertid påvirket tilgjengeligheten av kilder. Mesteparten av den innsamlede informasjonen har vi fått fra professor Masao Horibe ved Chuo universitetet i Tokyo.²² Gjennom samtaler med ham har vi fått klargjort mye av situasjonen på området. Bruk av muntlige kilder gir lett rom for misforståelser, og er vanskelige å etterprøve. Vi har imidlertid forsøkt å bøte på dette ved å basere spørsmålsstillingen på eksisterende regler og artikler for på den måten å ha et felles referansepunkt. Vi har også i ettertid gått gjennom det materialet vi har diskutert for å luke ut eventuelle misoppfatninger. Professor Horibe har også vurdert og bekreftet autenticiteten av de japanske rettskildene vi bruker. Mye av den juridiske teori vi har å støtte oss på er skrevet av professor Horibe. Man kan stille spørsmål ved om dette vil gi et nyansert nok bilde av situasjonen, eller om det vil bli en ensidig fremstilling. Det viste seg fort ved vårt besøk i Japan at det er professor Horibe som er den ledende autoritet på området. Han er også en av veldig få som befatter seg med personvernrett. Til tross for at vi gjerne skulle hatt mer informasjon fra annet hold, har det vist seg at det nærmest ikke eksisterer og derfor blir professor Horibe så sentral. Vårt mål er uansett ikke å foreta en fullstendig tolking av japansk personvernrett, men bruke det som eksempel sett opp mot EUs regler om tilstrekkelig beskyttelse av personopplysninger.

²² Professor Horibe er også professor emeritus ved Hitotsubashi universitetet, Tokyo

Vi vil også nevne noen momenter i forbindelse med vår bruk av elektroniske kilder. Mange av de kildene vi baserer drøftelsen på er lastet ned fra Internett. Dette er gjort av praktiske hensyn. Flere av kildene, og i særlig grad de japanske, er svært vanskelige å få tak i. Dessuten gir elektroniske versjoner av kildene det enklere å finne frem til relevante passuser ved hjelp av tekstsøk. Vi har forsøkt å kvalitetskontrollere alle kildene ved å basere oss på nettsteder med en viss autoritet, for eksempel statlige organer og velkjente organisasjoner. Ved bruk av disse kildene er det henvist til URL²³ og dato for siste nedlasting. Vi har også tatt papirkopi av alle kildene for sikker referanse.

1.4 Den videre fremstillingen

I den videre fremstillingen vil vi i kapittel 2 gi en oversikt over personvernteori sett med norske øyne. Her vil vi også gå igjennom sentrale begreper som personopplysningsbegrepet og behandlingsbegrepet. I kapittel 3 vil vi se på hva en overføring er, og hva som menes tredjeland. I kapittel 4 vil vi se på hvilke krav som stilles i vurderingen av om et land innehar tilstrekkelig beskyttelse, og hvordan vurderingen foretas. Det er i dette kapittelet vi vil bruke japansk rett som eksempelmateriale, og vi vil forut for tilstrekkelighetsdrøftelsen gå gjennom rettskildene i japansk personvernrett. Avslutningsvis vil vi i kapittel 5 sammenfatte de problemene direktivet reiser og knytte noen kommentarer til disse.

²³ Universal Resource Locator – en angivelse av adresser til sider på World Wide Web.

2. PERSONVERN OG SENTRALE BEGREPER

2.1 Generelt om personvern

Innholdsmessig er begrepet *personvern* svært vidt og kan ses fra et utall vinkler. Det er derfor vanskelig å gi et enhetlig bilde av hva det omfatter rent språklig. Personvern er i dag en samlebetegnelse som omfatter en rekke rettigheter knyttet til individet. Felles er imidlertid at rettighetene anses som ideelle, altså knyttet til forhold av ikke-økonomisk betydning. Det utelukker ikke at ideelle interesser også kan fremme økonomiske hensyn, men stort sett vil disse interessene stå mot hverandre. Idéen om personvern kan oppfattes som antitesen til andre ideelle rettigheter som ytringsfrihet og krav til offentlighet. Dette gir et unyansert bilde fordi ingen av disse begrepene er absolutte. På enkelte områder vil personvernet komme i motstrid med andre prinsipper, mens de andre ganger vil utfylle hverandre.

I norsk rett ble personvern som begrep innført i forbindelse med arbeidet til personregisterloven på 1970-tallet, men det ble ikke inntatt noen legaldefinisjon av begrepet i loven.²⁴ En mulig definisjon av personvern er at det er beskyttelse av individer mot farer og ulemper forbundet med bruken av datamaskiner i offentlig og privat forvaltning.²⁵ Man må imidlertid forstå begrepet langt videre enn det lovens virkeområde skulle tilsi. Før arbeidet med personregisterloven begynte benyttet man seg av betegnelsen *personlighetens rettsvern*. Begrepet ble brukt for å beskrive den ulovfestede rett individet har til legemlig integritet, frihetsvern, rett til ære og vern om den enkelte som personlighet.²⁶ Fokus var rettet mot individets rett til å ha sitt eget privatliv i fred. Behovet for vern av privatliv vokste stadig som følge av teknologisk utvikling. Særlig bidro fremveksten av massemediene til at fokus mot enkelt-individer kunne oppfattes som krenkende. Medienes mulighet til å spre informasjonen raskere og til flere mottakere bido til å øke skadeevnen. Retten til privatlivets fred ble for første gang slått fast i norsk rett gjennom saken mot filmen *To mistenkelige personer* Rt 1952/1217. Filmen var basert på virkelige hendelser rundt en drapssak tredve år tidligere. Da filmen skulle

²⁴ NOU 1974:22 Persondata og personvern og NOU 1975:10 Offentlige persondata system og personvern

²⁵ Selmer, Knut «Datatilsynets rolle i et komplisert samfunn», Eirik Dønne (red) *Datatilsynet – ti år som personvernets vokter*, Complex 4/90 TANO, Oslo 1990:60

²⁶ Lassen, Birger Stuevold (red) *Knophs oversikt over Norges rett*, (10. utgave) Universitetsforlaget, Oslo 1993:113 flg

lanseres hadde den ene av hovedmennene sonet sin straff, og mente derfor at visning av filmen ville være i strid med hans rett til privatliv. Høyesterett anerkjente at *alminnelig rettsvern for personligheten*²⁷ kunne eksistere på ulovfestet grunnlag, og forbød visning av filmen. Denne retten vil imidlertid være begrenset til bare å gjelde sivilrettslige rettigheter. Skillet blir tydelig når vi ser hen til *Telefonsjikanedommen* Rt 1952/989 hvor en kvinne ble plaget av utidige telefonoppringninger, og ville ha oppringeren straffet. Høyesterett kom her til at legalitetsprinsippet sto i veien for at den tiltalte kunne straffes.

Samfunnsutviklingen har ført til at forståelsen av personvern som vern av privatlivets fred er for snever. I NOU 1997:19 *Et bedre personvern* presenteres tre synsvinkler på personvernet.²⁸ Det *integritetsfokusede* personvernet har mange paralleller til det som er nevnt ovenfor, fordi det tar utgangspunkt i individets behov for selvbestemthet innenfor sin egen private sfære. Dette strekker lengre enn å bare verne individet overfor overgrep. I dansk rett er det fremholdt at man har eiendomsrett over informasjon om en selv, og dermed også full kontroll over disse opplysningene.²⁹ Denne presumsjonen har ikke hatt samme betydning i norsk rett, men viser ett av ytterpunktene i debatten. En annen synsvinkel er å se på den potensielle makt innehaveren av personopplysninger kan få i kraft av informasjonen. Dersom bedrifter og offentlige institusjoner fritt kan tilegne seg og bruke slik informasjon, kan det føre til en forrykkelse av maktbalansen i samfunnet. Dette kan man kalle det *maktfokusede* personvern. Personopplysninger brukes også som grunnlag for beslutninger av ulike slag. Beslutningene tas gjerne av autoritetsorganer som stat, bedrifter eller organisasjoner, og påvirker ofte individets rettigheter og plikter. Mengden, typen og kvaliteten på opplysningene kan påvirke beslutningsprosessen. For å hindre vilkårlighet, forskjellsbehandling og maktmisbruk blir det derfor viktig å sørge for at grunnlaget for beslutningene er korrekte, og man snakker her om det *beslutningsfokusede* personvern. Det er ikke noe motsetningsforhold mellom disse måtene å se på personvernet på, men synsvinklene bidrar til å identifisere ulike problemstillinger knyttet til personvern.

Gjennom norsk juridisk teori er det utviklet en modell som beskriver enkelte personvern hensyn som interesser tillagt individet – *interesseteorien*. Modellen ble utarbeidet av Dag Ragnar Blekeli og Knut S. Selmer på 70-tallet, og baserer seg på syv antatte interesser delt opp i de to hovedkategoriene individuelle og kollektive interesser.³⁰ For individet gjelder dette *dis-*

²⁷ Rt 1952/1217 s. 1219

²⁸ NOU 1997:19 *Et bedre personvern* s. 21-24

²⁹ Blume, Peter «Om den skandinaviske registerlovgivning», *Tidsskrift for rettsvitenskap* 2/87:455-483

³⁰ Blekeli, Dag Ragnar og Selmer, Knut S *Data og personvern*, Universitetsforlaget, Oslo 1977

kresjon – den enkeltes mulighet til kontroll over egne opplysninger; *fullstendighet* – de opplysningene som finnes skal være korrekte og oppdaterte; *inn-syn* – muligheten til å følge med i behandlingen av egne opplysninger og *privatlivets fred* – den enkeltes rett til å få være i fred. I tillegg kommer de kollektive interesser som beskriver interessene individene har som gruppe i en *borgervennlig forvaltning*, et *robust samfunn* og et *begrenset overvåkningsnivå*. Dette må ikke betraktes som en uttømmende liste med absolutte interesser. Essensen i denne tilnærmingen til personvern er å gi individene antatte interesser ut ifra hvordan samfunnet fungerer. Metoden gir derfor mulighet for supplering av interesser ved endrede samfunnsforhold eller annen vektlegging innen spesielle fagområder.³¹

2.2 Personopplysningsbegrepet

EU-direktivet gjelder bare for overføring av personopplysninger, og vi må derfor gå nærmere inn på hva en personopplysning egentlig er. Personopplysninger er i direktivet art. 2 litra a definert som *enhver form for informasjon om en identifisert eller identifiserbar fysisk person*. Det er altså tre sentrale punkter knyttet til en personopplysning: den skal ha et *informasjonsinnhold* og dette skal kunne knyttes til en *fysisk person* slik at det kan bidra til en *identifisering* av personen.

2.2.1 Informasjonskravet

EU-direktivet sier at *enhver form for informasjon* omfattes, men hva er egentlig *informasjon*? Språklig sett er dette et svært vidt begrep, og omfatter kunnskap av nær sagt enhver type. Nøyaktighet eller kvalitet spiller i utgangspunktet ingen rolle. At solen går ned eller at en bil er grønn må oppfattes som informasjon på samme måte som detaljer fra Peder Ås kontoutskrift. Kunnskapen behøver heller ikke være basert på noe objektivt eller konkret, også antagelser, vurderinger og andre subjektive betraktninger vil være inkludert.

Ved å legge til grunn en vid forståelse av hva som er informasjon sikrer man at det ikke er informasjonsinnholdet som begrenser hvorvidt noe anses som en personopplysning. I stedet bruker man personen selv og tilknytningen til denne til å avgrense mot hva som er relevant informasjon.

³¹ I NOU 1993:22 *Pseudonyme helseregistre* omformuleres Blekeli og Selmers interessemodell ved at fokus rettes mot pasienters rettigheter innenfor helsevesenet.

2.2.2 Tilknytningskravet

EU-direktivet tar i sin definisjon i art. 2 litra a utgangspunkt i at informasjonen skal kunne knyttes til en *fysisk person*. Dette utelukker i utgangspunktet juridiske personer, men ser en hen til direktivets fortale punkt 24 hindrer ikke dette at man på nasjonalt nivå kan velge å inkludere juridiske personer, slik det er gjort etter personregisterloven § 1 annet ledd. Primært er det overfor fysiske personer at personvern hensynene bør ivaretas, mens det for juridiske personer er mer økonomiske motiver bak en eventuell beskyttelse.³²

Det fremkommer ikke av direktivet hvorvidt man med fysiske personer mener levende personer eller om også døde personer er omfattet. Bruken av begrepet *fysiske personer* synes å være begrunnet i å markere skillet mot juridiske personer, og ikke nødvendigvis for å ekskludere døde individer. Denne vagheten kan tyde på at det er opp til medlemslandene selv å avgjøre i nasjonal lov hvorvidt opplysninger om avdøde personer skal omfattes eller ikke,³³ og som eksempel sies det eksplisitt i den svenske personoppgiftslagen § 3³⁴ at personopplysninger skal knyttes til en fysisk person *som är i livet*. Formålet med direktivet er å verne det enkelte individs rettigheter og frihet,³⁵ og man kan spørre om døde personer har behov for slikt vern. Det kan være hensiktsmessig å beskytte informasjon om personen for å verne dennes ettermæle, men dette bør muligens reguleres av andre bestemmelser enn personvernreglene. I norsk rett reguleres for eksempel ærekrenkelse mot avdødes minne av straffeloven § 252.³⁶ Vanskeligere kan det være å avgrense mot døde personer i forbindelse med kartlegging av genetisk informasjon. Informasjon om genetiske defekter hos avdøde personer kan anses som personopplysninger fordi den bidrar med kunnskap som kan ha betydning for levende slektninger. Det er også dette standpunkt departementet har tatt i innstillingen til personopplysningsloven der det heter at *opplysninger om en avdød person er bare «personopplysning» i lovens forstand dersom opplysningen også kan knyttes til en levende person.*³⁷

³² Ot. prp. nr. 92 (1998-99) om lov om behandling av personopplysninger s. 26

³³ Cullen international (red) *A business guide to changes in European data protection legislation*, Kluwer law international, Den Haag 1999:27

³⁴ Personoppgiftslag SFS 1998:204 av 29. april 1998

³⁵ EU-direktivets fortale nr. 7

³⁶ Almindelig borgerlig Straffelov 22. mai 1902 nr. 10

³⁷ Ot. prp. nr. 92 (1998-99) om lov om behandling av personopplysninger s. 102

2.2.3 Identifikasjonskravet

Det er opplysninger som *direkte* eller *indirekte* kan bidra til identifikasjon av en person som anses som personopplysninger. Direkte identifikasjon skjer der en opplysning kan knyttes til en spesifikk person uten forutgående undersøkelser. Det typiske eksemplet på dette er et navn eller et bilde. Indirekte identifikasjon skjer når data knyttes til en person, men da bare etter nærmere undersøkelser. Dette vil være tilfellet med for eksempel et kontonummer, nummerskilt på bil eller IP-nummer.³⁸ Dette bildet må imidlertid nyanseres noe. Språklig kan direkte identifikasjon ofte oppfattes som sikker eller *entydig* identifikasjon, men dette er ikke alltid tilfellet. Et navn kan innehas av flere personer og et bilde kan vise en enegget tvillingbror. På samme måte kan indirekte identifikasjon også gi entydig identifikasjon gjennom for eksempel fødselsnummer. Blir flere informasjonstyper sammenholdt, for eksempel navn og fødselsnummer, er man derimot sikrere på at identifikasjonen er entydig.

En direkte og entydig identifikasjon representerer kjerneområde for hva som er personopplysninger. Det går imidlertid også en grense for hvor perifer informasjonen får bli med hensyn til identifikasjonskravet. Det kan være opplysninger som har en svært fjern tilknytning til personer eller persondata som har blitt anonymisert. De problemene man da står overfor er på den ene siden å sette en grense for hva som er relevant informasjon i identifikasjonsøyemed, og på den andre siden å sette en grense for de ressurser som skal til for å bidra til identifikasjon.

Ser vi på hvor nær tilknytning det er mellom informasjonen og personen er det først og fremst indirekte informasjon som fører til problemer. Et eksempel kan være en person som deltar i et rasistisk møte og parkerer bilen utenfor. Hvis noen velger å registrere bilskiltene til de tilstedeværende vil dette være personopplysninger. Velger man bare å registrere biltype vil ikke kravet til identifikasjon være oppfylt. Det kan derimot oppstå et problem dersom en av deltagerene har en svært karakteristisk bil slik at man gjennom modell og farve kan knytte den opp mot en enkelt person. Informasjonen kan da få et så entydig preg at kravet til identifikasjon er oppfylt, og opplysningene må anses som personopplysninger. En sammenstilling av perifere data kan

³⁸ IP-nummer eller Internet Protocol number er en unik gruppe av tall som identifiserer data-maskiner på Internett. For å få tilgang til Internett må alle maskiner ha en slik nummeradresse. IP-nummer kan være statiske slik at du har det samme nummeret hver gang, eller dynamiske når man for eksempel kobler seg opp via en modempool og dermed får tildelt et nytt nummer for hver nye oppkobling. IP-nummeret identifiserer bare maskinen som er oppkoblet. Det er først dersom man sammenholder denne informasjonen med lister over hvem som innehar de forskjellige maskinene at identifikasjon av personer kan skje.

altså gjøre informasjonen relevant. Man må derfor ikke bare vurdere opplysningene for seg, men også se dem i den sammenheng de skal bli brukt.

Anonymisering stiller oss overfor problemet med hvor store ressurser som kreves for at identifisering skal kunne skje. Gitt ubegrensede ressurser kan knapt noen opplysninger oppfattes som anonyme. Her gir EU-direktivets fortale punkt 26 en pekepinn ved at alle hjelpemidler skal tas i betraktning som med rimelighet kan tenkes anvendt for å identifisere den aktuelle personen. Det kreves altså ikke at opplysningene er absolutt sikre, men at det skal foretas en rimelighetsvurdering av de tiltak som kan settes i verk for å identifisere en person. Finner man at de ressurser som kreves for å identifisere en person overgår det man med rimelighet kan forvente, skal personen anses som anonym med den konsekvens at dataene ikke anses som personopplysninger. Hva som er rimelig vil kunne variere ut i fra forholdene, men tatt i betraktning at teknologien ofte utvikler seg hurtigere enn lovverket vil denne løsningen gi rom for fleksibilitet. Uansett er det ikke bare den enkelte databehandlers ressurser som skal vurderes, men også enhver annen som kan tenkes å behandle opplysningene, jf fortalen punkt 25.

I en situasjon hvor opplysninger er krypterte vil forholdene være noe annerledes. Her vil opplysningene i utgangspunktet være så sikre at kravet til identifikasjon ikke er oppfylt. Problemet oppstår når noen har tilgang til krypteringsnøkkelen. Ved hjelp av denne vil man kunne frembringe opplysningene i deres opprinnelige form, og da vil de utvilsomt være personopplysninger. Bør man i et slikt tilfelle operere med flere definisjoner av samme type data? Velger man å betrakte krypterte opplysninger som personopplysninger bare overfor den som har nøkkelen, men som anonyme data overfor andre vil man få en spesiell regel som kan være vanskelig å håndheve. Selve krypteringsnøkkelen vil ikke være underlagt restriksjonene i direktivet, og kan dermed distribueres fritt også til utlandet. Dermed kan det bli svært vanskelig å kontrollere at opplysningene behandles forsvarlig. Hensynet til en retts teknisk enkel regel og den utvidede muligheten til å omgå bestemmelsene i direktivet tilsier derfor at krypterte opplysninger bør anses som personopplysninger så lenge noen har muligheten til å dekode dem. Skulle krypteringsnøkkelen gå tapt, vil nok derimot kravet til identifikasjon ikke være oppfylt.

2.3 Behandlingsbegrepet

Måten personvernet håndheves på er avhengig av hvilken betraktning man legger til grunn. I personregisterloven tar man utgangspunktet i at personopplysninger bør beskyttes dersom de inngår i et *register* eller på annen måte

bidrar til overvåking, jf personregisterloven § 1 første ledd og §§ 37a og 37b. I EU-direktivet og personopplysningsloven er lovens saklige virkeområde blant annet angitt ut ifra om det skjer en *behandling* av personopplysningene, jf direktivet art. 2 litra b. Et registerbegrep fordrer at det eksisterer flere opplysninger og at disse er satt i system, jf personregisterloven § 1 annet ledd annet punktum. Når fokus rettes mot behandlingen blir ikke antall opplysninger og deres sammenstilling avgjørende, men hvorledes de håndteres. Behandling av opplysninger favner altså videre enn registrering av opplysninger.

Hva en behandling innebærer er definert i direktivet art. 2 litra b som *enhver operation eller række af operationer [...] som personoplysninger gøres til genstand for*. Deretter følger en oppramsing som antyder rekkevidden av begrepet. Listen er ikke uttømmende, jf *f.eks.*, men er ment som en eksemplifisering for å understreke at alle typer bruk av personopplysninger dekkes. Hvorvidt en serie av operasjoner vil anses som en eller flere behandlinger vil variere og må vurderes særskilt.³⁹ Innsamling, lagring, sammenstilling og overføring kan derfor samlet betraktes som én behandling i enkelte tilfeller. Behandling etter direktivet er begrenset av forhold som faller utenfor fellesskapsretten, og som ellers angår den enkelte stats offentlige sikkerhet, jf direktivet art. 3 nr. 2 første strekpunkt. Direktivet utelukker også behandling foretatt av en fysisk person til rent personlig bruk, jf direktivet art. 3 nr. 2 annet strekpunkt.

Når fokus er rettet mot behandlingen i stedet for registreringen betyr det at reguleringen av personvernet utvides. En slik utvidelse kan styrke personvernet, men resultatet vil også være at mengden av saker til behandling vil øke. Dette kan virke hindrende på informasjonsflyten, og føre til mindre effektivitet. EU-direktivets løsning er å gjøre det enklere å behandle personopplysninger ved å introdusere en meldeplikt i stedet for en konsesjonsplikt, jf direktivet art. 18. Man slipper dermed tidkrevende forhåndsgodkjenning, og kan iverksette behandlingen umiddelbart. Slik forenklet saksbehandling kan svekke personvernet. For å motvirke dette er den behandlingsansvarlige pålagt flere plikter, og skal i en overføringssituasjon selv vurdere om mottakerlandet innehar tilstrekkelig beskyttelse.

³⁹ NOU 1997:19 *Et bedre personvern* s. 56

3. OVERFØRING TIL TREDJELAND

EU-direktivet om personvern skal på den ene side sørge for fri flyt av personopplysninger mellom medlemsstatene, og på den annen side sikre individenes grunnleggende rettigheter, jf direktivets fortale punkt 3. Dette motsetningsforhold mellom økonomiske og ideelle interesser er forsøkt løst ved at man innad i EU sørger for ensartet regulering av personvern, jf direktivets fortale punkt 8. Samtidig er utveksling av personopplysninger med land utenfor EU nødvendig for vekst i internasjonal handel, men man ønsker ikke at slik utveksling skal svekke det personvern individenes har etter EU-direktivet, jf direktivets fortale punkt 56. For å ivareta dette vernet, har man valgt å regulere overføringer av personopplysninger ut av EU. I direktivet art. 25 nr. 1 heter det:

Medlemsstaterne fastsetter bestemmelser om, at videregivelse til et tredjeland af personopplysninger, 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 [...].

Vi har ovenfor sett hva som ligger i begrepene *personopplysninger* og *behandling*, og vi vil i det følgende se hva som menes med *overføring* og *tredjeland*.

3.1 Overføring av personopplysninger

Det er bare dersom det skjer en overføring av personopplysninger ut av EU at direktivet art. 25 får anvendelse. Hva som ligger i en *overføring* må derfor drøftes nærmere. Vi har ikke funnet EU-rettslige kilder som gir henvisninger til hvordan begrepet skal tolkes. Tolkningen av begrepet vil derfor være basert på en språklig forståelse sett i sammenheng med direktivets formål. Overføring er en faktisk handling som ikke er begrenset til personvernsammenheng innen EU. Andre kilder kan derfor gi nyttig innsikt. I det følgende vil vi se hen til noen av de vurderingene som kommer frem i forarbeidene til personopplysningsloven.

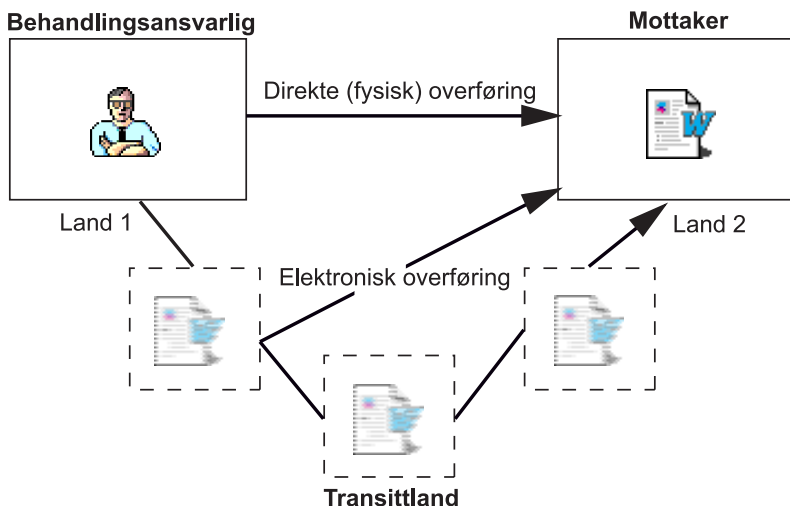
Direktivet gjelder både for manuell og elektronisk behandling av personopplysninger, jf art. 3 nr. 1. I en overføringssituasjon er det bruk av elektroniske medier som reiser de mest interessante problemstillingene, og det er

disse vi vil konsentrere oss om. Reglene vil imidlertid være like for manuell og elektronisk overføring.

3.1.1 Hva er en overføring?

Språklig forståelse av begrepet overføring krever at det skjer en eller annen form for overflytting av den aktuelle informasjonen fra en hånd til en annen. Overføring kan skje ved utlevering av lagringsmedier som diskett, tape eller dokumenter, men også elektronisk i nettverk. Hvorvidt opplysningene kopieres og således også blir igjen på opprinnelsesstedet er uten betydning. I utgangspunktet er det besittelsen av opplysningene som avgjør om en overføring har skjedd, men som vi skal se passer ikke denne definisjonen inn i alle situasjoner. Når fokus flyttes fra registeret til behandlingen vil det oppstå flere muligheter en overføring kan skje på. Overføringen vil derfor i større grad være knyttet til hvor behandlingen finner sted, og ikke hvor opplysningene rent fysisk befinner seg.

Den vanligste oppfatningen av en overføring er at opplysninger passerer fra en behandlingsansvarlig i ett land til en ny behandlingsansvarlig i ett annet. Dette kan skje mellom to naboland eller gjennom transittland til land som ikke deler felles grense. Se Figur 1.

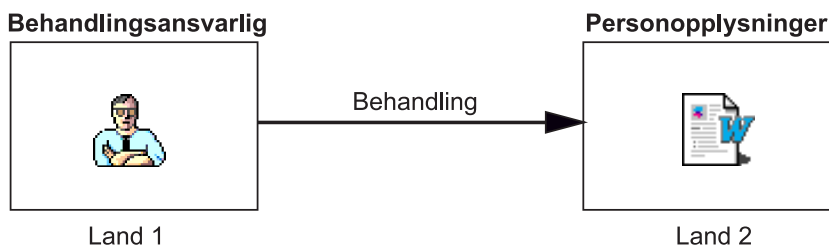


Figur 1

Ved manuell overlevering over en felles grense vil det oppstå få problemer. Skjer derimot overføringen elektronisk er det fullt mulig at informasjonen pas-

serer transittland på vei til mottakerlandet selv om de er naboland, og da må man se om kravet til tilstrekkelig beskyttelse også gjelder for disse landene. I tilfeller der kommunikasjonskanalene selv velger ruten for overføring er det en faktor som avsender av personopplysningene ikke kan kontrollere. For eksempel vil elektronisk overføring gjennom telenett kunne innebære transport via satellitt eller telelinjer som befinner seg utenlands. Det vil vanskeliggjøre kommunikasjon dersom man ved enhver bruk av elektroniske kommunikasjonsmidler må ta høyde for at overføringen til nabokontoret kan skje via utlandet. Dette står i kontrast til direktivets formål som er å lette informasjonsflyten,⁴⁰ og det taler for at tilstrekkelighetsvurderingen ikke gjelder for rene transittland. Et annet moment er at man på forhånd ikke vet hvilke land informasjonen vil bli sendt gjennom, og man kan derfor ikke foreta noen konkret vurdering av transittlandets personvernbeskyttelse.

En annen måte overføring kan skje på er når behandlingsansvarlig befinner seg i ett land mens opplysningene er i ett annet land. Se Figur 2.



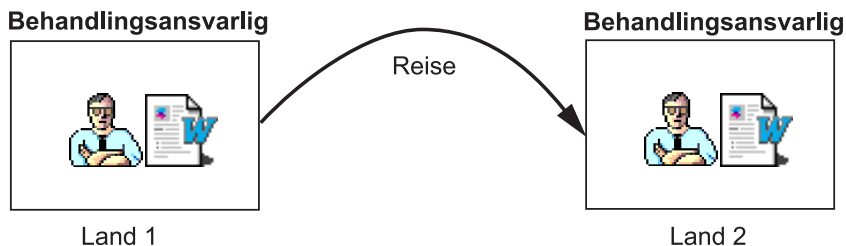
Figur 2

Dette vil være tilfellet der man har en sentral database i et land, som andre kan nå via sitt datanettverk.⁴¹ Her forblir både behandlingsansvarlig og opplysningene værende på hvert sitt sted. Ingen utveksling av data finner sted, og det er eventuelt bare resultatet av behandlingen som kommer behandlingsansvarlig i hende. Likevel må man betrakte dette som en overføring fordi det skjer en behandling av opplysningene. EU-direktivet art. 25 gjelder nemlig der personopplysninger *gøres til genstand for behandling*.

Overføring kan også skje der hvor behandlingsansvarlig har opplysningene i sin besittelse, og tar med seg opplysningene når han flytter seg. Se Figur 3.

⁴⁰ EU-direktivets fortløpende punkt 3

⁴¹ Et eksempel på dette er reservasjon av en flyreise. Alle slike reservasjoner registreres i reservasjonssystemet AMADEUS som er en sentral database lokalisert i Tyskland. Tilgang til denne skjer gjennom terminaler fra flyselskaper og reisbyråer over hele verden.



Figur 3

Dette kan være aktuelt der en person tar med seg sin bærbare datamaskin inneholdende en kundedatabase på en utenlandsreise. Informasjonen flyttes fysisk til utlandet, men det skjer ingen overføring som reguleres av direktivet så lenge den er i behandlingsansvarlig besittelse og ikke overlates til andre. Det kan allikevel være snakk om en overføring dersom han foretar en behandling av opplysningene mens han er på reisen, fordi direktivet art. 25 knytter overføring til om det skjer en behandling i tredjelandet. Flyttes det fysiske lagringsmediet ut av landet for at behandling av personopplysningene skal foretas der, innebærer selve flyttingen en overføring. Dette er et viktig element for å unngå at behandlingsansvarlig tar med seg opplysninger for behandling i personvernparadis eller *data havens* – land med svakere personvern håndhevelse enn opprinnelseslandet. Her vil altså den reelle situasjonen bestemme hvorvidt en overføring har skjedd eller ikke.

Utgangspunktet for hva som er en overføring var at det skjer en overlevering. I de tilfeller hvor personopplysningene ikke kommer frem til mottaker, kan man etter denne forståelsen ikke snakke om at overføringen er fullført. Som vi har sett ovenfor må imidlertid overføring tolkes mye videre. Muligens bør fokus ikke være på hvorvidt informasjonen er kommet andre i hende, men om behandlingsansvarlig har gitt den fra seg. Overføring til utlandet vil da skje i det opplysningene forlater behandlingsansvarligs kontroll med den hensikt at de skal behandles i et tredjeland. Dette skillet har ikke så stor praktisk betydning fordi vurderingen av om overføring kan skje uansett må skje i forkant.

Et annet spørsmål er om det skal anses som en overføring dersom mottaker ikke kan nyttiggjøre seg av opplysningene. Dette er aktuelt dersom personopplysningene er kryptert eller på annen måte sikret overfor utenforstående. I en tenkt situasjon har en bedrift kapasitetsproblemer, og har funnet det økonomisk gunstig å lagre større mengder persondata utenlands. Den reelle situasjonen er da at opplysningene er overført. Personopplysningene vil imidlertid ikke ha noen funksjon for andre enn de som er utstyrt med krypteringsnøkkelen. Under slike omstendigheter kan det være nærliggende å tolke

idéen om besittelse utvidende. Opplysningene vil i såfall være i den behandlingsansvarliges besittelse så lenge han har kontroll over dem, og en overføring har dermed ikke skjedd. Det kan imidlertid oppstå et problem dersom bedriften velger å fjernbehandle opplysningene, men med bruk av krypteringsrutiner slik at sikkerheten fortsatt er i varetatt overfor andre. Aksepterer man denne løsningen kan kravene til overføring fort uthules. Dersom man ikke klassifiserer transporten som en overføring, vil det heller ikke være noen muligheter for å kontrollere virksomheten. Det er jo bare ved overføring at melding skal sendes etter direktivet art. 18. Dermed er det vanskelig å kontrollere at sikkerhetstiltakene faktisk er gode nok. I en slik situasjon vil det være mer nærliggende å benytte seg av unntaket i direktivet art. 26 nr. 2, hvor overføring kan tillates selv om kravene i direktivet art. 25 ikke er oppfylt, dersom den behandlingsansvarlige sikrer tilstrekkelige garantier for at opplysningene beskyttes.

3.1.2 Overføring via Internett

Bruk av moderne kommunikasjonskanaler som Internett reiser spørsmål i forhold til overføring. Internett er kort fortalt en infrastruktur for datamaskiner som i utgangspunktet enhver kan benytte seg av. Nettet er globalt og består av en mengde lokale nett som er koblet sammen, herav navnet. Gjennom dette nettet er det opprettet en del tjenester for distribusjon av informasjon. De mest kjente er elektronisk post (e-post) og World Wide Web (WWW). E-post blir hovedsakelig brukt til å sende meldinger til bestemte adressater, mens WWW blir brukt til publisering av informasjon. Disse tjenestene muliggjør overføring av enhver type elektronisk informasjon. For å sørge for best mulig ytelse blir informasjonen splittet i pakker med unike adresser. Disse pakkene tar den mest effektive ruten frem til mottaker hvor de blir satt sammen igjen til det originale budskapet. Dermed kan pakkene godt ta forskjellige veier gjennom nettet og således være innom forskjellige land før de når mottaker.

Personopplysninger kan lett overføres via e-post, enten i meldingen selv eller som vedlegg. En e-post melding er i prinsippet lik en skriftlig melding i funksjon, det er bare formen som skiller. Således bør bruk av e-post likestilles med bruk av andre mer tradisjonelle kommunikasjonskanaler, og reguleres deretter.⁴² Dersom man overfører personopplysninger til utlandet ved hjelp av e-post, vil dette falle inn under direktivet art. 25. For personopplysninger publisert på World Wide Web via såkalte hjemmesider oppstår det problemet at informasjonen gjøres tilgjengelig for alle brukere av nettet. Slik sett vil

⁴² NOU 1997:19 *Et bedre personvern* s. 102

enhver aksessering av sidene innebære en fysisk overføring. Det er imidlertid ikke gitt at de publiserte opplysningene gjøres til gjenstand for videre behandling. Her må imidlertid behandlingsbegrepet gis en videre betydning enn etter vanlig språkbruk. Ifølge direktivet art. 2 litra b innebærer behandling *enhver operation[...] som personopplysninger gjøres til gjenstand for*. Dette vil inkludere oppbevaring, søking og bruk. At en hjemmeside trolig vil få lite besøk, er ikke noe argument for at publisering på denne ikke skal ses på som overføring. Ved tilgjengeliggjøring er det derfor stor sannsynlighet at overføring vil skje. Personopplysningslovutvalget har da også gått inn for at publisering på Internett er å anse som overføring av personopplysninger til utlandet.⁴³ Hjemmesider for rent personlig formål vil ikke omfattes av direktivet selv om de skulle inneholde personopplysninger, da direktivet art. 3 nr. 2 annet strekpunkt gjør unntak for slik behandling. Hva som er *personlige formål* kan være vanskelig å avgjøre, og vi vil her bare komme inn på hovedtrekkene. Som hovedregel kan man si at sider med informasjon om vedkommende selv og dennes familie vil være til personlige formål. Har en derimot idrettsklubbens sider liggende på ens eget hjemmeområde vil dette ikke være rent personlig formål. At selve hjemmesiden tilhører en privatperson er ikke tilstrekkelig for at bruken skal være personlig, og dermed unntatt direktivets bestemmelser.

3.1.3 EU-direktivets geografiske virkeområde

Tar man med sin bærbar datamaskin til Japan og behandler opplysninger på reisen, vil overføringen – dvs. den fysiske transporten av maskinen – reguleres av EU-direktivet art. 25, som nevnt i punkt 3.1.1. Men vil selve behandlingen kunne reguleres av EU-direktivet? Utgangspunktet er at det implementerte direktivet skal omfatte aktiviteter innenfor medlemsstatens område, jf direktivet art. 4 nr. 1 litra a. Det betyr at direktivet vil gjelde for et firma som er etablert i Sverige, men som samler inn opplysninger i Frankrike. Er et firma registrert i Sverige og har kontorer også i Spania og Frankrike, betyr ikke det at svensk lov vil gjelde for alle kontorene. Ved å ha kontorer i de andre landene, vil firmaet regnes som *etablert* også der og må overholde de respektive lands regler. *Etablert* vil da innebære at man fysisk holder til i landet. I situasjonen hvor opplysninger samles inn i Sverige, kan det være vanskelig for de registrerte å hevde sine rettigheter fordi firmaet forholder seg til svensk lov. For de land direktivet gjelder vil det være slik at den nasjonale tilsynsmyndighets kompetanse vil være uavhengig av hvilken jurisdiksjon behandlingsansvarlig faller under. Tilsynsmyndigheten kan gripe inn i alle behandlinger

⁴³ NOU 1997:19 *Et bedre personvern* s. 102

som foretas på territoriet. Det betyr at et firma etablert i Sverige som behandler informasjon i Frankrike vil følge svensk lov, men franske tilsynsmyndigheter har kompetanse til å gripe inn i behandlingen, jf direktivet art 28 nr.6 *Den enkelte tilsynsmyndighet er, uansett hvilken national lov der måtte gælde for den pågældende behandling, kompetent til på sin medlemsstats område at udøve de beføjelser, der tillægges den [...]*. Det innebærer at personer som blir registrert i Frankrike av det svenske firmaet, kan hevde sine rettigheter gjennom den nasjonale tilsynsmyndighet *Commission Nationale de l'Informatique et des Libertés* (CNIL). Tilsynsmyndighetene i de forskjellige landene skal også samarbeide, jf direktivet art. 28 nr. 6, og CNIL kan anmode Datatilspektionen i Sverige om å gripe inn i en behandling av opplysninger om personer bosatt i Frankrike som foretas i Sverige.

Direktivet vil også omfatte behandlingsansvarlige som befinner seg utenfor medlemsstaten, men hvor nasjonal lov gjelder i henhold til folkeretten, jf direktivet art. 4 nr. 1 litra b. Dette gjelder primært medlemsstatenes ambassader. Omfattet er også behandler som befinner seg utenfor EU, men som benytter hjelpemidler som befinner seg på medlemsstatens område, jf direktivet art. 4 nr. 1 litra c. Denne regelen skal sikre at direktivets regler ikke omgås ved at behandlingsansvarlig etablerer seg utenfor EU. Er man etablert i Japan og behandler opplysninger på en datamaskin i Italia via nettverk, vil denne behandlingen falle under direktivets virkeområde. Overføres opplysninger fra Japan til USA via EU, vil dette kun være transitt og ikke være bruk av hjelpemidler innen EU som omfattes av direktivet, jf direktivet art. 4 nr. 1 litra c. Det forutsettes at opplysningene kun sendes gjennom og det ikke foretas noen behandling. *Transitt* impliserer at det heller ikke foretas lagring eller sikkerhetskopiering.

3.1.4 Datatilsynets jurisdiksjon

Hvorvidt vil Datatilsynet ha kompetanse etter personopplysningsloven til å gripe inne i behandling som ikke faller under lovens geografiske virkeområde? Personopplysningsloven har ingen bestemmelse tilsvarende direktivet art. 28 nr. 6 om at tilsynsmyndighetens kompetanse er uinnskrenket på nasjonalt territorium. Datatilsynets oppgaver knytter seg primært til om loven overholdes, jf *kontrollere at lover*, jf personopplysningsloven § 42 tredje ledd nr. 3 og *i sin kontroll med at lovens regler etterleves*, jf personopplysningsloven § 44 annet ledd 1. punkt. Loven gjelder kun for behandlingsansvarlig som er etablert i Norge, jf personopplysningsloven § 4 første ledd 1. punkt. Etter lovens ord kan dermed Datatilsynet bare gripe inn overfor behandling som faller under lovens virkeområde, og ikke alle behandlingene som foretas på norsk territorium. I følge forarbeidene vil Datatilsynet ha

tilsynskompetanse i forhold til opplysninger som oppbevares i Norge for en behandlingsansvarlig etablert utenfor landet. Tilsynet må da baseres på lovgivningen i det landet hvor den ansvarlige er etablert.⁴⁴ Dette er ikke nærmere forklart eller drøftet i forarbeidene, men fremkommer kun som en kommentar til personopplysningsloven § 4. Datatilsynets kompetanse bør ikke baseres på en bemerkning i forarbeidene alene. Kjenner man ikke direktivet er det heller ikke opplagt at man vil komme til det resultat ved en tolking av personopplysningsloven. En slik bestemmelse er av såpass betydning at den bør fremkomme av lovens ordlyd.

Hvilken situasjon har man når behandlingsansvarlig er etablert i Sverige, men samler inn informasjon i Norge? Etter personopplysningsloven § 4 annet ledd 1. punkt gjelder også loven der hvor hjelpemidler i Norge benyttes til behandlingen. Dette kan være tilfelle dersom det svenske firmaet henter informasjon fra en database i Norge. Formelt gjelder bestemmelsen der hvor behandlingsansvarlig befinner seg utenfor EØS-området. I dette tilfellet er virksomheten etablert utenfor Norge, men innenfor EØS. Etter ordlyden reguleres ikke slik virksomhet av loven. Man har da en situasjon hvor behandlingen ikke kan reguleres av norsk lov fordi behandlingsansvarlig faller utenfor lovens geografiske virkeområde etter personopplysningsloven § 4, og Datatilsynet kan ikke gripe inn i behandlingen fordi deres kompetanse er begrenset til lovens virkeområde. En slik løsning vil innebære et smutthull i lovgivningen. På den annen side vil behandlingsansvarlige etablert innenfor EØS reguleres av sin nasjonale lovgivning basert på EU-direktivet, slik at det ikke vil representere noen særlig fare for personvernet. Derimot kan det være vanskelig for de registrerte personer å benytte sine rettigheter som innsyn og retting. Forarbeidene nevner ikke hvorvidt EØS-området omfattes av loven. Det blir bare nevnt at loven vil omfatte behandling foretatt av et datterselskap eller filial av en behandlingsansvarlig med hovedsete i annet EØS-land.⁴⁵ Dette vil være en følge av at datterselskapet eller filialen regnes som en etablering, og ikke av at moderselskapet befinner seg i EØS. I lys av lovens formål og helhetlige karakter, er det mest hensiktsmessig at personopplysningsloven § 4 annet ledd også omfatter EØS-statene.

På den annen side kan man ha en situasjon hvor et firma etablert i Sverige samler inn informasjon via telefon fra personer bosatt i Norge. Svensk lov vil gjelde for behandlingen, men vil norsk lov også kunne gjelde? Spørsmålet vil være hvorvidt innsamlingen foretas ved bruk av hjelpemidler i Norge. Ved muntlig innsamling via telefon, er da registrertes telefonapparat et slikt hjel-

⁴⁴ Ot. prp. nr. 92 (1998-99) om lov om behandling av personopplysninger s. 105

⁴⁵ Ot. prp. nr. 92 (1998-99) om lov om behandling av personopplysninger s. 29

pemiddel? Eller telefonlinjene? I forarbeidene er det nevnt at telenett vil være omfattet av begrepet *hjelpemidler*, og tilfellet over vil muligens omfattes av loven. Lovens løsning innebærer at skillet mellom hvem som omfattes av loven og ikke, blir viktig for omfanget av Datatilsynets kontroll. Dersom Datatilsynet ikke kan gripe inn overfor behandling i Norge som faller utenfor loven, vil det medføre en fordelaktig situasjon for disse behandlere. Det vil også skape mindre forutberegnelighet for den registrerte, som vil oppleve at Datatilsynet ikke kan hjelpe i alle tilfeller. Disse hensynene samt hensynet til en retts teknisk enkel regel, tilsier at Datatilsynet kompetanse bør gjelde for all behandling som foretas på norsk område uavhengig av om den omfattes av personopplysningsloven. Slik kompetanse bør fremkomme av lovteksten.

3.2 Tredjeland

EU-direktivet art. 25 regulerer overføring til *tredjeland*. Med dette får man et skille mellom hvilke regler som gjelder for de land som omfattes av definisjonen og de som faller utenfor. For alle land som defineres som tredjeland, må det foretas en vurdering av personvernbeskyttelsen ved overføring. Land som ikke anses som tredjeland må derimot ikke vurderes, da det presumeres at disse har tilstrekkelig beskyttelse.

3.2.1 EU-landene

Med tredjeland menes land utenfor EU. For overføringer av personopplysninger mellom EU-land har man ingen restriksjoner i direktivet, og direktivet art. 25 kommer ikke til anvendelse. Begrunnelsen er at direktivet skal sørge for fri flyt av personopplysninger innad i EU, og medlemslandene skal ikke hindre slik overføring til hverandre, jf direktivet art. 1 nr. 2 *Medlemsstatene må ikke [...] innskrenke eller forbyde fri udveksling af personopplysninger mellom medlemsstatene*. En forutsetning for at man skal ha fri flyt av varer, tjenester, kapital og personer er at personopplysninger fritt kan utveksles, jf direktivets forale punkt 3. Selv om fristen for implementering i nasjonal lov var i oktober 1998 har kun seks av femten medlemsland gjennomført denne per mai 1999.⁴⁶ Vil disse landene regnes som tredjeland? Di-

⁴⁶ De land som har gjennomført direktivet er Belgia, Finland, Hellas, Italia, Portugal og Sverige.

Status of implementation of Directive 95/46. Director General XV, EU kommisjonen, Brussel 12. mai 1999. <http://europa.eu.int/comm/dg15/en/media/dataprot/law/impl.htm> (8. september 1999)

rektivet retter seg mot alle medlemsstatene, og det ville være lite naturlig å anse land innenfor Unionen som tredjeland. Når man har valgt direktivformen for rettsakten innebærer dette at det er opp til nasjonale myndigheter å bestemme formen og midlene for gjennomføring av implementeringen, jf Romatraktaten art. 249 tredje ledd. Personvernreguleringen kan derfor variere fra land til land, men til tross for forskjeller skal det være fri flyt av personopplysninger. Skulle land innenfor EU mene at et annet medlem har utilstrekkelig beskyttelse av personopplysninger, kan overføring derfor ikke hindres med hjemmel i direktivet art. 25. Det vil i stedet være opp til Arbeidsgruppen nedsatt med hjemmel i direktivet art. 29 å underrette Kommisjonen om forskjeller i medlemsstatenes lovgivning eller praksis som kan medføre en fare for den ensartede beskyttelse av personvern innenfor EU, jf direktivet art. 30 nr. 2.

3.2.2 EFTA-landene

Er EFTA-landene tredjeland? Etter EØS-avtalen skal rettsakter som vedtas etter at avtalen som trådte i kraft 1. januar 1994 vurderes individuelt i EØS-komiteén før de kan inkluderes i avtalen.⁴⁷ 25. juni 1999 besluttet EØS-komiteén å innlemme EU-direktivet i EØS-avtalen, og vedtagelse det medfører at Norge er folkerettslig forpliktet til å gjennomføre implementering av direktivet.⁴⁸ Når man er forpliktet på den måte vil det være naturlig å regne Norge og de andre EFTA-landene blant de landene som direktivet retter seg mot, slik at de ikke anses som tredjeland. Eventuell utilstrekkelig personvernpraksis må dermed behandles på andre måter enn ved nektelse av overføring etter direktivet art. 25 av personopplysninger fra EU-landene. Hadde derimot direktivet ikke blitt innlemmet i EØS-avtalen, vil Norge vært *tredjeland* etter direktivet art. 25 og vurdering av personvernbeskyttelsen måtte foretas.

3.2.3 Kan land utenfor EØS tiltre direktivet?

Kan så andre land tiltre direktivet? Det er ikke sagt uttrykkelig i direktivet om tredjeland kan eller ikke kan tiltre. art. 34 sier at direktivet er rettet til medlemsstatene. Dette utelukker i seg selv ikke andre land, men betyr at kun medlemsstatene blir direkte bundet av direktivet. EUs helhetlige natur tilsier at andre stater ikke kan tiltre enkelte rettsakter, men må bli med i Unionen og dermed bli bundet av alle EUs bestemmelser. Dette utelukker at andre

⁴⁷ Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. av 27.november 1992 nr. 109 (EØS-loven) art. 102

⁴⁸ Arnesen, Finn; Borgli, Anneke B.; Bull, Henrik; Foyn, Stein; Rognstad; Ole-Andreas og Stemshaug; Helge *Oversikt over EØS-retten*, (1. utgave) Universitetet i Oslo, Oslo 1994:54

land kan tiltre personverndirektivet for å ikke regnes som tredjeland. På den annen side er det ikke noe i veien for at andre stater kan bygge sin personvernlovgivning på direktivet, og på den måten implementere det. Skulle noen land gjøre dette vil de allikevel regnes som tredjeland, da man må foreta en vurdering av gjennomføringen av lovgivningen og hvordan den praktiseres.

3.2.4 Uttrykket *stater* i personopplysningsloven § 29

I forslag til personopplysningslov § 29 første ledd 2. pkt bruker man ikke uttrykket *tredjeland*, men snakker om overføring til *stater*. Dette innebærer at ingen land er unntatt kravet om *forsvarlig behandling*, i motsetning til direktivet hvor alle EØS-land er unntatt slik vurdering.⁴⁹ Det er imidlertid presisert at stater som har *gjennomført* EU-direktivet oppfyller dette kravet. At statene må ha *gjennomført* direktivet tilsier at de land som ennå ikke har fullført implementeringen, ikke vil være blant de stater som er unntatt vurderingen etter § 29. Det er også sagt i NOU 1997:19 *Et bedre personvern*⁵⁰ at overføring til andre EØS-land kan nektes dersom landet ikke har gjennomført direktivet. Kan Norge nekte overføring på generelt grunnlag til en annen EØS-stat med denne begrunnelsen?

Fordi direktivet er innlemmet i EØS-avtalen, vil Norge være folkerettslig bundet av det. Personopplysningsloven vil dermed inngå i EØS-samarbeidet, og man må forholde seg til de kjøreregler som gjelder innenfor EØS. Norge vil da være mer bundet i sin praksis, og dette vil legge føringer på lovens selvstendighet. Et direktiv retter seg mot medlemsstatene, og før det er gjennomført i nasjonal rett vil derfor individer normalt ikke fremstå som rettighetssubjekter etter direktivet.⁵¹ Når fristen for implementering oversittes, har imidlertid Europadomstolen lagt til grunn at direktiver i visse tilfeller allikevel kan ha direkte virkning og dermed gjøre borgerne til rettighetssubjekter.⁵² Sett at det overføres personopplysninger fra Norge til et EØS-land som ikke har implementert direktivet, og opplysningene vedrører en person som er bosatt i mottakerlandet. Denne personen vil ha en mulighet til å reise sak for sin nasjonale domstol for å få anerkjent sine rettigheter etter direktivet,⁵³ med den følge at informasjonen som er overført behandles tilfredsstillende. Over-

⁴⁹ EØS-landene består av EU- og EFTA-landene

⁵⁰ NOU 1997:19 *Et bedre personvern* s. 100

⁵¹ Arnesen, Finn; Borgli, Anneke B.; Bull, Henrik; Foyn, Stein; Rognstad; Ole-Andreas og Stemshaug; Helge *Oversikt over EØS-retten*, (1. utgave) Universitetet i Oslo, Oslo 1994:96

⁵² Kapteyn, P. J. G. og Verloren van Themaat, P. *Introduction to the law of the European Communities – After the coming into force of the Single European act*, (2. utgave) Kluwer law and taxation publishers, Deventer 1989:345

⁵³ Følger av *Marleasing saken*, C-106/89, 13. november 1990

føres derimot opplysninger om en norsk borger, vil denne personen ikke ha mulighet til å reise sak mot mottakerlandet på det grunnlag at direktivet ikke er implementert. Grunnen til dette er at den manglende implementeringen ikke har direkte virkning for denne personen, slik den vil ha for en borger i den aktuelle staten. På grunnlag av dette er det mindre betenkelig å tillate overføring til ikke-implementerende stater dersom opplysningene vedrører borgere i mottakerstaten, enn å overføre informasjon om norske borgere. En slik regel vil imidlertid være lite praktisk. Man må derfor enten tillate eller nekte overføring til landene som ikke har implementert direktivet.

Direktivet selv sier ingenting om hva som skjer dersom medlemsstater ikke implementerer direktivet i tide. Etter EU-direktivet art. 1 nr. 2 må ikke medlemsstatene innskrenke eller forby fri utveksling av personopplysninger mellom seg *af grunde, der har forbindelse med den i stk. 1 foreskrevne beskyttelse*. Det betyr at overføring ikke kan nektes med begrunnelse i personvern. Nekter man overføring fordi implementering ikke har skjedd vil dette være begrunnet i personvern hensyn, og utgangspunktet er at dette ikke kan gjøres. På den annen side sier direktivet art. 1 nr. 1 at medlemsstatene skal sikre slikt personvern *i overensstemmelse med dette direktiv*. Dette taler for at direktivet art. 1 nr. 2 kun gjelder overfor stater som har gjennomført direktivet. Samtidig binder direktivet alle medlemsstatene uavhengig av implementeringen. Overholder en stat ikke fristen for implementering er dette ikke et brudd på direktivet, men på Romatraktaten art. 10: *Medlemsstatene skal treffe alle generelle eller særlige tiltak som er egnet til å oppfylle en forpliktelse som følger av denne traktat eller av rettsakter vedtatt av Fellesskapets organer*.⁵⁴ Etter Romatraktaten art. 227 kan enhver medlemsstat som mener at et annet medlem har unnlatt å oppfylle sine forpliktelser etter traktaten, bringe saken inn for Europadomstolen. Det er da domstolen som avgjør hvilke tiltak som skal treffes, jf Romatraktaten art. 228. Dette taler for at man med hjemmel i forslag til personopplysningslov § 29 ikke kan nekte overføring til andre EØS-land til tross for at de ikke har gjennomført direktivet. En slik konflikt må i såfall løses av Fellesskapets organer. Dette støttes også av at Kommisjonen i henhold til Romatraktaten art. 226 29. juli 1999 avga en grunnlagt uttalelse til Danmark, Frankrike, Irland, Luxemburg, Nederland, Spania, Storbritannia, Tyskland og Østerrike fordi de ikke har gjennomført implementeringen. Får

⁵⁴ Arnesen, Finn; Borgli, Anneke B.; Bull, Henrik; Foyn, Stein; Rognstad; Ole-Andreas og Stemshaug; Helge *Oversikt over EØS-retten*, (1. utgave) Universitetet i Oslo, Oslo 1994:96

den ikke tilfredsstillende svar innen to måneder på hvorfor dette ikke er gjort, kan Kommisjonen bringe saken inn for Europadomstolen.⁵⁵

Det må presiseres at dette gjelder hvor Norge skulle nekte overføring på generelt grunnlag til en annen EØS-stat. Norge kan allikevel nekte overføringer til andre EØS-land, men da kun i konkrete saker. Begrunnelsen for nektelsen kan ikke være at mottakerlandet ikke har gjennomført direktivet, men at behandlingen ikke ville være tillatt i Norge, for eksempel på grunn av manglende datasikkerhet eller innsynsmuligheter. Det viktige ved en slik begrensing av overføring til EØS-land er at reglene ikke praktiseres diskriminerende til fordel for nasjonale behandlingsansvarlige, jf EØS-avtalen art. 4 *Enhver forskjellsbehandling på grunnlag av nasjonalitet skal være forbudt innenfor denne avtales virkeområde.*

Hvilken situasjon får man dersom Norge allikevel skulle nekte overføring til EØS-land på grunn av manglende implementering? Etter EØS-avtalen art. 3 skal avtalepartene treffe alle generelle eller særlige tiltak som er egnet til å oppfylle de forpliktelser som følger av avtalen. Rettsakter som er omhandlet i eller inntatt i vedlegg til avtalen eller i EØS-komiteens vedtak, skal være bindende for avtalepartene, jf EØS-avtalen art. 7. Dette vil omfatte EU-direktivet om personvern siden det er innlemmet i EØS-avtalen, og etter direktivet kan ikke Norge hindre overføring av personopplysninger til andre EØS-land. Slik hindring kan innebære at Norge gjør seg skyldig i brudd på EØS-avtalen. *Avtale mellom EFTA-statene om opprettelse av et Overvåkingsorgan og en Domstol* (ODA-avtalen) art.5 nr. 1 litra a sier at EFTAs overvåkingsorgan skal sikre at EFTA-statene oppfyller sine forpliktelser etter EØS-avtalen. Finner overvåkingsorganet at en EFTA-stat har unnlatt å oppfylle en av sine forpliktelser, skal den avgi en uttalelse om dette, jf ODA-avtalen art. 31 første ledd. Retter vedkommende stat seg ikke etter uttalelsen, kan overvåkingsorganet bringe saken inn for EFTA-domstolen, jf ODA-avtalen art. 31 annet ledd.

⁵⁵ Data protection: Commission decides to send reasoned opinions to nine Member States, IP/99/592 Brussel 29. juli 1999
<http://europa.eu.int/comm/dg15/en/media/dataprot/news/99-592.htm> (8. september 1999)

4. KRAVET TIL TILSTREKKELIG BESKYTTELSE

Hvorvidt personopplysninger kan overføres til tredjeland beror etter EU-direktivet art. 25 på om mottakerlandet innehar et *tilstrekkelig beskyttelsesnivå* for behandling av personopplysninger. I dette kapittelet kommer vi til å se på hva som ligger i dette begrepet. Først kommer vil til å gi en oversikt over japansk personvernrett fordi vi kommer til å bruke det som eksempel-materiale. Så vil vi se på innholdet av begrepet, nemlig hva kravet til tilstrekkelighet innebærer, og deretter hvilke betraktninger som skal legges til grunn i vurderingen av tilstrekkelighetsnivået. Her vil vi både være innom de materielle reglene og prosedyrer for håndhevelse. Til slutt vil vi se på hvem som skal foreta vurderingen og hvilken kompetanse disse har. Vi har valgt å se på denne problemstillingen til slutt, fordi drøftelsen forut for dette punktet vil bidra til å forstå problemstillingene bedre.

4.1 Oversikt over japansk personvernrett⁵⁶

Den japanske retten er basert på en resepsjon av tysk og fransk rett, og har således en kontinentaleuropeisk rettstradisjon som legger til rette for studier og sammenligninger mellom japansk og europeisk rett. Nedenfor vil vi gå gjennom de japanske rettskildene som er aktuelle i drøftelsen av personvernsspørsmål.

4.1.1 Grunnloven

Utgangspunktet for personvern i Japan er Grunnloven av 3. november 1946 art. 13:

All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not inter-

⁵⁶ For mer utfyllende informasjon om japansk rett se for eksempel: Noda, Yosiyuki *Introduction au droit japonais*, Librairie Dalloz, Paris 1966, Noda, Yosiyuki *Introduction to Japanese law*, University of Tokyo Press, Tokyo 1976. Oversettelse og bearbeidelse av førstnevnte bok tilpasset lesere med common law bakgrunn, mens originalen har referansepunkt i fransk rett, Oda, Hiroshi *Japanese law*, Butterworth & Co, London 1992

ferre with the public welfare, be the supreme consideration in legislation and governmental affairs.

Denne passusen beskytter i større grad privatlivets fred enn personopplysninger, og det er i betydningen vern av privatlivets fred man først og fremst har benyttet begrepet personvern i Japan. Rettslig tilhører personvernretten den konstitusjonelle rett. Man bruker ikke et eget japansk ord for personvern, men benytter puraibashi som er avledet fra engelske privacy.

4.1.2 Nasjonal lovgivning

Det finnes én formell lov som regulerer beskyttelse av personopplysninger i Japan: *Act for the protection of computer processed personal data held by administrative organs* av 10. oktober 1989⁵⁷ – heretter personvernloven. Denne loven ble gitt som et resultat av at Japan vedtok OECDs retningslinjer for beskyttelse av personlige data. Loven tar hensyn til de prinsippene som ligger til grunn for retningslinjene, men mangler – som retningslinjene – bestemmelser om sanksjoner. Loven gjelder for offentlig sektor, og utenfor lovens virkeområde faller behandling av personopplysninger utført av statlig eide bedrifter, privat sektor, manuell behandling og behandling for statistisk bruk. Sistnevnte reguleres dog av egne lover.⁵⁸

Loven omfatter bare offentlig sektor på nasjonalt nivå, jf art 2 første ledd, og gjelder altså ikke for lokale myndigheter på fylkes- og kommunenivå.⁵⁹ Dette gir loven begrenset virkning da større mengder persondata holdes på kommunalt nivå enn riksnivå. Lokale myndigheter er derimot oppfordret til å ta hensyn til loven gjennom personvernloven art. 26. Det har vært diskusjon om å få en lov som også gjelder innen privat sektor. Motstanden er imidlertid stor hos både næringsliv og myndighetene. Begge parter ser en regulering av personvern som et hinder for teknologisk utvikling og ytringsfrihet. De siste årene har regjeringen satset på deregulering av næringslivet, og man er derfor generelt skeptisk til å regulere det ved lovgivning.⁶⁰

⁵⁷ Loven har utstrakt forskriftshjemler hvor primært *Cabinet orders* blir benyttet for å gi nærmere regler.

Det er regjeringen som står bak *Cabinet orders*.

⁵⁸ Statistics law, lov nr. 18 1947 og Statistical reports coordination law, lov nr. 148 1952

⁵⁹ Dette er et utslag av det svært vide lokale selvstyret, se nærmere punkt 4.1.3 om lokal lovgivning.

⁶⁰ Ifølge samtale med professor Masao Horibe 16. januar 1999.

Dette standpunktet kommer til uttrykk fra offisielt hold gjennom Australia-Japan joint statement on Electronic commerce 6. juli 1999:

Governments should create a favourable environment which maximises private sector initiatives and fosters open competition in electronic commerce. They should avoid the im-

Det finnes også andre regler i lovs form som gjelder beskyttelse av personopplysninger, men de er ikke samlet i én lov. Ved tolking av enkelte bestemmelser kan man derimot utlede et slikt vern på enkelte områder. I *lov om telekommunikasjon* art. 1 og 4⁶¹ er det regler om sikring av brukernes interesser og taushetsplikt. Denne regelen blir tolket slik at den kan anvendes for å beskytte personopplysninger fra å bli videredistribuert. Andre eksempler er *lov om pengeutlånning* art. 30⁶² som sier at personlige kredittdata ikke kan brukes til andre formål enn til å slå fast subjektets mulighet til å betale sin gjeld. En likelydende bestemmelse finnes også i *lov om kjøp på avbetaling* art. 42-4.⁶³ Fra lovgiver hold mener man at disse bestemmelser gir vern nok, og ser det som unødvendig med en felles lov.⁶⁴ Holdningen er også den at næringslivet selv må regulere sin aktivitet, da de kjenner sine behov best.⁶⁵

4.1.3 Lokal lovgivning

Japan har utstrakt lokal autonomi som er slått fast i Grunnloven art. 94, jf 92. Dette gjelder også lovgivningsmyndighet. Denne kompetansen gjelder innen den lokale myndighets geografiske område, men må være innenfor grensene satt av nasjonal lov.⁶⁶ Japansk Høyesterett har hatt flere saker til behandling hvor det har vært motstrid mellom nasjonal og lokal lovgivning. Det er nå slått fast at der hvor nasjonal lov skal innføre en felles standard for landet og loven dermed representerer en maksimumsgrense, kan man ikke på lokalt nivå regulere samme område strengere eller mildere. På den annen side kan lokal regulering være strengere der hvor den nasjonale lovgivning kun setter en minimumsstandard.⁶⁷ Et stadig debattert problem har vært regule-

sition of unnecessary regulations or restrictions on electronic commerce.

http://www.mofa.go.jp/policy/economy/e_commerce/statemt9907.html (19. juli 1999)

⁶¹ *Law on telecommunications business*, lov nr. 86 1984

http://www.mpt.go.jp/policyreports/english/laws/Tb_index.html (16. juli 1999)

⁶² *Law on the regulation of credit and loan business*, lov nr. 32 1983

⁶³ *Law on instalments sales*, lov nr. 159 1961

⁶⁴ Ifølge samtale med professor Masao Horibe 16. januar 1999

⁶⁵ «With regard to frameworks for personal data protection, governments and businesses should consider consumers' concern about their private information. Since content, usage, and the method for collection of private information differ from industry to industry, means for privacy protection should be considered by each industry. Enforcement mechanisms would be developed and implemented by the private sector, including preparing guidelines and developing verification and recourse methodologies, and supported by the public sector.» US-Japan joint statement on Electronic commerce 15. mai 1998.

http://www.mofa.go.jp/policy/economy/e_commerce/statemt9805.html (19. juli 1999)

⁶⁶ *Jf law on local self-administration*, lov nr. 67 1947 art. 14

⁶⁷ Oda, Hiroshi *Japanese law*, Butterworth & Co, Storbritannia 1993:59

ring der det ikke finnes nasjonal lovgivning som setter grenser. Utgangspunktet er at lokale myndigheters lovgivningskompetanse etter *law on local self-administration* art. 14 også gjelder i lovtomme rom. Skeptikere har uttrykt at lokale myndigheter ikke har kompetanse til å regulere privat sektor, da det er naturlig at slikt bare kan reguleres fra sentralt hold.⁶⁸

Lokal lovgivning er svært utbredt. Innenfor personvernretten har 1407 av i alt 3300 lokale myndigheter gitt regler på dette området, men bare 191 av disse har regler som dekker både offentlig og privat sektor.⁶⁹ En ulempe med disse reglene er at ingen ennå er oversatt. Siden reglene også bare gjelder innenfor et begrenset geografisk område vil det bli for snevert å behandle noen av disse. Vi vil derfor ikke ta for oss disse kildene.

4.1.4 Ulovfestet rett

Generelt er rettspraksis en relevant rettskilde i japansk rett, men tillegges ikke særlig vekt i enkeltsaker. Avgjørelser blir i større grad brukt til å trekke opp grenser i lovtomme rom. Innen personvernretten ble retten til privatlivets fred først anerkjent gjennom en dom fra 1964 *Utage no ato*,⁷⁰ Japans parallell til den norske dommen *To mistenkelige personer*.⁷¹ En tidligere diplomat saksøkte forfatteren Yukio Mishima fordi han mente at hans roman *Utage no ato* (*After the banquet*) blottla opplysninger om hans privatliv. Tokyo District Court anerkjente denne retten, og Mishima måtte betale den til da største erstatning for ikke-økonomisk tap. Til tross for at dommen er fra en lavere instans, har den hatt stor betydning for rettsoppfattningen på området. Det var første gang uttrykket personvern ble brukt i en domstol, og dommen slo også fast at et slikt vern kan utledes fra Grunnlovens art. 13.

4.1.5 Forarbeider

Forarbeider blir tillagt liten vekt som rettskilde i Japan. Den debatt som foregår i parlamentet anses hverken som bindende eller rettleidende. En av årsakene til dette er den bevisste tvetydighet i lovspråket, som vi kommer tilbake til i punkt 4.1.8.⁷²

⁶⁸ Ifølge samtale med professor Masao Horibe 16. og 19. januar 1999

⁶⁹ Horibe, Masao «The information society and privacy: Current state of personal data protection in Japan» *JIPDEC Informatization Quarterly: The information society and privacy* JIQ nr. 115/1998:5

⁷⁰ Tokyo District Court, 28. september 1964 (Kaminshu 15-9-2317: *Utage no Ato* case).

⁷¹ Rt 1952 s. 1217. Se punkt 2.1.

⁷² Kawashima, T «Japanese way of legal thinking» Dean, Meryll (red) *Japanese legal system: Text and materials*, Cavendish publishing limited, London 1997:165

4.1.6 Juridisk teori

Juridisk teori er ikke anerkjent som en rettskilde i japansk rettskildelære. Rettsvitenskapen anses likevel for å ha betydning ved at den påvirker rettsoppfatningen, og kan et være fundament for lovarbeid. Teori kan danne basis for retten, og i den forstand være en rettskilde. I norsk rettskildelære er dette argumenter for at juridisk teori er en rettskilde,⁷³ men det japanske rettskilderegrep er snevrere og mer formelt. Rettsvitenskapens rolle kan allikevel være av betydning fordi domstolene anerkjenner dens rolle i utviklingen av retten.⁷⁴

På personvernrettens område finnes det lite japansk juridisk teori. Dette rettsområdet er lite debattert i Japan, og det finnes lite tilgjengelig litteratur som dekker temaet. Noe av den manglende interessen kan nok tilskrives japanernes sterke kollektive oppfatning,⁷⁵ men personvern blir også oppfattet som en mulig begrensning av økonomisk vekst.⁷⁶

4.1.7 Offentlig rettledning

*Administrative guidance*⁷⁷ eller offentlig rettledning står for rundt 80 % av all byråkratisk aktivitet i Japan.⁷⁸ Dette er vedtak av forvaltningsmessig karakter, men anerkjennes ikke som noen rettskilde i juridisk forstand. Derimot er det en meget viktig reguleringsmetode. Det er en ikke-rettslig handling som formelt verken skaper rettigheter eller plikter. Det er en rettledning fra statens side, innenfor grenser satt av lovgivningen, som anmoder om en spesiell handling eller ikke-handling korresponderende med det mål forvaltningen har for øyet gjennom samarbeid med de berørte parter.⁷⁹ Den part man henvender seg til er i stor grad næringsdrivende. Målet er å oppnå en mer smidig og fleksibel forvaltning i stedet for å regulere ved hjelp av lov eller forskrift. Kort oppsummert har offentlig rettledning tre særtrekk: det er ingen rettslig hand-

⁷³ Eckhoff, Torstein *Rettskildelære*, (3. utgave) TANO, Oslo 1993:230-240

⁷⁴ Noda, Yosiyuki *Introduction au droit japonais*, Libraire Dalloz, Paris 1966:243

⁷⁵ Hiramatsu, Tsuyoshi «Telecommunication in Japan: Non-protection of privacy» *The international computer lawyer*, volume 1 nr. 3, februar 1993

⁷⁶ Uten navn «Rights to send and receive information freely to be recognizes as fundamental human rights» *Telecom tribune* volume 10 issue 12, februar 1996.
Publisert på <http://www.telecomtribune.com/1996issues/TT9602/TT11A.HTM> (23. august 1999)

⁷⁷ Gyosei shido på japansk

⁷⁸ Young, Michael K. «Administrative guidance in the courts: A case study in doctrinal adaptation» Fujikura, Koichiro (red.) *Japanese law and legal theory*, Dartmouth publishing company limited, Aldershot 1996:151

⁷⁹ Matsushita, M «International trade and competition law in Japan» Dean, Meryll (red) *Japanese legal system: Text and materials*, Cavendish publishing limited, London 1997:194-204

ling, målet er å endre adferd og etterlevelse er frivillig. Typen av disse rettledninger kan være fra det anmodende til det regulerende, og muntlig form benyttes like gjerne som skriftlig. Det at man ikke har noen fast form på utformingen, og at de kan være svært uformelle gjør det derfor vanskelig å betrakte som en relevant rettskilde. Tidligere har domstolene avvist ethvert krav søkt hjemlet i offentlig rettledning, men i nyere tid har man ved enkelte anledninger godtatt at krav kan oppstå dersom man for eksempel blir påført tap som resultat av slik rettledning. Dette gjelder særlig saker hvor man har å gjøre med vilkårlighet eller myndighetsmisbruk.⁸⁰

En av de formene den offentlige rettledning tar, er ved retningslinjer – *guidelines*. Det er denne formen man primært har valgt for å regulere personvern i privat sektor. En sentral retningslinje i forhold til personvern er *Guidelines concerning the protection of computer processed personal data in the private sector* utarbeidet av *Ministry of International Trade and Industry* (MITI) – heretter kalt MITI-retningslinjen.⁸¹ Denne retningslinjen er opprinnelig fra 1987, og er basert på prinsippene i OECDs retningslinjer om personvern. I 1997 reviderte man denne, primært for å tilpasse den EUs personverndirektiv. I ordbruk og utforming er den derfor meget lik direktivet. I seg selv regulerer ikke retningslinjen noen ting, men skal være en mal for utarbeidelse av bransjeregler på området. På den måten sikrer man at reglene blir tilpasset hver enkelt bransje og dennes behov. Det er derimot opp til den enkelte bransje om og når de vil utarbeide egne regler. Det kan være vanskelig å få fullstendig oversikt over de retningslinjer som er utarbeidet på grunnlag av denne fordi det ikke er noe krav om publisering. Til nå har man ret-

⁸⁰ Se f.eks. *Sawarabi Kabushiki Kaisha v. City of Kyoto*, Hanrei jiho (No. 691) 57 (Kyoto District Court, 14. juli 1972). I denne saken ønsket en person å sette opp en bensinstasjon på et område som var vernet på grunn av sin skjønnhet. Personen ble informert av planleggingskontoret i Kyoto at dersom en bensinstasjon skulle bygges måtte den følge strenge estetiske krav. Disse var så strenge at utbygging ville bli ulønnsom, og mannen solgte eienkomsten. Kjøperen bygget straks en bensinstasjon på området uten at det fikk noen konsekvenser for ham. Selgeren gikk da til sak, og hevdet han var urettferdig behandlet. Han fikk ikke erstatning, men retten mente at planleggingskontorets vedtak falt inn under artikkel 1 i *National compensation law* selv om det var fattet som offentlig rettledning. Fra Young, Michael K. «Administrative Guidance in the Courts: A Case Study in Doctrinal Adaptation» Fujikura, Koichiro (red.) *Japanese law and legal theory*, Dartmouth publishing company limited, Aldershot 1996:157

⁸¹ Ministry of International Trade and Industry, Notification nr. 98 av 4. mars 1997. Se for eksempel: <http://www.hni.uni-paderborn.de/cim/datenschutz/seiten/Japan2.html> (8. juli 1999)

ningslinjer for bl.a. elektronisk handel,⁸² informasjonstjenester,⁸³ administrering av elektroniske nettverk⁸⁴ og «cyber business»,⁸⁵ og i tillegg har *Ministry of Post and Telecommunication* (MPT) utarbeidet egne retningslinjer for telekommunikasjons bransjen.⁸⁶

4.1.8 Metodiske problemer ved bruken av japanske kilder

Ved bruk av de japanske kildene, støter man på flere metodeproblemer. Et problem er at vi ikke har kunnskap nok til å studere kildene på originalspråket. Vi har derfor måttet bruke oversettelser, men det er også en mangel på dokumenter som er oversatt. Et annet problem er at en del informasjon kan gå tapt ved oversettelse. Det japanske skriftspråk består av to alfabeter: hovedalfabetet *kanji* er ideografisk, hjelpealfabetene *katakana* og *hiragana* fonetiske. Et ideografisk skriftspråk øker muligheten for semantisk flertydighet, og fører til stort rom for tolking av lovtekster. At man bevisst har valgt å beholde denne flertydigheten, er et utslag av den japanske kulturen hvor tveetydighet og subtile vendinger blir verdsatt mer enn klare svar.⁸⁷ Det er dermed en fare for at enkelte ord og begreper innsnevres ved en oversettelse, slik at man ikke får med seg alle nyansene. Våre tolkinger vil være basert på de tilgjengelige oversettelsene, og i mangel av andre kilder er det lovteksten og juridisk teori som vil være våre primære rettskilder. Juridisk teori vil være en sentral kilde i arbeidet med å vurdere de japanske kilder ellers på grunn av mangel på primærkilder.

⁸² Electronic commerce promotion council *Guidelines concerning the protection of personal data in electronic commerce in the private sector*, Tokyo mars 1998
http://ecom.econ.or.jp/eng/output/wg12/privacy_guideline.htm (1. juni 1999)

⁸³ Japan information service industry association *Guidelines concerning the protection of computer processed personal data in the information service industry in Japan*, Tokyo 26. november 1997 <http://www.jisa.or.jp/statistics/JISAprivacyguideline-e.htm> (21. september 1998)

⁸⁴ Electronic network consortium *Guideline for protecting personal data in electronic network management*, Tokyo 3. desember 1997
<http://www.nmda.or.jp/enc/privacy-rev-english.html> (2. juni 1999)

⁸⁵ Cyber business association *Guidelines for protecting personal information in cyber business*, Tokyo 17. desember 1997
<http://www.iiinet.or.jp/fmmc/501e.html> (28. mai 1999)

⁸⁶ Ministry of Post and Telecommunications *Guidelines on the protection of personal data in telecommunications business*, Tokyo 2. desember 1998
http://www.mpt.go.jp/whatsnew/guideline_privacy-e.html (29. mai 1999)

⁸⁷ Kawashima, T «Japanese way of legal thinking» Dean, Meryll (red) *Japanese legal system: Text and materials*, Cavendish publishing limited, London 1997:163-165

Majoriteten av de personopplysninger som behandles skjer i privat sektor. Som nevnt regulerer ikke den japanske personvernloven slik behandling. Vi mener at eksemplene fra japansk rett vil bli snevre hvis vi kun skal konsentrere oss om offentlig sektor. Ulempen med denne tilnærmingen er at rettskildebildet blir mer uoversiktlig. Det eksisterer ingen formell lovgivning innen privat sektor, og vi må derfor se hen til retningslinjer gitt av departementene. Først og fremst må vi vurdere om disse retningslinjene overhodet er relevante for bruk i drøftelsen. Utgangspunktet er at retningslinjene ikke er noen rettskilde i tradisjonell forstand. Reglene er bransjespesifikke, og er således avhengige av at det utarbeides særlige regler for den enkelte sektor. På den annen side er retningslinjene utarbeidet av tunge fagdepartement som *Ministry of International Trade and Industry* og *Ministry of Post and Telecommunications*. Siden man ikke har valgt å benytte lovs form er dette den eneste formen for regulering som eksisterer på området. Samtidig bygger de på OECDs retningslinjer og EU-direktivet, slik at det ofte er de samme prinsippene som kommer til uttrykk i japansk så vel som i norsk og europeisk personvernrett. Det gir et incitament for å benytte reglene i diskusjonen. EU-direktivet art. 25 nr. 2 åpner i tillegg for at man ved vurderingen av et lands beskyttelsesnivå kan legge vekt på annet enn formell lov. Vi finner derfor at bruken av disse retningslinjene er relevante i drøftelsen av Japans beskyttelsesnivå for personopplysninger.

4.2 Vurderingen av tilstrekkelighetsnivået

Tilstrekkelig i EU-direktivet art. 25 nr. 1 gir lite informasjon om hvilke krav man skal stille til mottakerlandet. I direktivet art. 25 nr. 2 finner man en presisering av begrepet, og det gis hjelpemomenter for vurderingen. Overveielser skal være basert på en helhetsvurdering, jf *samtlige [...] forhold*, men direktivet art. 25 nr. 2 nevner at det blant annet skal legges vekt på opplysningens art, den planlagte behandlingens formål og varighet samt de rettsregler, regler for god forretningsskikk og sikkerhetstiltak som gjelder i vedkommende stat. Listen er ikke ment å være uttømmende, og det kan dermed være andre temaer som bør vektlegges i den enkelte sak.⁸⁸ Tilstrekkelighetsvurderingen skal baseres på alle forhold knyttet til overføringen. I forkant må forhold som formål med behandlingen, varigheten og typen av opplysning som behandles tas med i betraktningen. Dette er imidlertid forhold som uansett må vurderes i enhver behandlingssituasjon, jf direktivet art. 6 og 8. Det spesielle med vurderingen i forbindelse med en overføring er at mottakerlandets

⁸⁸ Ot. prp. nr. 92 (1998-99) om lov om behandling av personopplysninger s. 126.

rett også må inngå i overveielser. Dette er vesentlig for at ikke reglene om beskyttelse skal bli uthult. I den følgende drøftelsen kommer vi til å konsentrere oss om forhold som utelukkende berører overføringen, og derfor se på hvordan mottakerlandets rett skal vurderes.

4.2.1 Hva menes med begrepet tilstrekkelig?

Begrepet *tilstrekkelig* åpner for mange tolkinger. Vi har funnet få kilder som kan bidra som tolkingsmomenter, og vi må derfor basere oss på en språklig forståelse av begrepet. Men heller ikke dette gir oss mye å gå på. Normal forståelse av *tilstrekkelig* vil si at det som skal vurderes må være på et visst nivå, men ikke nødvendigvis på samme nivå.

Betyr et *tilstrekkelig* beskyttelsesnivå at det må være lik direktivets beskyttelsesnivå? Dette kreves blant annet i Europarådskonvensjonen om personvern fra 1981 art. 12 om overføring av personopplysninger. Etter bestemmelsen kan transaksjoner bare skje dersom det er et *tilsvarende* beskyttelsesnivå – *equivalent protection* – hos mottaker. Hovedregelen etter konvensjonen er imidlertid at det skal være fri flyt av personopplysninger. I tilfeller hvor opplysningens art tilsier det kan man begrense overføring, men ikke hvor mottaker kan vise til tilsvarende beskyttelse. Skal man tolke direktivets *tilstrekkelig* på samme måte? Når man i direktivets tekst har valgt å bruke *tilstrekkelig*, som er et mildere uttrykk, bør man ikke forstå dette som det strengere *tilsvarende*. Ved bruken av *tilsvarende* peker man på at mangler hos mottakerlandet kan kompenseres. Dette passer også godt sammen med at direktivet ved sin ordlyd legger opp til fleksibilitet ved å si at nivået av tilstrekkelighet skal vurderes på *grundlag af samtlige de forhold der har indflydelse på en videregivelse*, jf direktivet art. 25 nr. 2. Et krav om at Japan som mottakerland for personopplysninger skal ha lik beskyttelse av personvern som EU-landene, vil derfor være en meget streng tolking. Dette tilsier at man ved vurderingen av mottakers beskyttelsesnivå kan tillate at dette ligger under direktivets, så lenge direktivets formål og prinsipper ikke blir skadelidende. Kravet må innebære at det ikke skal skje en vesentlig forringelse av det vern direktivet gir.

Bruken av ordet *tilstrekkelig* indikerer at bare delvis overensstemmelse er påkrevet. Et relatert spørsmål er hvorvidt tilstrekkelighet utelukkende kan vurderes opp mot direktivets materielle regler, og at man kan se bort ifra bestemmelsene om kontroll. Dersom man ikke tar kontrollreglene i betraktning, vil man få en liten overensstemmelse mellom hovedregelen i direktivet art. 25 og unntakene i direktivet art. 26. Etter direktivet art. 26 nr. 2 kan man tillate eksport i enkelte tilfeller til tross for at kravet om tilstrekkelig beskyttelse ikke er oppfylt, men det krever at man har garantier for kontroll. Dette tilsier at kontrollregler blir tatt i betraktning ved vurderingen av nivået

på beskyttelsen, og at det er bakgrunnen for at man krever dette eksplisitt for å tillate unntak fra direktivet art. 25.⁸⁹ Som vi har sett skal det skje en helhetsvurdering, og det vil da bli inkonsekvent dersom enkelte deler av direktivet kan ses bort i fra.

Vurderingen av tilstrekkelighet gjelder for hele direktivets virkeområde og omfatter derfor både de materielle reglene, de registrertes rettigheter og andre krav som tilsyn og sikkerhet. Det skal også legges vekt på om det er mulig å få kontrollert og overprøvd for domstolene om reglene overholdes.⁹⁰ Dette innbyr til en omfattende og helhetlig tolking av retten i mottakerlandet.

4.2.2 Hvilke regler skal vurderes?

Hvilke regler skal så vurderes i mottakerlandet? Utgangspunktet finnes i EU-direktivet art. 25 nr. 2 der det blant annet heter at det skal legges vekt på *de retsregler – almindelige regler eller sektorregler – der er i kraft i det pågældende tredjeland, samt de regler for god forretningsskik og de sikkerhedsforanstaltninger, der gælder i landet.*

4.2.2.1 Vurdering av formell lov

Først vil vi se på hva som menes med *retsregler*. I norsk rettskildelære er en rettsregel den regel man kommer frem til ved en tolking basert på de aktuelle rettskildefaktorene.⁹¹ Man kan spørre om dette også er betydningen etter fellesskapsretten eller om begrepet skal forstås snevert slik at det kun omfatter formell lov. På den ene side vil vurderingen av tilstrekkelighet være enklere dersom man bare kan holde seg til den formelle lovgivningen i mottakerlandet. Siden det stilles generelt strenge krav til publisering og klassifisering av lover, vil det være forholdsvis lett å finne fram til de relevante bestemmelsene. Dette vil gjøre det enklere for behandlingsansvarlig å kunne foreta sin vurdering. På den annen side må man se hen til helheten i regelen. Det fremgår av direktivet art. 25 nr. 2 at både alminnelige regler, sektorregler samt regler for god forretningsskikk skal vurderes. Det vil derfor bli snevert å bare se hen til formell lov. Rettsregler i direktivets forstand må dermed anses å være tolkingsresultatet ikke bare av lov, men også av sedvane, kutyme og rettspraksis. For norsk retts vedkommende er slike rettskilder viktige på per-

⁸⁹ Greenleaf, Graham «A proposed privacy code for Asia-Pacific cyberlaw» *Emerging law on the electronic frontier, Journal of computer mediated communication*, volume 2 nr. 1: Part 1 of a special issue June 1996, Harvard university program on information resources policy s. 12-13. <http://jcmc.msc.huji.ac.il/vol2/issue1/asiapac.html> (28. mai 1999)

⁹⁰ Ot. prp. nr. 92 (1998-99) om lov om behandling av personopplysninger s. 126

⁹¹ Eckhoff, Torstein *Rettskildelære*, (3. utgave) TANO, Oslo 1993:24

sonvernrettens område, illustrert ved sentrale dommer som *To mistenkelige personer* Rt 1952/1217, *Sykejournaldommen* Rt 77/1035 og *Gatekjøkkenkjennelsen* Rt 1991/616, og man bør ikke utelukke at det samme kan være tilfelle i andre land. Vi mener derfor at rettsregler må forstås slik at alle typer regler med rettslig relevans omfattes av vurderingen.

Vurderingen av mottakerlandets rettsregler kan heller ikke begrenses til personvernrettens område fordi utfyllende bestemmelser kan finnes på andre rettsområder. I norsk rett utfyller for eksempel straffeloven § 390⁹² og forvaltningsloven §§ 13 flg.⁹³ personregisterlovens regler om henholdsvis privatlivets fred og taushetsplikt. Man må altså se hen til hele rettsbildet, og ikke bare til personvernretten i vurderingen av rettsreglene.

4.2.2.2 Vurdering av andre regler

Hvordan et land utformer sin lovgivning er påvirket av både lovtekniske og politiske vurderinger. Teknologisk utvikling stiller krav til lovgiver. På den ene siden bør loven være mest mulig teknologiavhengig for ikke å bli utdatert på grunn av tekniske nyvinninger. På den andre siden må lovgiver ta hensyn til at teknologien faktisk finnes og sørge for at dette reguleres i loven. Både generell og spesiell lovgivning kan ha problemer med å regulere et svært dynamisk fagfelt. En måte å avhjelpe dette på kan være å velge andre reguleringsformer enn lov, for eksempel ved at det utvikles bransjenormer som er bedre tilpasset bransjenes særegenheter.

Som vi så i punktet ovenfor er det ikke noe krav om at reglene i mottakerlandet må være i lovs form. I tillegg åpner EU-direktivet for at et nivå av tilstrekkelighet også kan utledes fra andre regler, som forretningsskikk, jf direktivet art. 25 nr. 2. Etter norsk rett vil forretningsskikk kunne omfatte sedvane og kutyme, men dette utelukker ikke at man kan godta en løsere form for praksis etter direktivet. Direktivet selv oppfordrer bransjer innad i EU til å utvikle egne regler gjennom art. 27. Slike bransjemessige retningslinjer kan defineres som et sett av bestemmelser om beskyttelse av opplysninger som gjelder for et flertall av behandlingsansvarlige innen samme yrkeskategori eller bransje, og hvis innhold først og fremst er fastsatt gjennom beslutninger av personer innen den aktuelle bransjen eller yrkeskategorien.⁹⁴ Med tanke på den helhetsvurdering som skal foretas etter direktivet art. 25, vil det være nærliggende at man også kan vurdere slike bran-

⁹² Almindelig borgerlig Straffelov av 22. mai 1902 nr. 10

⁹³ Lov om behandlingsmåten i forvaltningssaker av 10. februar 1967

⁹⁴ Working party on the protection of individuals with regard to the processing of personal data Working document: Transfers of personal data to third countries – applying articles 25 and 26 of the EU data protection directive, DG XV D/5025/98 WP12, 24. juli 1998:10

sjenormer i mottakerlandet. Dette vil gi et videre spillerom for tilstrekkelighetsvurderingen. Spesielt vil det være viktig i forhold til land hvor andre reguleringsformer enn lov ofte blir brukt, som i Japan.

I Japan har regjeringen oppfordret til utvikling av bransjenormer gjennom retningslinjer. Retningslinjen utarbeidet av *Ministry of International Trade and Industry* er en mal for utvikling av retningslinjer ellers. Dette tillater at hver bransje kan gjøre tilpasninger til sine spesielle forhold. Under punkt 4.1.8 diskuterte vi retningslinjenes relevans, og konkluderte med at de er relevante i diskusjonen om tilstrekkelighet. Når MITI-retningslinjen drøftes nedenfor vil fokus være rettet mot hvilken vekt de tillegges i de enkelte tilfellene.

4.2.3 Hvilke krav stilles til mottakerlandets regler?

Vi har nå sett hvilken rekkevidde beskyttelsen skal ha og hvilke regler som er relevante i vurderingen. I det følgende er temaet hvilke krav mottakerlandet må oppfylle for at beskyttelsen skal anses som tilstrekkelig. Dersom mottakerlandets regler skal gi tilstrekkelig beskyttelse må de på den ene siden inneholde regler som ivaretar EU-direktivets beskyttelse av personvern, og på den andre siden må det være en forutsetning at reglene faktisk følges, jf *sikrer* et tilstrekkelig beskyttelsesnivå i direktivet art. 25 nr. 1. I det følgende er det med eksempler fra japansk rett vi vil belyse kravet til tilstrekkelig beskyttelse.

4.2.3.1 Utgangspunkt for vurderingen

Hvordan mottakerlandets regler skal vurderes er ikke angitt i direktivet. Tolkning av direktivet byr på noen problemer fordi det er få rettskilder på rettsområdet. Formålsbetraktninger, juridisk teori og reelle hensyn vil derfor være sentrale før det foreligger praksis på området.

Når et fremmed lands håndhevelse av personvern skal vurderes ut ifra et europeisk regelsett er det ikke gitt at synsvinklene er direkte overførbare. Å sammenligne regler bestemmelse for bestemmelse for å se om ordlyden er mer eller mindre sammenfallende, er en svært tidkrevende og lite fleksibel tilnærmingstype. Vi har tidligere nevnt at interessenmodellen sammenfatter personverntanken i norsk rett som enkelte grunnleggende interesser tillagt individet. Det kan være nyttig å benytte denne tankegangen, og forsøke å trekke ut noen rettslige utgangspunkter av de reglene som fremkommer i direktivet. På en slik basis er det enklere å betrakte fremmede regelsett. Fokus skiftes da fra kartlegging av innholdet av enkeltbestemmelser til videre betraktninger innenfor rammen av de enkelte momentene. Dette vil også være i tråd med vår konklusjon ovenfor hvor det ikke kreves regel *likhet* mellom mottakerlandets

rett og EU-direktivet, men beskyttelse på et *tilstrekkelig* nivå. I drøftelsen nedenfor vil vi sammenfatte direktivets regler om beskyttelse i flere hovedpunkter. Disse momenter er formålsbegrensning; datakvalitet og proposjonalitet; innsyn, retting og sletting; åpenhet; sikkerhet og begrensning av videre overføring.⁹⁵ Sett i sammenheng er disse ment å dekke essensen i direktivets krav til mottakerlandets beskyttelsesnivå. På samme måte som med interessemodellen er det viktig å understreke at momentene ikke skal brukes slavisk, men at man må ta hensyn til den konkrete overføringens særegenhet. I enkelte tilfeller kan man se bort fra noen av momentene, og i andre tilfeller må momentene suppleres. Et moment som det må tas hensyn til ved enkelte overføringer er hvorvidt personopplysning er av sensitiv karakter eller ikke, og dette vil også bli behandlet.

Momentenes fulle innhold skal ikke drøftes her da det vil sprengte rammene for avhandlingen. Vi vil imidlertid forklare tanken bak dem, og knytte dette opp mot regler innen den japanske personvernretten.

4.2.3.2 Formålsbestemthet

Formålsbestemthet går ut på at innsamling og behandling av personopplysninger bare kan foretas for et bestemt formål, og all videre bruk må være forenlig med dette formålet. Kravet til formål er en måte å motvirke behandling som medfører en krenkelse av den personlige integritet, ved at personopplysninger ikke kan benyttes på en måte som ikke var tiltenkt på innsamlingstiden. Blir man i en markedsundersøkelse spurt om man snyter på skatten, skal ikke disse opplysningene senere brukes av skatteetaten som bakgrunn for å innkreve skatt. Eller tar fotoboksen bilde ved fartsovertredelse, kan ikke nødvendigvis informasjonen benyttes som bevis i en annen straffesak, jf *Fotobokskjennelsen* Rt 1990/1008. Et eksempel på en behandling som kan ha gått utover formålet er internettbokhandelen Amazons publisering av bestselgerlister. Detaljerte opplysninger om kundenes kjøpevaner oppdelt etter arbeids- eller studieplass er gjort tilgjengelig på deres nettsider. Det opprinnelige formålet med disse kjøpeprofilene var å benytte de til intern bruk og til markedsføring.⁹⁶ At innsamling skal skje for et særskilt formål innebærer

⁹⁵ Disse momentene er også foreslått som vurderingstemaer i: Working party on the protection of individuals with regard to the processing of personal data *Working document: Transfers of personal data to third countries – applying articles 25 and 26 of the EU data protection directive*, DG XV D/5025/98 WP12, 24. juli 1998:6

⁹⁶ Uten navn «Amazon avslører lesevaner» VG 3. september 1999
<http://www.vg.no/pub/vgart.hbs?artid=2748580> (6. september 1999).
 Pekere til kundeprofilene er tilgjengelig på Amazons hjemmeside:
http://www.amazon.com/exec/obidos/subst/lists/best/amazon-bestsellers.html/ref=gw_m_r_

at den ansvarlige må definere hensikten med innsamlingen og behandlingen så presist som mulig. En altfor generell definisjon eller almen beskrivelse av formålet vil ikke oppfylle kravet til bestemthet. For at behandlingens mål ikke skal endres underveis må formålet angis før behandlingen starter. Formålsbestemthet fremkommer av direktivet art. 6 nr. 1 litra b hvor personopplysninger skal innsamles for *udtrykkeligt angivne og legitime formål, samt at senere behandling heraf ikke må være uforenlig med disse formål*. Det er også styrende for hvilke opplysninger man kan samle inn og hvor lenge man kan oppbevare dem, jf direktivet art. 6 nr. 1 litra c og e.

Etter den japanske personvernloven art. 4 første ledd skal formålet med personregisteret spesifiseres, og dette formålet skal oppgis i melding til kontrollinstansen *Management and coordination agency*, jf art. 6 første ledd nr. 3.⁹⁷ Innsamlede personopplysninger skal heller ikke anvendes til andre formål enn det opprinnelige, jf personvernloven art. 9 første ledd.

I MITI-retningslinjen er hovedprinsippet at innsamling av personopplysninger bare skal skje til et klart spesifisert formål. Dette skal ligge innenfor virksomhetens legitime drift, og innsamlingen skal kun utføres i den utstrekning det er nødvendig for å oppnå formålet, jf art. 5. Videre skal innsamlingen skje på lovlig og rettfærdig vis, jf art. 6. Selve behandlingen av opplysningene må holdes innenfor formålet, jf art. 10. Hvorvidt man går utover formålet dersom en annen avdeling innen virksomheten bruker opplysningene, vil avhenge av angivelsen av formålet. Er det slik at opplysningene benyttes av en avdeling som den registrerte ikke kunne forutse, må man ha samtykke dersom formålet brytes. Innhenter et varehus personopplysninger for å sende ut informasjon om sine produkter, vil det være innenfor dette formålet dersom man sender en postordrekatalog fra varehuset. Samler et hotell personopplysninger for å informere om tilbud fra butikker i hotellet, vil det være et brudd på formålet dersom man sender produktinformasjon fra et varehus som eies av samme kjede som hotellet.⁹⁸ Utlevering av opplysninger til andre må også være i overensstemmelse med formålet, jf art. 13.

Både innenfor offentlig og privat sektor i Japan finnes det altså regler som ivaretar formålsbestemtheten, men loven har en svakhet ved at det ikke frem-

bo_4/002-1247707-3662255 (6. september 1999)

Se også Amazons privacy statement:

<http://www.amazon.com/exec/obidos/subst/misc/policy/privacy.html/002-0620454-6805218> (6. september 1999)

⁹⁷ *Management and coordination agency* presenteres nærmere i punkt 4.3.2.1.

⁹⁸ Ministry of International Trade and Industry «Handbook concerning protection of personal data» *JIPDEC Informatization Quarterly: The information society and privacy* JIQ nr. 115/1998:50-51

kommer hvilke krav som stilles til formålet. MITI-retningslinjen er mer omfattende og gir klarere regler om bruken av opplysningene. På dette punkt ligger den svært nær direktivets egne regler.

4.2.3.3 Datakvalitet og proporsjonalitet

Krav til datakvalitet betyr at personopplysningene som behandles må være nøyaktige og oppdaterte, og proporsjonalitet at de er relevante og ikke overflødige. Blir det registrert opplysninger ved opprettelse av et avisabonnement, vil ikke opplysninger om økonomiske forhold være relevante. Informasjonen man skal samle inn og behandle må stå i forhold til formålet med behandlingen. Når behandlingsansvarlig bare har tilgang til opplysninger som er relevante for behandlingen, minker sjansen for at utenforliggende hensyn virker inn på vurderingen. Det vil sikre at beslutninger ikke tas på feil grunnlag, og ivaretar den registrertes interesse i diskresjon. Etter direktivet art. 6 nr. 1 litra c må personopplysningene være nøyaktige og om nødvendig oppdaterte, og de må videre være tilstrekkelige, relevante og ikke overflødige i forhold til formålet med behandlingen.

Datakvalitet og proporsjonalitet sikres i den japanske personvernloven ved at omfanget av de innsamlede opplysninger ikke skal gå utover hva som er nødvendig for å oppnå formålet med behandlingen, jf personvernloven art. 4. Den behandlingsansvarlige skal også sørge for at opplysningene er korrekte, jf personvernloven art. 5 annet ledd.

I MITI-retningslinjen art. 16 sikres kvaliteten av opplysningene ved at det kreves at de er nøyaktige og ajourførte i den grad det er nødvendig for formålet. Dette skal forhindre at individets interesser krenkes ved at det benyttes gale eller utdaterte opplysninger. Opplysninger som ikke lenger er nødvendige for formålet med behandlingen skal ødelegges på en passende måte.⁹⁹

Spesifikke krav til kvaliteten kommer ikke frem i de japanske reglene. Hva som anses som korrekt og nøyaktig kan ofte være kulturelt betinget, og derfor vanskelig å vurdere uten flere kilder. Betraktningen ovenfor henger imidlertid nøye sammen med formålet. Gode regler om formålsbestemthet kan derfor virke positivt inn på vurderingen av kvalitet og proporsjonalitet. Mangel på kilder gir oss dessverre liten mulighet til å gå nærmere inn på problemstillingen. Vi konstaterer derfor bare det som er uttrykkelig fastsatt, nemlig at det finnes bestemmelser som ivaretar dette momentet i de japanske reglene.

⁹⁹ Ministry of International Trade and Industry «Handbook concerning protection of personal data» *JIPDEC Informatization Quarterly: The information society and privacy* JIQ nr. 115/1998:54

4.2.3.4 Innsyn, retting og sletting

Der momenter som formålsbestemthet og datakvalitet retter seg mot den behandlingsansvarlige, er kravet til innsyn, retting og sletting en rettighet særlig knyttet til individet. Dette gir individet en kontrollerende funksjon i forhold til behandlingsansvarlig. Innsyn er også med på å sikre datakvalitet fordi den registrerte kan holde seg orientert om behandlingen og påpeke feil. Innsynsretten medvirker derfor til å ivareta registrertes interesse i både fullstendighet og diskresjon. Krav om retting av feilaktige opplysninger eller sletting fra registre vil være avhengig av at man faktisk får vite hva som er registrert. Motsetningsvis vil innsynsmuligheten ha mindre effekt dersom man ikke har muligheten til å få rettet eller slettet feilaktige eller overflødige personopplysninger.

Retten til innsyn, retting og sletting etter direktivet følger av art. 12. Etter norsk rett vil innsyn også følge av andre regler som offentlighetsloven § 2,¹⁰⁰ som har regler om innsyn i forvaltningens saksdokumenter, og rettspraksis.¹⁰¹ Det man kan få innsyn i etter direktivet er om opplysninger vedrørende en selv blir behandlet, hvilke typer opplysninger det er snakk om, hvorvidt de utleveres og formålet med behandlingen. Dette er ikke en absolutt rett fordi man kan gjøre unntak av hensyn til blant annet statens sikkerhet, kriminalsaker og registrertes eller andres interesser, jf direktivet art. 13.

Etter den japanske personvernloven kan den registrerte skriftlig anmode om å få innsyn i sine opplysninger, jf personvernloven art. 13 første ledd. Imidlertid har man ikke innsynsrett i enkelte dokumenter og registre som skoleregistre, opptaksprøver til skoler, filer som inneholder opplysninger om diagnose og behandling ved sykehus, og opplysninger vedrørende kriminalsaker. Hovedregelen er at anmodningen om innsyn skal etterkommes, jf personvernloven art. 13 tredje ledd. Det er en rekke unntak fra innsynsretten: Opplysningene kan ikke meddeles registrerte dersom en slik utlevering kan hindre gjennomføringen av kriminalitetsbekjempelse og etterforskning eller vurdering av noens kvalifikasjoner, jf personvernloven art. 14 første ledd nr.1. Unntaket omfatter også tilfeller hvor informasjonen er fra tredjemann, jf personvernloven art. 14 første ledd nr. 2, eller hvor slike opplysninger kan være til skade for noens liv, legeme, eiendom eller andre interesser, jf personvernloven art. 14 første ledd nr. 3. Dersom innsyn blir nektet, skal begrunnelsen meddeles den som ber om innsyn, jf personvernloven art. 14 annet ledd. Etter personvernloven har en registrert som oppdager feil med personopplysningene kun en rett til å søke om å få disse rettet. Organet som har ansvaret for registeret skal undersøke de feilaktige informasjonen og hvorvidt det er nødvendig å rette disse, jf

¹⁰⁰ Lov om offentlighet i forvaltningen av 19. juni 1970 nr. 69

¹⁰¹ Se for eksempel *Sykejournaldommen* Rt 1977/1035.

personvernloven art. 17 første ledd. Er registrerte misfornøyd med resultatet av undersøkelsen, kan han søke om en ny undersøkelse, jf personvernloven art. 17 annet ledd. Prosedyrene for behandling av søknaden og eventuelt retting følger ikke av personvernloven, men av *Administrative complaints act*.¹⁰²

I MITI-retningslinjen er hovedregelen at krav om innsyn skal bli akseptert innen rimelig tid, jf art. 20. Finner man ved innsynet at personopplysninger er feil, har man i utgangspunktet krav på å få rettet eller slettet disse. Bestemmelsen åpner for at retting og sletting kan nektes, men det fremgår ikke av retningslinjene hvilke tilfeller det vil gjelde.

Som vi har sett er ikke retten til retting eller sletting ubetinget etter personvernloven eller MITI-retningslinjen. Dette er ikke ulikt den ordningen som eksisterer i personregisterloven § 8 i dag. Det er bare når manglene ved opplysningene kan få betydning for den registrerte at retting eller sletting skal innrømmes. Regelen er blant annet begrunnet i behovet for fullstendighet i statistisk eller historisk materiale.¹⁰³ I direktivet art. 12 litra b heter det at man *etter omstændighederne* kan få rettet eller slettet personopplysninger, og formuleringen åpner for at slik rett ikke må innrømmes i alle tilfeller. Den oppmerksomhet innsynsretten blir viet i de japanske kildene tyder på at dette er et viktig moment også for deres personvernrett. I en kommentar til MITI-retningslinjen understrekes det at den registrertes rett til innsyn, retting og sletting er en garanti for at individets interesser ivaretas.¹⁰⁴

4.2.3.5 Åpenhet

Åpenhet rundt behandlingen er tett knyttet til innsynsretten. Sammenhengen ligger i at der innsynsretten gir individet rettigheter og forutsetter at man selv tar initiativet overfor behandlingsansvarlig, vil reglene om åpenhet gjelde for allmennheten og rette seg mot den behandlingsansvarlige. Åpenhet gjelder altså hele behandlingsbildet og ikke enkeltoperasjoner. For at allmennheten kan følge med på at behandlinger skjer på en rimelig måte bør den ha tilgang til informasjon om formålet med behandlinger, identiteten til behandlingsansvarlig i mottakerlandet eller annen informasjon som er nødvendig for å sikre opplysthet om behandlingen. I forhold til forvaltningens behandling av personopplysninger vil åpenhet også være en viktig demokratisk rett.

¹⁰² I følge samtale med Professor Masao Horibe 16. januar 1999

¹⁰³ Djønne, Eirik; Grønn, Tove og Hafli, Tor *Personregisterloven med kommentarer*, TANO, Oslo 1987:79

¹⁰⁴ Ministry of International Trade and Industry «Handbook concerning protection of personal data» *JIPDEC Informatization Quarterly: The information society and privacy* JIQ nr. 115/1998:57

Reglene som knytter seg til åpenhet i direktivet er spredte. Prinsippet følger delvis av direktivet art. 21 om at medlemsstatene skal sørge for at det føres offentlig tilgjengelige registre over behandlinger. Ved at informasjon om behandlinger er tilgjengelige for allmennheten, kan datasubjektene få nok kunnskap til å hevde sine rettigheter. I tillegg skal det ved innsamling av personopplysninger gis informasjon som knytter seg til behandlingen, deriblant formålet og hvem som er behandlingsansvarlig, jf direktivet art. 10 og 11.

Etter den japanske personvernloven art. 7 skal hvert organ lage en fortegnelse over de personregistre det fører, og listen skal inneholde navn på registrene, hvem som er behandlingsansvarlig, formålet med registeret, hva som registreres, hvilke metoder som benyttes ved innsamling og hvorvidt opplysningene skal videregis. Denne fortegnelsen skal gjøres tilgjengelig for allmennheten, og i tillegg skal det offentliggjøres lister over registre minst en gang i året i *The Official Gazette*,¹⁰⁵ jf personvernloven art. 8. Etter MITI-retningslinjen art. 8 må visse opplysninger formidles til den registrerte før behandlingen kan ta til. Dette er opplysninger om at det er frivillig å gi fra seg opplysninger, hvem som er behandler med navn og kontaktinformasjon, formålet med behandlingen, planlagte utleveringer av opplysningene, hvem som er mottaker og at man har rett til innsyn, retting eller sletting.

Åpenhet etter personvernloven må sies å være godt ivaretatt. Fordi Japan ikke har noen nasjonal offentlighetslov,¹⁰⁶ vil de klare reglene om publisering være viktige for å sikre kontroll med forvaltningens behandling av personopplysninger. Tilsvarende regel finner vi ikke i MITI-retningslinjen, men demokratihensynet er ikke så fremtredende som ved forvaltningens behandling. Individets oversikt vil sikres av notifikasjonen som skal gis i forkant av behandlingen. Hvordan disse reglene fungerer i praksis vil henge sammen med hvordan formålet blir ivaretatt.

4.2.3.6 Sikkerhet

Sikring av personopplysningene er nødvendig for å hindre at informasjon går tapt eller at uvedkommende får adgang til informasjonen. Dårlig sikkerhet kan også føre til at informasjonen lekkes til andre, og at personopplysninger brukes til andre formål. Et nylig eksempel er Microsofts sikkerhetshull i deres gratis e-posttjeneste Hotmail, som har medført at brukernes e-post har vært

¹⁰⁵ *The Official Gazette* er regjeringens offisielle publikasjon

¹⁰⁶ Et forslag til offentlighetslov ble fremlagt for parlamentet 27. mars 1998 etter 20 års debatt og lobbyering.

Chafee, Judy og Repeta, Lawrence *Japanese government information: New rules for access*, Japan information access project, Washington D.C. juni 1998
<http://www.nmjc.org/jiap/specrpts/joho.html> (13. september 1999)

tilgjengelig uten passord.¹⁰⁷ Sikkerheten må ivaretas både ved tekniske og organisatoriske tiltak. Informasjonen kan for eksempel sikres ved kryptering, ved å oppbevares i adskilte nettverk som ikke kan aksesserer utenfra eller ved sikkerhetskopiering. Å sikre seg mot at ansatte lekker informasjon kan være vanskeligere, men det kan gjøres ved å begrense tilgangen til opplysningene til en begrenset krets av personer, ved instruksjonsmyndighet eller ved regler om taushetsplikt.

I følge direktivet art. 17 skal behandlingsansvarlig iverksette tiltak av teknisk og organisatorisk art for å beskytte personopplysningene. Sikkerhetstiltakene skal stå i forhold til den risiko behandlingen innebærer og opplysningenes art, og til de omkostninger innføringen av disse vil kreve. Overskriften til direktivet art. 16 er *Behandlingernes fortrolige karakter*, men bestemmelsens innhold er at behandling kun kan skje etter instruks fra behandlingsansvarlig og etter ordlyden kreves ikke konfidensialitet.

Den japanske personvernloven art. 5 første ledd fastsetter at behandlingsansvarlig skal innføre nødvendige tiltak for å hindre uautorisert tilgang, tap og ødeleggelse av personopplysningene. De personer som er involvert i behandlingen har taushetsplikt, jf personvernloven art. 12. Etter MITI-retningslinjen art. 17 skal sikkerhetstiltak innføres både på administrativt og teknisk plan for å sikre seg mot uautorisert tilgang, tap, endringer og lekkasje av personopplysninger. For å illustrere hvilke teknologiske løsninger som kan benyttes for å oppnå god sikkerhet vises det til *Information systems security guidelines*.¹⁰⁸ Eksempler på administrative tiltak som kan innføres er etableringen av interne regler og klare presiseringer av ansvar.¹⁰⁹ Alle ansatte i bedriften har taushetsplikt i overensstemmelse med lov eller arbeidsinstruks, uansett om de er involvert i behandlingen eller ikke, jf MITI-retningslinjen art. 18.

Både loven og retningslinjene har relativt godt utviklede regler for å ta vare på personopplysningers sikkerhet. For at disse skal ha noen funksjon er det imidlertid viktig at kravet til sikkerhet ses opp mot regler om håndhevelse ved brudd på sikkerhetsreglene. Hvordan etterlevelse kan skje ser vi på under punkt 4.3.3.

¹⁰⁷ Kvilesjø, Svend Ole «330000 norske e-postkasser åpne på nettet i går» *Aftenposten (Morgen)* 31. august 1999:2

Se også pressemelding fra Microsoft:

<http://www.microsoft.com/presspass/misc/08-30hotmail.htm> (6. september 1999)

¹⁰⁸ Ministry of International Trade and Industry, Notification nr. 518 av 29. august 1995

¹⁰⁹ Ministry of International Trade and Industry «Handbook concerning protection of personal data» *JIPDEC Informatization Quarterly: The information society and privacy* JIQ nr. 115/1998:55

4.2.3.7 Begrensning av videre overføring

Videre overføring fra mottaker av personopplysninger bør bare være tillatt der hvor det stilles likelydende krav til beskyttelse av senere mottaker. Dette fremgår ikke direkte av direktivet, men fravær av en slik regel vil bety et smutthull i reglene og føre til at direktivets betydning innskrenkes. I motsatt fall vil opplysninger kunne overføres til et land uten tilstrekkelig beskyttelse via et land med god beskyttelse. Skal en videregivelse skje må det nye mottakerlandets regler vurderes på samme måte som det originale mottakerlandets. Kravet vil da være det samme som i direktivet art. 25 ved at det kreves tilstrekkelig beskyttelse.

Når det gjelder begrensning av videre overføring av opplysninger i japansk rett, har ikke personvernloven regler som begrenser overføring til andre land. Det kan allikevel være restriksjoner for utlevering fordi personopplysningene ikke kan brukes til annet enn formålet, jf personvernloven art. 9 første ledd, eller formålet kan være av en slik art at det forhindrer videre utlevering. Det skal også i meldingen til *Management and coordination agency* opplyses hvorvidt opplysningene rutinemessig skal overføres til andre, jf personvernloven art. 6 første ledd nr. 6, slik at man kan føre kontroll med hvilke overføringer som foretas.

Etter MITI-retningslinjen vil videre overføring først og fremst være begrenset av art. 13 hvor utlevering av personopplysninger skal holdes innenfor behandlingens formål. Når slik utlevering skjer, må man på forhånd ha den registrertes samtykke, jf art. 14. Slikt samtykke er derimot ikke nødvendig dersom mottaker stiller garantier for at behandlingen skjer på tilsvarende – *equivalent* – måte som i avsenderbedriften, jf art. 14 nr. 2. Slike garantier må fremgå av en kontrakt som opprettholder konfidensialiteten rundt behandlingen, forbyr videre utlevering og plasserer ansvaret for urettmessig behandling.

Det er en svakhet i forhold til kravet om tilstrekkelighet at personvernloven ikke begrenser overføring til andre land. Hensynet til individets vern blir svekket i forhold til hensynet til en effektiv forvaltning. Ved overføring av personopplysninger fra EØS-området til Japan kan man risikere at opplysningene sendes videre til et fjerdeland med et dårligere beskyttelsesnivå. Denne mangelen kan avhjelpes ved at det stilles garantier for at slik overføring ikke vil skje, men disse må i så fall gis i hvert enkelt tilfelle. Heller ikke MITI-retningslinjen begrenser overføring til andre land, men kravet om likhet av behandlingen hos mottaker vil gjelde uansett om mottaker befinner seg i nabokommunen eller i utlandet. Retningslinjen kan derfor ha ringvirkning utover sitt virkeområde fordi virksomheter som ikke følger retningslinjen må garantere at de gir tilsvarende vern for å få utlevert personopplysninger.

4.3.2.8 Sensitive opplysninger

I enkelte tilfeller anses personopplysninger å ha en så nær tilknytning til personens integritet at det må stilles særlige krav til bruken av dem. Slike opplysninger betegnes som *sensitive opplysninger*. Disse opplysningene utgjør en spesiell risiko for datasubjektet fordi de har større skadeevne enn andre opplysninger dersom de skulle komme på avveie eller bli misbrukt. Ved en overføring vil denne typen av opplysninger kreve en særskilt beskyttelse. Oppfatningen av hva som er sensitive opplysninger er ikke universelt, men vil avhenge av kulturelle forhold og andre samfunnsoppfatninger. Hva som ligger i *sensitive opplysninger* i direktivets forstand fremgår av art. 8 nr. 1 og nr. 5: rasemessig eller etnisk bakgrunn; politisk, religiøs eller filosofisk overbevisning; fagforeningsmessig tilhørighet; opplysninger om helse- og seksuelle forhold og opplysninger om straffbare forhold. Denne listen må anses som uttømmende.¹¹⁰

I Japan har man ingen tilsvarende regel i personvernloven. At sensitive opplysninger ikke er omtalt, kan ha sammenheng med at den bygger på OECDs retningslinjer hvor sensitive opplysninger ikke er nevnt. Dette betyr ikke at slik informasjon ikke er spesielt beskyttet, men at man har valgt å begrense behandlingen av slike opplysninger på annet vis. Dette gjøres ved at formålet for behandling av personopplysninger må spesifiseres nøye: *There are two primary methods of restricting the collection of personal data from the perspective of the data subject: restricting the type and nature of the data that can be collected, and specifying the purposes of collection.*¹¹¹

I MITI-retningslinjen art. 7 finner vi bestemmelser om sensitive opplysninger, og hensikten er å styrke beskyttelsen av individets rettigheter.¹¹² Rase og etnisitet er å regne som sensitive opplysninger etter art. 7 nr. 1, mens opplysninger om straffbare forhold ikke omfattes. Filosofisk syn er heller ikke nevnt i retningslinjene. Derimot nevnes politisk og religiøs overbevisning i art. 7 nr. 3, hvor sistnevnte omfatter ideologi og tro. Ved å la religion også omfatte ideologi, kan det hende at det kan dekke enkelte opplysninger som vil omfattes av filosofisk overbevisning. I art. 7 nr. 4 er opplysninger om helse, medisinsk behandling og seksuelt liv ansett som sensitive opplysninger. Opplysninger om helse inkluderer informasjon om både tidligere, nåværende

¹¹⁰ Ot. prp. nr. 92 (1998-99) om lov om behandling av personopplysninger s. 28

¹¹¹ Ministry of International Trade and Industry «Handbook concerning protection of personal data» *JIPDEC Informatization Quarterly: The information society and privacy* JIQ nr. 115/1998:43

¹¹² Ministry of International Trade and Industry «Handbook concerning protection of personal data» *JIPDEC Informatization Quarterly: The information society and privacy* JIQ nr. 115/1998:43

og fremtidige fysiske og psykisk tilstand. Helseopplysninger om en person vil omfatte helsejournaler til dennes foreldre, søsken og andre slektninger i tilfeller hvor man har å gjøre med genetiske sykdommer.¹¹³ Opplysninger om fagforeningstilknytning regnes som meget sensitive i Japan,¹¹⁴ og reguleres av art. 7 nr. 3. Det er et sterkt motsetningsforhold mellom fagforeninger og arbeidsgivere, og bare 23% av de sysselsatte er organisert i fagforeninger¹¹⁵ mot 65% i Norge.¹¹⁶

I Japan finner man en kategori av sensitive opplysninger som man ikke gjenfinder i norsk rett eller fellesskapsretten. I MITI-retningslinjen art. 7 nr. 2 nevnes *family origin* og *legal domicile*. *Legal domicile* må tolkes svært vidt, og betyr ikke bare bosted eller folkeregistrert adresse. Det inkluderer blant annet lokal tilhørighet, fødselssted, opprinnelsesland og nasjonalitet. Både dette og familiebakgrunn kan blant annet si noe om ens sosiale status, og i det hierarkiske japanske samfunnet kan det gi grunnlag for sosial diskriminering. Det følger også av Grunnloven art. 14 at politisk, økonomisk eller sosial diskriminering ikke skal forekomme på bakgrunn av ens sosiale status eller familiebakgrunn. Slike opplysninger anses derfor som meget sensitive.¹¹⁷ At det er forbudt å innsamle opplysninger om bosted vil medføre store hindringer for korrespondanse og forsendelser, og det er heller ikke et absolutt forbud. Man kan samle opplysninger om vedkommendes bosteds fylke,¹¹⁸ men for mer detaljert informasjon må man ha vedkommendes uttrykkelige samtykke eller det må følge av lov eller være nødvendig for å ta rettslige skritt, jf MITI-retningslinjen art. 7. Derfor vil det ikke være noe hinder for et postordrefirma å behandle opplysninger om kundens bosted når kunden frivillig har oppgitt sin adresse i den hensikt å få tilsendt varene.

¹¹³ Ministry of International Trade and Industry «Handbook concerning protection of personal data» *JIPDEC Informatization Quarterly: The information society and privacy* JIQ nr. 115/1998:43

¹¹⁴ Samtale med professor Masao Horibe 16. januar 1999

¹¹⁵ I følge den offisielle hjemmesiden til *Ministry of Labour* <http://www.mol.go.jp/english/outline/09-1.htm> (12. september 1999)

¹¹⁶ Fra Statistisk sentralbyrå 1998
Hovedsammensetninger for arbeidstakere og andre landsomfattende arbeidstakerorganisasjoner
http://www.ssb.no/ukens_statistikk/utg/9919/12-1t.txt (12. september 1999)
Personer i alderen 16-74 år i arbeidsstyrken, sysselsatte og arbeidsledige, etter kjønn (AKU).

<http://www.ssb.no/emner/06/01/aku/tab-1999-08-12-02.html> (12. september 1999)

¹¹⁷ Ifølge samtale med professor Masao Horibe 16. januar 1999

¹¹⁸ Jf MITI-retningslinjen art. 7 nr. 2 – not including data relating to prefecture of current residence

At den japanske personvernloven ikke nevner sensitive opplysninger utelukker ikke at disse blir beskyttet gjennom for eksempel strengere krav til formålet. Muligens kan Grunnloven art. 14 legge føringer for hvordan personopplysninger av denne art skal behandles med sitt forbud mot diskriminering på grunnlag av rase, tro, kjønn, sosial status og familiebakgrunn. Hvorvidt det i praktiseringen av personvernloven foretas begrensninger av behandlinger som involverer sensitive opplysninger, har vi ikke kunnskap om. Det er en svakhet ved loven at det ikke kommer klarere frem hvordan sensitive opplysninger behandles, men dette svekker ikke tilstrekkelighetsnivået generelt. Det er kun i de tilfeller hvor det foretas en overføring av sensitive opplysningene at man må stille krav til at mottakerlandet behandler disse særskilt.

MITI-retningslinjen korresponderer i stor grad med direktivet, men den dekker ikke filosofisk overbevisning og straffbare forhold. Som vi så kan filosofisk overbevisning falle inn under religion som en ideologi. Overføring av kriminalopplysninger vil ofte bli behandlet særskilt under egne avtaler eller traktater. Spørsmål er om det skal kreves at Japan har tilsvarende regler på dette punkt når vi tidligere har sett at beskyttelsen ikke behøver å være lik, jf punkt 4.2.1. Når disse typer opplysninger på grunn av sin natur er regulert særskilt, kan det være begrunnet i at de skal anses som et absolutt krav. Som nevnt ovenfor kan oppfatningen av hva som anses som sensitivt variere. Eksempler er at fagforeningstilhørighet tradisjonelt ikke anses som en sensitiv personopplysning i Norge,¹¹⁹ og at man i Japan inkluderer opplysninger som ikke er sensitive etter direktivet. Konklusjonen er at beskyttelsen på dette punkt kan være god nok selv om man ikke har regel likhet, men at man kan hindre overføringer av enkelte sensitive opplysninger dersom man ikke får garantier for at disse får spesielt vern.

4.2.4 Oppsummering

Utgangspunktet i fremstillingen ovenfor var at innholdet i personvernreglene ikke behøver å være likt det direktivet krever for behandling innad i EU. Man må derfor akseptere at variasjoner innenfor både reglenes innhold og omfang forekommer. Vurderingen må da bli skjønnspreget, men ved å forholde seg til momenter som sammenfatter reglenes innhold kan man få en smidigere løsning enn ved en ordrett sammenligning.

De momentene som er drøftet ovenfor er alle i større eller mindre grad tilstede i de japanske personvernreglene vi har sett på. Det er en del ulikheter mellom personvernloven og MITI-retningslinjen, og en del av disse kan nok tilskrives lovens alder. Personvernloven er ikke tilpasset nye behandlingssitu-

¹¹⁹ NOU 1997:19 *Et bedre personvern* s. 133

asjoner eller den endrede bevissthet rundt personvern. det kan være en svakhet i forhold til EU-direktivet, med mindre praktiseringen av loven har endret seg i takt med tiden. Det peker på problemet med at en vurdering av mottakerlandets regler ikke gir det fullstendige bildet dersom man ikke også ser på hvordan de fungerer i praksis. Ser man til den norske personregisterloven fra 1978 er ikke praktiseringen alltid i overensstemmelse med lovens ordlyd, og på flere områder modifiseres mange viktige regler av forskrifter.¹²⁰ For å gi et helt korrekt bilde av den japanske personvernloven bør man derfor ikke bare se til lovteksten, men også til forskrifter, forvaltningens og kontrollorganets praksis og rettspraksis.

Momenter som er godt ivaretatt i japansk personvernrett er de sentrale personverngarantiene innsyn og åpenhet, som sikrer individets deltagelse og påvirkningskraft. Spesielt er det bra at det finnes klare regler for publisering av oversikter over offentlige registre, for åpenhet er viktig for at det skal kunne føres kontroll med forvaltningen. Motsetningvis kommer det ikke frem av direktivet hvordan den fortegnelse over behandlinger tilsynsmyndighetene i EU fører skal gjøres tilgjengelig for allmennheten.

Det er interessant å se hvilken plass sensitive opplysninger har i den japanske personvernretten. Omfanget av sensitive opplysninger er mer omfattende enn etter direktivet, og viser at kulturelle forskjeller påvirker personverntanken. Det må derfor vises varsomhet overfor mottakerlandets kulturelle forhold når tilstrekkeligheten skal vurderes.

Gjennomgangen viser også vanskeligheten med å slå fast om innholdet av reglene tilfredsstiller direktivets krav. Selv om man har hjelpemomenter er det et vanskelig spørsmål å finne ut i hvor stor grad disse skal oppfylles. Grensen for hvor store variasjonene kan være er vanskelig å trekke, og gjennomgangen vi har foretatt vil bare være rettleidende. Som vi har nevnt vil vurderingen av reglenes innhold være nødvendig, men like fullt bare være en del av den totale overveielser som må gjøres. Det er helhetsbildet som til slutt får avgjøre om tilstrekkelighetskravet er oppfylt.

4.3 Kontrollordninger

Dersom et tredjeland skal anses å ha et tilfredsstillende beskyttelsesnivå betyr dette at det ikke bare skal stilles krav til behandlingen av personopplysningene.

¹²⁰

Et eksempel på dette er at overføring i utgangspunktet krever konsesjon jf personregisterloven § 36. Den praktiske hovedregel er imidlertid at det bare kreves at melding sendes til Datatilsynet forut for overføringen jf forskriftene til personregisterloven § 8-1.

Det må også føres en viss kontroll med selve behandlingen. Dette vil være med å sikre etterlevelse av de regler som finnes. Slik kontroll kan tenkes foretatt på mange måter: internkontroll, selvregulering eller særlige overvåkingsorgan. Som en samlebetegnelse kan man kalle dette *kontrollordninger*. Det fremgår ikke direkte av direktivet at mottagerlandets mekanismer for kontroll med behandlingen skal vurderes, men i og med at det skal legges vekt på samtlige forhold som har innflytelse på overføringen, jf direktivet art. 25 nr. 2, vil det være naturlig at kontrollen av reglene også må tas i betraktning.

Spørsmålet som skal drøftes nedenfor er om de krav til kontroll av behandlingen EU-direktivet stiller for medlemsstatene, også skal kreves av mottagerlandet. Vi vil derfor først se på hvilke krav EU selv setter til kontroll over behandlingen, deretter eksemplifisere dette ved å se på hvilken løsning som er valgt i norsk rett og til slutt se hvilke mekanismer som finnes i japansk rett.

4.3.1 EUs krav til tilsynsmyndighet

Etter EU-direktivet art. 28 skal hver medlemsstat sørge for at det utpekes en eller flere myndigheter som har til oppgave å påse at personvernreguleringen overholdes. Dette eller disse organene kalles i direktivet for *tilsynsmyndighet*. Man kan ha flere tilsynsmyndigheter ved at de overvåker forskjellige områder eller sektorer. For eksempel kan man ha en tilsynsmyndighet for privat sektor og en for den offentlige sektor, eller enda mer spesifikt med en for prosessindustrien og en for tjenesteytere. Sverige har valgt en delt løsning, hvor oppgavene er delt mellom et personoppgiftsombud og Datainspeksjonen, jf personoppgiftslagen §§ 38-40 og §§ 43-47.¹²¹ I norsk rett er disse pliktene tillagt Datatilsynet, og hjemlet i personregisterloven § 2 første ledd. Denne organiseringen er også fulgt opp i personopplysningsloven § 42.

Tilsynsmyndigheten er lagt til offentlig myndighet, og den skal være uavhengig, jf direktivet art. 28 nr. 1. Uavhengig må forstås som uavhengighet i forhold til den utøvende statsmakt, men helt løsrevet fra statsadministrasjonen kan den ikke være i og med at den skal være en offentlig myndighet. I praksis betyr dette at tilsynsmyndighetens funksjon skal være uten innblanding, men at det administrativt er underlagt et forvaltningsorgan.

Personregisterloven § 2 beskriver Datatilsynet som frittstående, men underlagt Justisdepartementet administrativt. Det kan imidlertid stilles spørsmål om Datatilsynets uavhengighet er tilstrekkelig siden det er Justisdepartementet som er klageinstans, jf forvaltningsloven § 28 første ledd.¹²² EU-direktivet stiller strengere krav til uavhengighet, og dette har ført til at det i perso-

¹²¹ Personoppgiftslag SFS 1998:204 av 29. april 1998

¹²² Lov om behandlingen i forvaltningssaker av 10. februar 1967

nopplysningsloven er foreslått å opprette en Personvernemnd, jf personopplysningsloven § 43. Personvernemnda skal være et uavhengig forvaltningsorgan som administrativt er underlagt Justisdepartementet. Leder og nestleder skal i henhold til personopplysningsloven § 43 annet ledd utnevnes av Stortinget, mens de øvrige fem medlemmer utnevnes av Kongen. Etter personopplysningsloven er det Personvernemnda som skal avgjøre klagesaker over Datatilsynets avgjørelser, og dens avgjørelser kan ikke omgjøres av departementet. Er man ikke tilfreds med nemndas avgjørelse må man i tilfelle gå til søksmål mot staten vedrørende avgjørelsens gyldighet, jf personopplysningsloven § 43 femte ledd.

Tilsynsmyndigheten har til oppgave å være høringsorgan ved utarbeidelse av forskrifter og administrative foranstaltninger om personvern, jf EU-direktivet art. 28 nr. 2. I tillegg har den myndighet til å blant annet undersøke behandlinger, gripe inn og stanse behandlinger dersom nødvendig og til å bringe overtredelser inn for domstolene, jf direktivet art. 28 nr. 3. Den oppramsingen som er gitt i direktivet art. 28 nr. 3 er ikke en uttømmende liste over oppgaver som tilfaller tilsynsmyndigheten, jf *skal bl.a. kunne*. Det er derfor opp til medlemsstatene å presisere oppgavene ytterligere. Etter personopplysningsloven § 42 er Datatilsynet gitt i oppgave å føre en fortegnelse over alle behandlinger; behandle konsesjoner, motta meldinger og gi pålegg; kontrollere at lov og forskrifter følges, og påse at feil og mangler ved behandlingen rettes; holde seg orientert om utviklingen av personvern; gi råd, veiledning og uttalelser.

Direktivets løsning innebærer en viss frihet for medlemsstatene. De organiserer selv sin tilsynsmyndighet, i tillegg til at oppgavene kan defineres nærmere av statene selv. Også mottagerlandene må ha frihet til å forme sine kontrollorgan. Vi har tidligere konkludert med at kravet til tilstrekkelighet ikke innebærer at man skal ha tilsvarende beskyttelse som EU-direktivet oppsetter, se punkt 4.2.1. Dette bør også gjelde for mottagerlandets kontroll med behandling av personopplysninger.

4.3.2 Kontrollordninger i Japan

Ovenfor ble kontrollorganets uavhengighet understreket som et viktig krav etter EU-direktivet. Bør man stille de samme kravene til et tredjelandets kontrollorgan? Direktivets krav til uavhengighet kan være begrunnet i at den løpende kontrollen med hvordan personopplysninger blir behandlet ikke skal være politisk motivert, slik tilfellet kan være dersom den utføres av den utøvende myndighet. For å få en mest mulig enhetlig praksis innen den Europeiske Union er det viktig at personopplysninger ikke blir behandlet forskjellig ut ifra det enkelte medlemslands politiske klima. Disse momentene er ikke umiddelbart

overførbare når man ser på kontrollordninger i mottakerlandet. Her vil forhold som faktisk og effektiv etterlevelse være viktigere. Kontrollordningenes organisering vil ha mindre betydning så lenge de sørger for at reglene overholdes. Vi mener derfor at det ikke kan stilles samme krav til uavhengighet av tredjelandets kontrollordninger som det direktivet art. 28 krever.

Å kreve en lik løsning for kontroll i mottagerlandene på linje med direktivet, vil være vanskelig fordi det kan være store forskjeller i hvordan administrasjonen er organisert eller hvilken myndighet den har. Løsningen må være at man ved tilstrekkelighetsvurderingen må akseptere at det er forskjellige måter å organisere kontrollordninger på. Tilsynsmyndighet er én form for kontrollordning, men det finnes alternative løsninger. Fordi mottagerlandets kultur, økonomiske forhold og administrasjon vil spille en stor rolle for hvordan kontroll forgår, er det vanskelig å fastsette bestemte minstekrav. Man må heller se hen til hvordan løsningen fungerer i praksis, og hvilken betydning den har.

4.3.2.1 The Management and coordination agency

Etter Japans personvernlov er det *The Management and coordination agency*¹²³ (MCA) som er gitt en kontrollerende funksjon. Organet ble opprettet i 1984, og er underlagt Statsministerens kontor. MCA ledes av en Director General som er minister med plass i regjeringen. MCAs primære oppgaver er å veilede regjeringen for å oppnå en mest mulig effektiv og koordinert forvaltning, for dermed å være best mulig skikket til å takle sosiale og økonomiske forandringer.¹²⁴ Dette arbeidet inkluderer også ettersyn med hvordan personvernloven overholdes. MCAs arbeidsoppgaver spenner altså langt videre enn bare å være kontrollerende instans for personvernloven.

Videre må vi se på om MCAs kompetanse er tilstrekkelig for å kunne utføre oppgaven som kontrollerende instans. Skal et offentlig organ behandle personopplysninger må det sendes melding om dette til MCA på forhånd, jf personvernloven art. 6 nr. 1. Meldingen blant annet skal inneholde formålet med behandlingen, innsamlingsmetoden og hvem som er ansvarlig for behandlingen. Behandlingsansvarlig skal også lage en fortegnelse over de registre som opprettes, og gjøre denne tilgjengelig for allmennheten, jf personvernloven art. 7 første ledd. Per 1. juli 1996 hadde 1486 registre blitt meldt til MCA.¹²⁵ Meldingene som MCA mottar offentliggjøres minst en gang i året i

¹²³ Somucho på japansk

¹²⁴ Fra *The Management and coordination agency* offisielle hjemmeside:
http://www.somucho.go.jp/soumu/index_e.htm (12. august 1999)

¹²⁵ Management and Coordination Agency *Summary of the 1996 Annual report*, Tokyo
<http://www.somucho.go.jp/soumu/cha000.htm> (19. august 1999)

The Official Gazette, jf personvernloven art. 8 første ledd. Hvert år foretar også MCA en undersøkelse av hvordan loven håndheves av de organer som faller under lovens virkeområde. MCA har også rett til å foreta inspeksjoner av registrene.¹²⁶ Etter personvernloven art. 21 kan MCA kreve en forklaring av lederen for det organet som behandler personopplysningene om hvorfor loven ikke er fulgt. Det kan også komme med uttalelser av eget initiativ til Statsministeren eller lederen for andre offentlige organer, dersom det synes nødvendig for å oppnå formålet med loven, jf personvernloven art. 22. I tillegg utferdiger MCA forskrifter for å utfylle loven.¹²⁷

Sammenligner man MCAs kompetanse med Datatilsynets, finner man mange likhetstrekk. Det som ikke fremkommer av personvernloven er om MCA har kompetanse til å gripe inn i behandlinger. Selv uten en slik rett til å gripe inn har nok uttalelsesmuligheten til MCA en viktig funksjon på grunn av det formelle japanske hierarkiet. MCAs organisering under Statsministerens kontor bidrar også til at dets vurderinger veier tungt, og i praksis har MCA stor makt til å kontrollere aktivitetene som foretas.¹²⁸ Dette kommer imidlertid sjelden datasubjektet til gode dersom en enkeltperson føler at behandlingen er gal, og her er neppe kontrollmuligheten god nok. Det kan også stilles spørsmål ved om MCAs mulighet til å gripe inn ved lovstridige behandlinger er vid nok.

4.3.2.2 Myndighet i henhold til lokal lovgivning

Som nevnt under punkt 4.1.3 finnes det utstrakt lokal lovgivning på personvernrettens område. De fleste av disse oppnevner en *Commision of privacy protection*. Denne komitéen består av personer med særlig kunnskap og erfaring med personvernspørsmål. Den kan undersøke enhver henvendelse fra individer, og rapporterer til ordføreren eller guvernøren i kommunen eller fylket.¹²⁹ Hvorvidt lokal lovgivning vil ha innflytelse på tilstrekkelighetsvurderingen er tvilsomt. Ingen av disse reglene er oversatt, og for en behandlingsansvarlig vil det være en vanskelig oppgave å orientere seg i disse reglene.

¹²⁶ Management and Coordination Agency *Summary of the 1996 Annual report*, Tokyo <http://www.somucho.go.jp/soumu/cha000.htm> (19. august 1999)

¹²⁷ SOU 1997:39 Integritet, offentlighet, informasjonsteknik. Betänkande av Datalagskommittén s. 317

¹²⁸ Samtale med professor Masao Horibe, Tokyo 19. januar 1999

¹²⁹ Franklin, Charles E. H. (red) *Business guide to privacy and data protection legislation*, Kluwer law international, Den Haag 1996:283

4.3.2.3 Privat sektor

Etter art. 22 i MITI-retningslinjen skal hver bedrift utpeke en person som har det overordnede ansvaret for at reglene etterleves – *Personal Data Manager*. Denne personen har etter art. 23 blant annet i oppgave å spre kunnskap, lage interne instruksjoner og implementere sikkerhetsløsninger, for på den måten å sørge for at retningslinjen blir iaktatt. Man har altså valgt at kontrollen skal skje gjennom selvregulering, og ikke ved et eksternt organ. Dette kan delvis forklares ut ifra japanernes misnøye med regulerende organer, men er også begrunnet i praktiske hensyn.¹³⁰ I Japan finnes det nesten to og en halv millioner bedrifter.¹³¹ Dersom ett enkelt organ skulle kontrollere alle behandlinger av personopplysninger disse foretar, ville det bety en enorm arbeidsbyrde og et voldsomt byråkrati. Et spørsmål er om et selvregulerende organ av denne typen kan anses å være en kontrollordning. I utgangspunktet har den som er utpekt som ansvarlig ingen mulighet til å påtale overtramp etter MITI-retningslinje.

Dersom kontrollen som er nedfelt i retningslinjen fungerer, kan dette være nok til at det anses å ha funksjon som en kontrollordning. Vi vet derimot for lite om oppfølgingen av retningslinjene i Japan til å kunne komme med noen konklusjon, men det er mye som tyder på at denne kontrollformen alene ikke er nok.

4.3.2.4 Privacy mark award system¹³²

Privacy mark award system (PMS) er et ordning som ble innført 1. april 1998 av MITI. Gjennom PMS kan bedrifter bli akseptert som «personvernvennlige» og gitt muligheten til å bruke PMS-merket (se Figur 4) i sin virksomhet.

¹³⁰ Management and Coordination Agency *Summary of the 1996 Annual report*, Tokyo <http://www.somuch.go.jp/soumu/cha000.htm> (19. august 1999)

¹³¹ *Japan almanac 1999*, Asahi shimbun, Tokyo 1998:90

¹³² Privacy Mark Award System er nærmere beskrevet i: Ministry of International Trade and Industry «Privacy mark award system» *JIPDEC Informatization Quarterly: The information society and privacy* JIQ nr. 115/1998:27-32 <http://www.jipdec.or.jp/security/privacy/pamph-e.html> (20. august 1999)



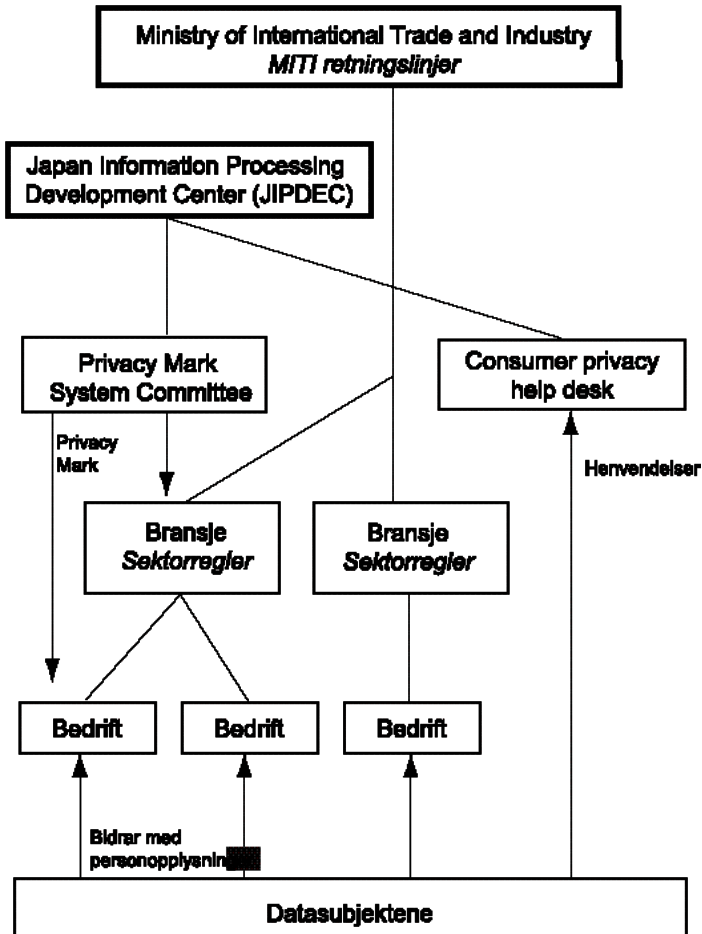
Figur 4

I konklusjonen ovenfor kom vi til at retningslinjens betydning kan være begrenset på grunn av manglende kontrollerende funksjoner. Japanske myndigheter har også innsett at landet, særlig innen privat sektor, ikke har noe fullgodt system for tilfredsstillende kontroll av behandling av personopplysninger. Ordningen er også opprettet for å gi retningslinjene større innflytelse enn de til nå har hatt innad i bransjene. Men der hvor retningslinjene først og fremst retter seg mot behandlingen av personopplysninger innad i bedriften, retter PMS seg i tillegg mot datasubjektene. Ved å bruke PMS-merket kan menigmann på en enkel måte identifisere de selskaper som oppfyller retningslinjene. Egne lister over bedrifter som oppfyller kravene skal også publiseres. På denne måten vil man øke folks årvåkenhet overfor personvernsspørsmål, slik at bedriftene blir nødt til å ta hensyn til dem for å opprettholde tilliten blant folk. *Privacy mark award system* er altså en ekstern håndhevelsesmekanisme knyttet opp til bransjemessige retningslinjer.

Systemet er organisert i to hovedelementer. Den ene delen skal representere de forskjellige bransjene, hvor hver bransje vil ha en egen bransjeorganisasjon. Denne skal utarbeide retningslinjer for sektoren basert på MITIs retningslinjer, drive veiledende virksomhet overfor bedriftene og motta søknader om godkjenning innen sitt område. Selve vurderingen og godkjenningen blir utført av *Japan Information Processing Development Center* (JIPDEC). JIPDEC er en uavhengig, «non-profit» organisasjon som har til formål å fremme den informasjonsbehandlernde industrien i Japan. Innenfor JIPDEC har man opprettet en faggruppe, *Privacy Mark System Committee*, som skal sørge for at de tekniske og juridiske sidene ved systemet er oppdatert, og som godkjenner bransjeorganisasjonene. I tillegg er det opprettet en ombudsordning, *Consumer privacy help desk*, som skal behandle klager og være rådgivende overfor forbrukere. Se Figur 5 for en skjematisk fremstilling av organiseringen.

Tegnforklaring

Strek (–) = Instruksjonsmyndighet/direkte underlagt
 Pil (→) = påvirkningsmulighet



Figur 5

Alle bedrifter har mulighet til å søke om å få bruke PMS-merket. I sin vurdering skal JIPDEC se på om kravene i retningslinjen for den aktuelle bransjen er fulgt av selskapet. I denne vurderingen skal alle kravene som stilles til behandling av personopplysninger i retningslinjene gjennomgås. Som vi har sett i punkt 4.2.3 er mange av disse kravene like de EU-direktivet krever for egne medlemsland. I vurderingen av kontrollfunksjonen skal det spesielt legges vekt på om firmaet har etablert en struktur for behandling av personopplysninger med en eller flere personer som ansvarlige; om det er en person som utad fungerer som kontaktperson for henvendelser; om det er tatt sikkerhetsmessige foranstaltninger for å hindre at uvedkommende får tak i informasjonen; om bedriften sørger for at alle underkontraktører eller andre eksterne som ønsker å benytte personopplysningene behandler disse på forskriftsmessig måte. Dersom bedriften anses å oppfylle kravene får den lov til å benytte seg av PMS-merket i en toårs periode. Deretter må en ny vurdering til før det kan fornyes. JIPDEC kan kreve rapportering av personverntiltakene i bedriften, og kan foreta undersøkelser. Bryter bedriften kravene i perioden, kan retten til å bruke PMS-merket trekkes tilbake og rettslige skritt tas.

PMS-systemet vil ikke bidra til at Japan som sådan sikrer et tilstrekkelig beskyttelsesnivå. Systemet kan imidlertid være relevant ved vurderingen av enkelte bransjer eller bedrifter når disse er mottagere av personopplysninger. Spørsmålet er hvorvidt retningslinjene sammen med PMS kan anses å ha en tilfredsstillende kontrollfunksjon. Systemet er frivillig, og vil derfor ikke medføre tilstrekkelighet for de bedrifter som ikke er tilknyttet ordningen. For de bedrifter som bruker systemet, vil man nok ha en viss sikkerhet for at bedriften ivaretar de grunnleggende hensynene til behandling av personopplysninger. Muligheten for privatpersoner til å klage på brudd på ordningen og retten til å frata en bedrift muligheten til å benytte PMS-merket gjør kontrollmuligheten mer reell.

4.3.2.5 Kontroll gjennom innsyn

Individets mulighet til innsyn i behandlinger om en selv kan virke kontrollerende overfor behandlingsansvarlig. Gjennom muligheten til å orientere seg om opplysninger registrert om en selv kan datasubjektet medvirke til at behandlingen skjer på en rettmessig måte. Dette forutsetter imidlertid ikke bare en rett til innsyn, men også at man som datasubjekt har rett til å komme med innvendinger dersom feil oppdages.

Under punkt 4.2.3.4 presenterte vi de mulighetene for innsyn som eksisterer i japansk personvernrett. Konklusjonen er at det finnes innsynsregler i både personvernloven og retningslinjene. Selv om kravet til innsyn skulle være oppfylt vil ikke dette være avgjørende for om regelsettet skal kunne

anses som en kontrollordning. En effektiv kontrollordning er avhengig av om innsynsretten faktisk brukes. Vi har ingen tall fra privat sektor som kan illustrere dette, da disse må samles inn fra hver enkelt bransje. I offentlig sektor var det i 1995 totalt 607 krav om innsyn i til sammen 14 personregistre,¹³³ og alle disse ble innvilget. Med så lave tall er det vanskelig å kunne se på innsynsretten som et fungerende kontrollmulighet. Dersom PMS-ordningen fungerer vil dette kunne gi datasubjektet mulighet til innsigelser gjennom *Consumer privacy help desk*. Se Figur 5. I så fall vil innsynsretten være en del av et større system og ikke stå på egne ben som kontrollordning.

4.3.3 Sanksjonsmuligheter

For at personvernreglene skal bli respektert og etterlevd, må brudd på disse ha følger for behandlingsansvarlig. For å sikre overholdelse av reglene er sanksjoner vesentlige. EU-direktivet art. 24 overlater til medlemsstatene å fastsette hvilke sanksjoner som skal anvendes ved overtredelse av de nasjonale personvernbestemmelsene. Det er ikke angitt nærmere hvilke typer sanksjoner man skal anvende, og det kan være både straffesanksjoner og andre tiltak. Kravet til tilstrekkelighet må derfor presiseres slik at reglene som skal vurderes også bør inneholde bestemmelser som sikrer etterlevelse.

4.3.3.1 Formell lov

I den japanske personvernloven er det bare én sanksjonsbestemmelse. Etter personvernloven art. 25 skal en person som urettmessig har fått tilgang til personregistre, ilegges en bot oppad begrenset til JPY 100.000.¹³⁴ Lengre enn dette strekker ikke sanksjonsmulighetene i personvernloven seg. I seg selv tilfredsstiller dette neppe kravet til sanksjoner etter EU-direktivet. Imidlertid må man ikke ved denne vurderingen bare se til personvernloven. Sanksjoner ved brudd på lovens bestemmelser kan følge av andre rettsregler. For eksempel sier personvernloven art. 12 at ansatte som er involvert i behandlingen av personopplysninger har taushetsplikt. Sanksjoner ved brudd på taushetsplikten reguleres ikke av personvernloven, men følger av *Law on government employees*¹³⁵ som inneholder straffebestemmelser. For andre brudd på lovens regler kan sanksjoner følge av for eksempel straffeloven og alminnelig erstatningsrett, se punkt 4.3.3.3 om oppreisning.

¹³³ Management and Coordination Agency *Summary of the 1996 Annual report*, Tokyo <http://www.somucho.go.jp/soumu/eha000.htm> (19. august 1999)

¹³⁴ Dette tilsvarende NOK 7000,- pr. august 1999.

¹³⁵ Lov nr. 120 1947

4.3.3.2 Retningslinjer

For retningslinjene kan man spørre om de må være obligatoriske for at etterlevelsen kan sies å være god nok. Hvorvidt et regelsett er obligatorisk eller ikke kan ses fra flere vinkler. På den ene siden kan det være frivillig å tiltre dem, men når det er skjedd må de etterleves. Tiltredelse vil i så fall skape en rettsplikt. En annen mulighet er at reglene både er frivillige å tiltre og også å følge. Dette kan være tilfellet der det ikke finnes noen sanksjonsmuligheter som følger reglene. En tredje løsning er at man er nødt til å tiltre reglene, men uten at noen sanksjoner er tilknyttet. Dette kan være tilfelle der man som medlem av en organisasjon automatisk må godta de regler denne utarbeider. Det ideelle for et godt nivå av etterlevelse er at regler både må tiltres og at oppfølging kreves. Den retningslinjen vi har sett på er i all hovedsak frivillig å tiltre, med få sanksjonsbestemmelser. Dette gjør vurderingen vanskeligere fordi man da må se på den faktiske etterlevelsen, og det krever merarbeid for den som foretar vurderingen. Retningslinjer som er frivillige vil også måtte tillegges mindre vekt når de bedømmes. Ved en overføring skal man imidlertid se hen til den konkrete transaksjonen, og dersom den aktuelle bedriften faktisk har gjennomført retningslinjene vil dette være et moment som må tas i betraktning.

Også for frivillige retningslinjer kan etterlevelse sikres gjennom muligheter for sanksjoner ved brudd på reglene. Siden vi her snakker om bransjemessige retningslinjer som ikke er gitt med hjemmel i lov, vil legalitetsprinsippet forhindre strafferettslig forfølgning ved brudd på retningslinjene.¹³⁶ MITI-retningslinjen har ikke egne regler om sanksjoner. Dette har sammenheng med at bransjene selv skal tilpasse retningslinjen til sin situasjon, og dermed også fastsette passende sanksjoner. Av de bransjeregler vi har sett på er det bare *The federation of bankers association of Japan* (Zenginkyo) som har en bestemmelse om at medlemmer ved brudd på reglene vil bli straffet.¹³⁷ Det viktige er ikke nødvendigvis sanksjonens art, men at den faktisk har en effekt. Siden retningslinjene er gitt av bransjeorganisasjoner vil man være tilknyttet en slik organisasjon dersom man tiltrer reglene. Internt kan organisasjonen ha regler om bøter eller utestengelse av bransjeorganene dersom reglene ikke blir fulgt. Utenom organisasjonene kan imidlertid også statsadministrasjonen spille en rolle. Den malen som skal ligge til grunn for bransjereglerne er jo utviklet av MITI. Dersom departementet føler at reglene ikke blir fulgt og dette kan være til skade for landet, kan det bruke sin

¹³⁶ Grunnloven av 1946 art. 31 [...] nor shall any other criminal penalty be imposed, except according to procedure established by law

¹³⁷ Japanese Bankers Association *Privacy protection, Personal credit information center*, Tokyo <http://www.zenginkyo.or.jp/en/pcic/pcic05.htm> (8. juli 1999)

innflytelse til å presse gjennom sin vilje og på den måten straffe overtredelser.¹³⁸ I et samfunn hvor det er viktig ikke å miste ansikt, vil også andre metoder være mer effektive. En er blant annet gjennom publisering av artikler av kjente akademikere med kritikk eller avsløring av bedrifter med dårlig personvernpraksis, noe som kan ha langt større effekt enn tradisjonelle sanksjoner.¹³⁹ Ellers kan domstolene dømme en behandlingsansvarlig til å avstå fra bestemte handlinger, for eksempel at behandlingen må opphøre, etter generelle prinsipper om personlighetens rettsvern.¹⁴⁰

Hvorvidt dette er tilstrekkelig for å oppfylle kravene etter EU-direktivet er usikkert. Generelt kan man neppe si at kravet til etterlevelse er oppfylt. Der- som man ser på den enkelte sak kan slike regler imidlertid ha sin funksjon. Problemet med en slik tilnærming vil være at behandlingsansvarlig sjelden har mulighet til å gjøre så grundige undersøkelser i mottakerlandets rett.

4.3.3.3 Muligheter for oppreisning

Etter EU-direktivet art. 23 har man krav på å få erstatning ved brudd på personvernreglene. Det fremkommer ikke av direktivet hvilke skader som erstattes, så dette vil avhenge av medlemsstatenes erstatningsrett. Etter personopplysningsloven § 49 tredje ledd skal erstatningen først og fremst svare til det økonomiske tap som er påført skadelidte ved ulovlig behandling av personopplysninger. Imidlertid kan den behandlingsansvarlige også pålegges å erstatte skade av ikke-økonomisk art.

Bestemmelser om erstatning finnes hverken i den japanske personvernloven eller MITI-retningslinjen, men etter alminnelig erstatningsrett kan erstatning kreves i enkelte tilfeller. Etter *Civil Code* art. 709¹⁴¹ følger det at *A person who intentionally or negligently violates the right of others shall be liable for the loss caused by the act*. Det er først og fremst økonomisk tap som dek-

¹³⁸ Et eksempel er Sumotomi Metal saken fra 1964. Det var nedgangstider og MITI hadde vedtatt at stålproduksjonen måtte reduseres for å stabilisere prisene. Alle stålprodusentene var enige om å redusere sin kvote bortsett fra Sumotomi Metal. Da disse ufortrødent fortsatte å produsere som før, ga MITI klar beskjed om at det også var dette departementet som kontrollerte fordelingen av utenlandsk kapital. Sumotomi Metal var avhengig av for å kunne importere jernmalm og kull. Sumotomi ville gå rettens vei, men saken ble løst i minnelighet. Eksempelet ligger på siden av personvernet, men er brukt for å illustrere MITIs mulighet til å gå aktivt inn med sanksjoner selv om det ikke finnes hjemmel i de aktuelle reglene.

Matsushita, M «International Trade and Competition Law in Japan», Dean, Meryll (red) *Japanese legal system: Text and materials*, Cavendish publishing limited, London 1997:196

¹³⁹ Samtale med Professor Horibe (16. januar 1999)

¹⁴⁰ Oda, Hiroshi *Japanese law*, Butterworth & Co, London 1992:228-229

¹⁴¹ Civil Code av 1896

kes av denne generalklausulen. Erstatning for ikke-økonomisk tap følger av *Civil Code* art. 710: *A person who, on the basis of the preceding provisions, is liable for damages of non-pecuniary loss, irrespective of whether he has harmed the other person physically, prejudiced his freedom, his honour or his property rights.* Slik erstatning ble tilkjent i saken *Utago no Ato*, nærmere beskrevet i punkt 4.1.4.

Det er ikke noe krav om at reglene om erstatning må kunne utledes av de aktuelle personvernreglene. Det er imidlertid viktig at man har erstatningsregler som kan brukes ved konflikter på rettsområdet. Vi har ikke god nok kjennskap til hvordan japansk erstatningsrett fungerer til å kunne komme med noe fullgodt svar på om kravene oppfylles. Vi må derfor nøye oss med å konkludere med at det finnes regelverk som dekker de mest vanlige formene for erstatning også innenfor personvernretten.

4.3.4 Oppsummering

For at formålet med å beskytte personers grunnleggende interesser skal ivaretas, må det sikres at reglene om personvern faktisk etterleves. Som vi har sett kan kontroll med behandlingen og regler om sanksjoner bidra til at behandlingsansvarlige respekterer reglene. Oppreisning kan også ha en viss preventiv effekt overfor behandlingsansvarlige, og i tillegg være reparerende overfor den registrerte som ofte er den svake part i forholdet.

Kontrollordningene i de japanske reglene er svært forskjellige. På den ene siden har man *Management and coordination agency* som er et offentlig organ med ansvar gitt gjennom formell lov. MCA har sider som gjør det godt egnet til å ivareta rollen som kontrollorgan, men blir noe svekket av en tilsynelatende begrenset mulighet til å gripe inn i behandlinger. Det andre ytterpunktet er *Privacy award mark system* som er en frivillig ordning knyttet til de enkelte bransjene. Dersom PMS skal fungere er det helt avhengig av at bedrifter faktisk benytter seg av systemet, og at sekretariatet klarer å behandle innkommende saker på en effektiv måte. Organisasjonen og konfliktløsningsmetoden under ordningen er derimot godt utviklet, og vil nok langt på vei kunne fylle rollen som kontrollordning. Siden systemet er nytt gjenstår det å se hvordan det vil fungere i praksis, men det er en spennende tilnærming for hvordan kontroll kan utføres. Innsynsretten virker derimot å ha begrenset effekt som kontrollmulighet når man tar i betraktning de få forespørslene til forvaltningen om innsyn.

Personvernloven har bare en straffebestemmelse, men enkelte krenkelser av personvernet og privatlivets fred kan rammes av strafferettslige bestem-

melser. Finansdepartementet arbeider for eksempel med utkast til en lov vil øke straffene for urettmessig salg av kredittopplysninger.¹⁴² Sannsynligvis vil man ikke finne mange straffebud som rammer slike krenkelser, fordi man generelt har få sanksjoner for lovovertridelser i japansk rett og helst løser konflikter utenfor rettsapparatet.¹⁴³ Dette er en svakhet ved det japanske rettssystemet sett med vestlige øyne. Et eksempel er en sak fra 1997 hvor et tidsskrift publiserte bilder av en tenåring som var mistenkt i en drapssak. *Law on juveniles*¹⁴⁴ forbyr offentliggjøring av informasjon som kan føre til identifisering av ungdom under 19 år som er mistenkt i kriminalsaker. Brudd på loven medfører imidlertid ikke straff. Utgiver kunne ikke stilles til ansvar, men for å markere sin avsky overfor utgiver boikottet utsalgsstedene tidsskriftet og nektet å tilby det for salg.¹⁴⁵ Til tross for at publiseringen ikke fikk noen rettslige følger for utgiver, kan privates initiativ og ikke minst vanæren slikt medfører ha en viss effekt som sanksjon.

4.4 Hvem skal foreta beskyttelsesvurderingen?

EU-direktivet art. 25 krever at det blir foretatt en vurdering av beskyttelsesnivået i mottakerlandet før en overføring av personopplysninger kan finne sted. Denne vurderingen skal skje hos det landet som skal overføre personopplysningene. I det følgende skal vi drøfte hvem som foretar denne vurderingen, og hvordan vurderingen foregår.

4.4.1 Behandlingsansvarlig

4.4.1.1 Hvem er behandlingsansvarlig?

Det fremgår ikke av EU-direktivet art. 25 hvem som skal foreta vurderingen av et mottakerlands beskyttelsesnivå. Sett i sammenheng med direktivet art. 18 om meldeplikt til tilsynsmyndigheten, vil det imidlertid være naturlig at den behandlingsansvarlige i opprinnelseslandet må foreta en slik

¹⁴² Akagawa, Roy K. «When the law is toothless» *Asahi evening news*, Tokyo 12.-13. juli 1997

¹⁴³ Haley, J. O. «Sheathing the sword of justice in Japan: An essay on law without sanctions» Dean, Meryll (red) *Japanese legal system: Text and materials*, Cavendish publishing limited, London 1997:38-43

¹⁴⁴ Lov nr. 168 1948

¹⁴⁵ Akagawa, Roy K. «When the law is toothless» *Asahi evening news*, Tokyo 12.-13. juli 1997

vurdering. Etter direktivet art. 19 skal slik melding blant annet inneholde opplysninger om planlagte overføringer til utlandet.

Hvem som er behandlingsansvarlig er definert i direktivet art. 2 litra d: den fysiske eller juridiske person, offentlige myndighet, institusjon eller ethvert annet organ, der alene eller sammen med andre avgjør, til hvilket formål og med hvilke hjelpemidler der må foretages behandling af personopplysninger.

Det stilles altså ingen formelle krav til hvem som kan være behandlingsansvarlig. Som det fremgår eksplisitt av direktivet behøver ikke den behandlingsansvarlige å være en fysisk person. Men hvis en bedrift fremstår som behandlingsansvarlig, vil det være ledelsen som har det endelige ansvaret for behandlingen. Dette vil riktig nok være begrenset slik at bare juridiske personer med sivilprosessuell partsevne kan være behandlingsansvarlige. Bakgrunnen for dette er at partsevne er nødvendig dersom man må benytte seg av rettsapparatet for å gjennomføre et krav mot behandlingsansvarlig. I en organisasjon med løse struktur må man dermed peke ut en enkeltperson som utad fremstår som behandlingsansvarlig. Det kan også være flere som anses som behandlingsansvarlige, jf ordlyden alene eller sammen med andre. Dette kan være tilfellet ved for eksempel over- og underordnede organer, men man behøver ikke være del av den samme organisasjonsstruktur. Sett i EU-perspektiv kan et holdingselskap godt være ansvarlig for databehandling som skjer i flere medlemsland. Dette fremgår forutsetningsvis av direktivet art. 4 nr. 1 litra a.

Det er ikke noe krav om at de aktuelle data må være i den behandlingsansvarliges besittelse, det er plasseringen av bestemmelsesretten for behandlingen som er viktig. Det må imidlertid trekkes en grense mot den rene databehandling. Setter man behandlingen bort til andre, for eksempel ved outsourcing, vil den som behandler opplysningene falle inn under betegnelsen *registerfører* i direktivet art. 2 litra, men ansvaret vil forbli hos den opprinnelige behandlingsansvarlige.

4.4.1.2 Behandlingsansvarligs vurdering

Den behandlingsansvarlige skal vurdere om mottagerlandets regler sikrer et tilstrekkelig beskyttelsesnivå for behandling av personopplysningene. Et spørsmål som må drøftes er hvor grensene går for denne vurderingen. Lovteksten setter her ytterpunktene. Man må sørge for at en viss minstestandard opprettholdes, men ikke stille strengere krav enn det loven selv oppstiller. Problemet ligger i at det settet med kriterier som skal vurderes gir stor fleksibilitet, og det kan derfor være vanskelig for behandlingsansvarlig å vite hvor grensen går. I tillegg må den behandlingsansvarlige sette seg nøye inn i mottagerlandets lovgivning på personvernrettens område. Dette kan være problematisk fordi man ikke alltid støter på rettssystemer eller rettsregler som er

kompatible med de en har i hjemlandet. Kunnskapsnivået hos de forskjellige behandlingsansvarlige vil også være svært varierende i og med at enhver person kan fremstå som ansvarlig for behandlingen.

Et aktuelt spørsmål er om de avgjørelsene behandlingsansvarlig tar må være individuelle eller om man kan foreta en generell vurdering av et lands beskyttelsesnivå, og basere etterfølgende overføringer på dette grunnlaget. For en bedrift med utstrakt kontakt med et gitt tredjeland vil den siste tilnærmingen kunne være effektiv og tidsbesparende. De momentene som er gitt i direktivet art. 25 nr. 2 er såpass vage at behandlingsansvarlig må innrømmes et visst skjønn når avgjørelsen skal tas om overføring kan tillates. Et slikt skjønn bør bygge på en konkret vurdering av det enkelte tilfellet. Et annet moment er at kunnskapsnivået til den enkelte behandlingsansvarlig ikke kan forutsettes å være godt nok til å foreta en generell vurdering av mottakerlandets beskyttelsesnivå. I tillegg finnes det ingen mekanismer for å kommunisere slike generelle vurderinger til andre behandlere, og man kan dermed ende opp med en svært ulik praktisering av reglene. Sett i sammenheng synes det klart at behandlingsansvarlig bare kan fatte avgjørelser om overføring i konkrete tilfeller.

4.4.2 Tilsynsmyndigheten

Det vil være opp til det enkelte land å bestemme hvilke prosedyrer som skal følges på nasjonalt plan når det gjelder overførsel, og det vil også være landenes oppgave å bestemme hvilken myndighet som skal ta stilling til om et bestemt tredjeland har et tilstrekkelig beskyttelsesnivå.¹⁴⁶ Det mest naturlige vil være at det organet som overvåker overføringer av personopplysninger, er det samme som kontrollerer overholdelse av personvernlovgivningen generelt. Et organ som har oversikt over hvordan personvernet fungerer i praksis, vil ha best forutsetninger for å vurdere hvorvidt overføringer kan gjennomføres. Det vil være naturlig at denne kompetansen tilfaller tilsynsmyndigheten i medlemsstatene. For å illustrere dette vil vi se hvilken kompetanse Datatilsynet er gitt etter forslag til personopplysningslov.

4.4.2.1 Datatilsynets kompetanse

Datatilsynet har kompetanse til å føre kontroll med at lovens regler om behandling overholdes, jf personopplysningsloven § 42 tredje ledd nr. 3. Av dette følger det at Datatilsynet kan føre kontroll med at vilkårene for overføring til andre stater er oppfylt, og eventuelt nekte eller sette vilkår for overfø-

¹⁴⁶ NOU 1997:19 *Et bedre personvern* s. 99

ringen. Datatilsynets vurdering av overføringer etter personopplysningsloven § 29 vil først og fremst knytte seg til de konkrete overføringer. Kontrollen med overføring vil først og fremst skje gjennom meldeplikten etter personopplysningsloven § 31. Meldingen skal inneholde opplysninger om hvem personopplysningene vil bli utlevert til, herunder mottakere i andre stater, jf personopplysningsloven § 32 første ledd litra h. Datatilsynet kan dermed fra de mottar meldingen vurdere hvorvidt overføring kan skje. Tilsynet kan da ha en viss forhåndskontroll av de overføringer som skal foretas. Datatilsynets rett til å gripe inn i behandling som ikke er i overensstemmelse med loven etter personopplysningsloven § 42 tredje ledd nr. 3, tilsier at det også kan gripe inn i etterkant av en overføring. Etter personopplysningsloven § 46 kan Datatilsynet gi pålegg om at behandling skal opphøre eller stille vilkår til fortsatt behandling. En overføring som allerede har skjedd kan ikke stanses, men videre overføringer av samme type kan pålegges stanset.

Kan Datatilsynet vurdere andre staters beskyttelsesnivå på eget initiativ? Etter personopplysningsloven § 42 tredje ledd nr. 7 skal Datatilsynet *etter henvendelse eller av eget tiltak* gi uttalelse i spørsmål om behandling av personopplysninger. Det er ingen grunn til at denne uttalelsesretten ikke også skal omfatte personopplysningsloven § 29 om overføring. Det følger dessuten av EU-direktivet art. 25 nr. 3 at medlemsstatene skal underrette Kommisjonen dersom de mener at et tredjeland ikke oppfyller kravet til tilstrekkelig beskyttelse. Denne underrettelsesplikten vil også omfatte EFTA-statene.¹⁴⁷ Det er naturlig at slik underrettelse skjer gjennom den nasjonale tilsynsmyndighet, selv om man ikke kan utelukke at enkelte underrettelser av mer politisk karakter kan komme direkte fra de nasjonale regjeringer. En slik underrettelse forutsetter at en generell vurdering har blitt foretatt.

4.4.2.2 Datatilsynets vurdering

Hvor stor frihet gir denne muligheten? Kan Datatilsynet foreta en generell vurdering av en stats beskyttelsesnivå, gi denne virkning for alle overføringer og på den måten lage sin egen «hviteliste» over godkjente land? Personopplysningsloven inneholder ingen regler som regulerer dette. Den vurderingen Datatilsynet skal foreta skal imidlertid baseres på personopplysningsloven § 29 annet ledd som legger opp til en konkret vurdering i hvert enkelt tilfelle. Det er på det rene at mengden av meldinger til Datatilsynet vil øke betraktelig som et resultat av

¹⁴⁷ EØS-komiteéns beslutning nr. 83/1999 av 25. juni 1999 om endring av EØS-avtalens protokoll 37 og vedlegg XI (Telekommunikasjonstjenester), artikkel 2: *Avtalepartene skal innen rammen av EØS-komiteén utveksle de opplysninger det vises til i [EU-direktivet om personvern] artikkel 25 nr. 3 og artikkel 26 nr. 3 første ledd*

personopplysningsloven. Noe av bakgrunnen for dette er som nevnt i punkt 2.3, nemlig at det er behandlingen av personopplysninger som kommer i fokus og ikke registreringen. Selv om det ikke er noen plikt for Datatilsynet å foreta saksbehandling alle meldingene vil nok den utvidede veiledningsplikten etter § 42 tredje ledd nr. 6 føre til større arbeidsbyrde. Det kan derfor være effektivt å ha «hvitelister» som henvendelser og meldinger kan sjekkes opp mot, i stedet for å ta en konkret vurdering i hvert enkelt tilfelle. Imidlertid er det hensyn som taler mot dette. Avgjørelser som Datatilsynet fatter kan påklages til Personvernemnda etter personopplysningsloven § 42 fjerde ledd. Dette gjelder imidlertid bare avgjørelser fattet etter enkelte bestemmelser, og disse vil stort sett være enkeltvedtak i henhold til forvaltningsloven § 2 første ledd litra b.¹⁴⁸ Personopplysningsloven § 29 er ikke blant de bestemmelser det knyttes klageadgang til. En forklaring kan være at Datatilsynets vedtak om et mottakerlands tilstrekkelighetsnivå på generelt grunnlag neppe er et enkeltvedtak. Spørsmålet vil da være hvorvidt behandlingsansvarlig som rammes kan få omgjort denne avgjørelsen. Mye taler for at dersom beskyttelsesnivået skal avgjøres på generelt grunnlag, bør dette skje gjennom forskrift. Dette er også forutsatt i personopplysningsloven § 30 tredje ledd hvor det sies at: *Kongen kan gi forskrift om overføring av personopplysninger til utlandet, herunder om å stanse eller begrense overføring til bestemte stater som ikke tilfredsstiller kravene i § 29.*

Det finnes imidlertid mellomløsninger. Det vil være hensiktsmessig å supplere en generell godkjenning eller ikke-godkjenning med individuelle vurderinger for særtilfeller av overføringer. En annen mulighet er å tillate overføringer av visse typer informasjon, til visse formål eller til visse sektorer eller livsområder. Japan har for eksempel bare en lov som gjelder offentlig sektor. De retningslinjene som gjelder privat sektor er ofte svært spesifikke, og utelukkende knyttet opp mot en enkelt bransje. Det kan derfor være bedre å se på deler av Japans regler, og ut ifra dette foreta en generell vurdering. For eksempel at alle overføringer til offentlige organer tillates, eller at kredittopplysninger kan overføres i forbindelse med lånesøknader.

4.4.3 Kommisjonen

Kommisjonen består av 17 medlemmer som skal utføre sine verv i full uavhengighet og i Fellesskapets interesse, jf Romatraktaten art. 213 nr. 1 og nr. 2. Blant Kommisjonens oppgaver er å overvåke anvendelsen av bestemmelser truffet av organene med hjemmel i traktaten, jf Romatraktaten art. 211. Den kan også få myndighet av Europarådet til å gjennomføre de regler Rådet fastsetter, jf Romatraktaten art. 202. Kommisjonen er det øverste organet i vurde-

¹⁴⁸

Ot. prp. nr. 92 (1998-99) om lov om behandling av personopplysninger s. 132

ringen av om et land tilfredsstillende kravene i EU-direktivet art. 25. Den kan på selvstendig grunnlag vurdere hvorvidt et tredjeland har tilstrekkelig beskyttelse eller ikke, jf direktivet art. 25 nr. 4 og 6. Prosedyren for dette følger av direktivet art. 31.

4.4.3.1 Kommisjonens vurderinger

På samme måte som i drøftelsen ovenfor kan man stille spørsmål om Kommisjonens avgjørelser etter EU-direktivet art. 25 nr. 4 og 6 vil gjelde i konkrete eller generelle tilfeller. Begge punktene henviser til vurderingen i direktivet art. 25 nr. 2 som synes å ta utgangspunkt i at avgjørelsene bare kan fattes på konkret grunnlag. Hver sak må med andre ord avgjøres for seg. For et organ som Kommisjonen er dette ikke praktisk mulig. Etter direktivet art. 25 nr. 6 om godkjenning av et lands beskyttelsesnivå, sies det at avgjørelsen tas på grunnlag av mottagerlandets nasjonale lovgivning eller internasjonale forpliktelser. Internasjonale forpliktelser kan for eksempel være Europarådskonvensjonen om personvern. Mottagerlandets internasjonale forpliktelse kan også være slik som følger av direktivet art. 25 nr.5. Etter denne skal Kommisjonen innlede forhandlinger med land som blir vurdert til ikke å ha tilstrekkelig beskyttelse etter direktivet art. 25 nr. 4, for å avhjelpe denne situasjonen. Kommisjonen har også startet slike forhandlinger i forkant, for eksempel med USA i forbindelse med utvikling av *Safe harbour* prinsipper.¹⁴⁹

Vi har tidligere sett at andre kilder enn formell lov kan tas i betraktning etter tilstrekkelighetsvurderingen, se punkt 4.2.2.1. I direktivet art. 25 nr. 6 står det imidlertid at Kommisjonen tar sin avgjørelse på grunnlag av mottagerlandets *nasjonale lovgivning*. Innebærer det at Kommisjonen fatter sin avgjørelse kun basert på mottagerlandets formelle lovgivning? En slik forståelse vil gi Kommisjonen mindre spillerom, men vil forenkle vurderingsprosessen. Fordi det gjelder en *godkjennelse* av tilstrekkelighetsnivået er det mindre betenkelig å kun legge vekt på nasjonal lovgivning enn dersom man nekter overføring basert på samme regler. En godkjenning av et lands beskyttelsesnivå eller «hviteliste» er mest effektiv dersom den gjelder generelt for alle typer overføring til mottakerlandet. En slik generell vurdering gjøres best når landets regler er allmenngyldige, og dette vil stort sett være tilfellet med formelle lover. Dersom Kommisjonen kommer til at et lands beskyttelsesnivå er tilstrekkelig, betyr det at behandlingsansvarlig ikke behøver å foreta noen

¹⁴⁹ Director General XV *EU considers draft US «safe harbor» principles*, Brussel 30. april 1999
<http://europa.eu.int/comm/dg15/en/media/dataprot/news/harbor.htm> (28. mai 1999)

selvstendig vurdering. En «hviteliste» fra Kommisjonens side vil altså bare forenkle overføringsprosessen, men ikke hindre at overføringer kan skje i konkrete tilfeller. Likevel kan man stille spørsmålet om Kommisjonen bare skal inkludere land som oppfyller kravene til tilstrekkelighet ved lovgivning i alle sektorer eller om de kan godkjenne enkeltsektorer i mottakerlandet. Den første løsningen vil medføre at Japan ikke kan få et slikt godkjennelsesstempel fordi den formelle loven bare dekker offentlig sektor. Det andre alternativet vil føre til at Kommisjonen kan vurdere Japan til å ha tilstrekkelig vern i offentlig sektor, mens privat sektor ikke kan gis slik godkjenning fordi det ikke eksisterer lovgivning på området. Det vil imidlertid bli dårlig sammenheng mellom reglene dersom vurderingen etter direktivet art. 25 nr. 2 krever at man ser til alle forholdene, mens direktivet art. 25 nr. 6 begrenser vurderingen til lovgivningen i tredjelandet. Det mest hensiktsmessige vil være at Kommisjonen kan vurdere alle forhold i et mottagerland for å fastslå om et land har tilstrekkelig beskyttelse. Likeledes må Kommisjonen stå fritt til å ikke bare å godkjenne et land under ett, men til å fastslå tilstrekkelighet for enkelte sektorer eller typer av overføringer.

Dersom Kommisjonen finner at et tredjeland ikke innehar et tilstrekkelig beskyttelsesnivå skal enhver overføring av personopplysninger av samme art stanses, jf direktivet 25 nr. 4. Det er altså ikke et generelt forbud mot å overføre opplysninger til det aktuelle tredjelandet som sådan, bare i tilfeller der opplysninger av *samme art* overføres. Dette innebærer at utilstrekkelighet ikke nødvendigvis refererer seg til landets regler som en helhet, men kan begrenses til enkelte sektorer eller typer av overføring.

Det må imidlertid presiseres at avgjørelser etter direktivet art. 25 nr. 4 og 6 ikke skal tolkes antitetisk. Dersom Kommisjonen anser beskyttelsen som tilstrekkelig i telekommunikasjonsbransjen i Japan etter direktivet art. 25 nr. 6, betyr ikke det at alle andre mottagere i Japan ikke gir tilstrekkelig vern. Tilstrekkelighet eller utilstrekkelighet fastslås etter prosedyren i direktivet art. 31, og dersom ikke slik avgjørelse er tatt er det opp til behandlingsansvarligs og tilsynsmyndighetens skjønn hvorvidt en overføring kan foretas.

4.4.3.2 Må Kommisjonen avgjørelser om tilstrekkelighet følges?

Etter direktivet art. 25 nr. 4 og 6 følger det at medlemsstatene skal treffe de foranstaltninger som er nødvendig for å etterkomme Kommisjonens avgjørelser. De må altså rette seg etter Kommisjonens avgjørelser uten innsigelser. Medlemsstatene kan imidlertid foreta overføringer til land med utilstrekkelig beskyttelse med hjemmel i unntakene i direktivet art. 26. Og de kan nekte overføringer til land med tilstrekkelig beskyttelse dersom slik overføring vil være i strid med nasjonal lovgivning. For eksempel kan bestemmelser om

taushetsplikt i norsk rett være til hinder for at personopplysninger utleveres til andre, jf forvaltningsloven §§ 13 flg.¹⁵⁰ En overføring til utlandet av slike opplysninger kan være et brudd på taushetsplikten, og kan medføre straffeansvar, jf straffeloven §§ 121 og 144.¹⁵¹

Hvilken betydning får Kommisjonens beslutninger for Norge? Ifølge personopplysningslovens forarbeider er det nødvendig å avklare hvilken virkning Kommisjonens beslutninger skal ha for EFTA-landene.¹⁵² For Norge er det viktig å kunne stå fritt til å velge om Kommisjonens avgjørelser skal følges. Dette er blant de forhold som det ble forhandlet om før direktivet ble innlemmet i EØS-avtalen. At Norge ikke ønsker å bli bundet av avgjørelsene har blant annet sammenheng med at Norge ikke kan ta del i utvalget etter direktivet art. 31 som bistår Kommisjonen fordi deltakelse er forbeholdt EU-landene. Etter EØS-avtalen må Norge underrette Kommisjonen hvorvidt tiltakene som er vedtatt i henhold til EU-direktivet art. 25 nr. 4 og 6, og art. 26 nr. 3 og 4, vil bli anvendt i Norge eller ikke. Det siktes her til de foranstaltninger medlemsstatene må innføre for å etterkomme Kommisjonens avgjørelser om tredjelandets beskyttelsesnivå. Reservasjonen mot å anvende tiltakene gjelder imidlertid kun inntil EØS-komiteén eventuelt treffer beslutning om å innlemme tiltakene i EØS-avtalen. Innlemmes slike tiltak i avtalen, vil disse være bindende for Norge. Skjer slik behandling ikke innen 12 måneder etter at tiltaket trådte i kraft, kan Norge allikevel slutte å anvende tiltakene. Norge kan dermed stå fritt i forhold til Kommisjonens avgjørelser så lenge disse ikke er gjort til en del av EØS-avtalen. Slik unnlatelse har imidlertid sine konsekvenser. Velger Norge ikke å anvende tiltakene, vil de andre EØS-landene være unntatt fra direktivet art. 1 nr. 2 om at overføringer av personopplysninger ikke kan hindres til EØS-land. Andre EØS-land kan dermed innskrenke eller forby overføringer av personopplysninger til Norge. Imidlertid kan det virke som om overføring bare skal nektes der hvor Norge ikke treffer tiltak for å hindre overføring til land uten tilstrekkelig beskyttelse, jf avtaleteksten *ettersom disse tiltakene hindrer overføring til en tredjestat av opplysninger som nevnt*.¹⁵³ Ordlyden er uklar, men det kan bety at Norge kan nekte overføring til land som ifølge Kommisjonen sikrer tilstrekkelig beskyttelse. At Norge ikke overfører personopplysninger vil jo ikke medføre noen fare for personvernet, i motsetning til der hvor overføring skjer til land med dårlig personvernbeskyttelse.

¹⁵⁰ Lov om behandlingsmåter i forvaltningssaker av 10. februar 1967

¹⁵¹ Almindelig borgerlig Straffelov av 22. mai nr. 10 1902

¹⁵² Ot. prp. nr. 92 (1998-99) om lov om behandling av personopplysninger s. 15

¹⁵³ EØS-komiteéns beslutning nr. 83/1999 av 25. juni 1999 om endring av EØS-avtalens protokoll 37 og vedlegg XI (Telekommunikasjonstjenester), artikkel 2

Alle medlemsstatenes tilsynsmyndigheter er representert i *Arbeidsgruppen* opprettet etter EU-direktivet art. 29. Dens oppgave er å gi råd til Kommisjonen i ulike spørsmål knyttet til behandling av personopplysninger, jf art. 30, og det er således bare et rådgivende organ. Blant annet skal Arbeidsgruppen gi uttalelser om beskyttelsesnivået både innenfor Fellesskapet og i tredjeland til Kommisjonen, jf art. 30 nr.1 litra b. Per august 1999 foreligger det en uttalelse om beskyttelsesnivået i Sveits.¹⁵⁴ Kommisjonen er imidlertid ikke bundet av uttalelsene, men må i sin årsrapport gjøre rede for hvordan den har tatt hensyn til Arbeidsgruppens anbefalinger, jf art 30 nr. 5. Det har også blitt forhandlet om EFTA-landenes tilsynsmyndigheter skal få delta i Arbeidsgruppen,¹⁵⁵ og resultatet er at EFTA-landene har blitt tildelt observatør-status uten stemmerett.¹⁵⁶

¹⁵⁴ Avis 5/99 Concernant le niveau de protection des données à caractère personnel en Suisse, DG XV 5054/99 WP22, 7. juni 1999

¹⁵⁵ <http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp22fr.pdf> (12. august 1999)

¹⁵⁶ Ot. prp. nr. 92 (1998-99) om lov om behandling av personopplysninger s. 15
EØS-komiteens beslutning nr. 83/1999 av 25. juni 1999 om endring av EØS-avtalens protokoll 37 og vedlegg XI (Telekommunikasjonstjenester), artikkel 2

5. SAMMENFATNING OG VURDERING

Regler om beskyttelse av personopplysninger og privatlivets fred er ansett som nødvendige for ikke å krenke individets interessesfære. Personvern skal sikre enkelte av individets grunnleggende rettigheter. Hvor viktig man anser et slikt vern for å være og hvordan man velger å sikre vernet varierer fra land til land. EU har forsøkt å avhjelpe disse forskjellene med et felles personvern i Unionen, men det fører til at en del spørsmål i forhold til andre land må avklares.

Innholdsmessig er direktivet et godt utgangspunkt for regulering av personopplysninger. Reglene viser at EU tar personvern på alvor, og ønsker å holde et relativt høyt nivå på beskyttelsen. For å ivareta denne beskyttelsen er det nødvendig at overføring ut av EU også reguleres. Det betyr at borgernes rettigheter vil være sikret uansett hvor deres personopplysninger befinner seg. Formuleringen av bestemmelsen om overføring i direktivet art.-25 er imidlertid vag og åpner for mange spørsmål. På den ene side er det nødvendig med en fleksibel ordlyd for at samfunnsmessig- og teknologisk utvikling ikke skal løpe fra direktivet. På den annen side skaper den generelle ordlyden, og spesielt innføringen av begrepet *tilstrekkelig* usikkerhet om tolkingen og praktiseringen av reglene. Det blir derfor vanskelig å avgjøre hvilken norm man skal legge til grunn for vurderingen, og det kan stilles spørsmål om direktivet i så henseende faktisk vil bidra til å sikre et godt personvern.

Flere av de begrepene vi har drøftet er teknologiavhengige. Hva som anses som en overføring vil for eksempel endres med kommunikasjonsteknologien. Etter hvert kan det hende at begrepet vil miste sin betydning som saklig begrensning dersom enhver handling vil medføre en overføring. Flyktig transport via transittland, som vi så i punkt 3.1.1, er i realiteten en overføring, men omfattes ikke av direktivet. Det er en type overføring som ikke er styrt av mennesket, men av teknologien. Med fremtidige og mer intelligente informasjonssystemer kan kanskje grensen mellom menneskelig og maskinell styring hviskes ut, og dette må man ta hensyn til ved utarbeidelse og tolking av reglene.

En annen faktor er at teknologien gjør det enklere for hvem som helst å gjennomføre operasjoner som før bare var forbeholdt større aktører. Bruken av Internett er et eksempel i så måte, og representerer et fremtidig problem for personvernreglene. Mediet gjør det svært enkelt å foreta overføringer, og derfor er det nødvendig å øke den alminnelige bevisstheten rundt personvernsspørsmålene. Et eksempel er den kjente eks-presten Ludvig Nessa som truet med å publisere personalia på leger som utførte abortinngrep på sin hjemme-

side.¹⁵⁷ Denne siden er på norsk, men lokalisert i USA. Hvorvidt hans publisering ville vært i tråd med norsk lov er usikkert, men teknologien gjør det mulig at enhver kunne tilegne seg informasjonen samtidig som det ville være svært tungvint å forsøke å stoppe den.

Hva som defineres som personopplysninger vil også endres over tid. Forbedret datateknologi gir nye muligheter til å koble sammen eller samle inn informasjon. Ved bruk av Internett-tjenesten World Wide Web genereres det for eksempel informasjon om en selv uten at man vet om det. Elektroniske spor som i dag anses som anonyme kan i nær fremtid føre til identifikasjon av den enkelte bruker. Når man på denne måte ufrivillig gir fra seg informasjon blir det vanskeligere å kontrollere om man er registrert og dermed ivareta sine rettigheter.

De muligheter teknologien gir vil kreve at personvernretten er dynamisk, og man kan stille spørsmål ved om direktivet tar høyde for dette. For beskyttelse av personopplysninger i telekommunikasjonssektoren har man for eksempel vedtatt et eget direktiv.¹⁵⁸ Utviklingen kan bli at man får flere spesielle lover tilpasset de enkelte sektorer fordi det blir for vanskelig og for lite fleksibelt å regulere ved generell lov.

Ved overføring til tredjeland legger EU-direktivet opp til en løsning hvor det ikke skal foretas en forhåndsgodkjenning, men eventuelt må gripes inn i etterkant. Her har behovet for effektivitet og flyt skjøvet personvernet mer i bakgrunnen. På den annen side vil det føre til en merkelig løsning dersom man skal kreve full kontroll med overføringene. Da vi må få situasjon der ønsket om å verne de som behandles mot overvåking fører til at behandlerne overvåkes. Også forhåndskontroll av alle transaksjoner vil være i strid med direktivets formål om fri flyt, fordi det byråkratiet som må være tilstede vil hindre dette. Direktivet overlater derfor i stor grad etterlevelse av overføringsregelen til selvregulering hos behandlingsansvarlig. Initiativ for opprettholdelse av reglene må også ligge hos data subjektene, ved at man melder fra til kontrollmyndigheten når man mener at behandlingen ikke er forsvarlig. Kanskje vil øket tilgjengelighet og generell styrking av kontrollmyndigheten gjøre terskelen lavere for å rapportere overtramp? Man kan man stille spørsmål ved om det i det hele tatt er nødvendig å gripe inn dersom individet ikke plages med måten opplysningene blir brukt på. Dette forutsetter imidlertid at personen kjenner hele behandlingsbildet eller kan forutse misbruk av infor-

¹⁵⁷ NTB Nessa kartlegger leger som utfører abortinngrep 26. juni 1999

Vassnes, Hanne Borgen «- Leger kan få ei kule i nakken» *Dagbladet* 27. juli 1999

¹⁵⁸ European Parliament and Council Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector, direktiv 97/66/EF av 15. desember 1997

masjonen, noe som sjelden vil være tilfellet. Begrensningen av overføring må heller ikke være så effektiv at den forhindrer individets interesser. I vårt innledende eksempel var jo Peder Ås liv avhengig av at hans personopplysninger ble overført.

Hva *tilstrekkelig beskyttelse* innebærer er vanskelig å få tak på. Det er klart at man ikke skal kreve lik beskyttelse, samtidig som personvernet ikke skal forringes. Det må altså være et minimum av personvernregler hos mottaker, og spørsmålet er hvor den grensen går. For å kunne gi et mer konkret svar kreves det at man foretar en helhetlig overveielse av både mottakerlandets rett og forhold vedrørende de personopplysninger som skal overføres. Dette forutsetter at man har god innsikt og nok resursser. Den drøftelse som er foretatt her viser bare noen sider ved vurderingen, og kan derfor bare være rettleidende og påpeke problemer som oppstår ved vurderingen. Blant annet kan man stille spørsmål om hvor ofte man må foreta en vurdering av mottaker. Dennes beskyttelse kan endres ved nye regler og praksis, og også tolkingen av begrepet *tilstrekkelig* vil endres med samfunnsoppfatningen.

Viktig er det imidlertid at bestemmelsen praktiseres slik at ikke blir oppfattet som proteksjonisme av EUs indre marked. Kravet til at mottakerland må tilpasse seg direktivet for å få tilgang til markedet kan oppfattes som favoriserende og konkurransevridende. Fra USA og uoffisielt hold i Japan har blitt sagt at man vil vurdere å trekke EU inn for Verdens handelsorganisasjon (WTO) dersom overføringer blir stoppet til disse statene fordi man betrakter direktivet som en potensiell handelsbarriere.¹⁵⁹

En slik løsning vil være stikk i strid med direktivets uttalte formål. Det er imidlertid viktig at man ikke benytter direktivet for å skjerme egne økonomiske interesser. Praktiseringen av direktivet art. 25 må være relativt konsekvent, slik at man ikke kommer i en situasjon hvor man tillater overføring til land med klart svakere vern enn land man har funnet ikke har tilstrekkelig beskyttelse. Kommisjonen bør derfor utvikle en norm for vurderingen med klare kriterier. Her kan ordlyden igjen føre til problemer i og med at den er såpass uklar. Denne ubestemtheten er bestemmelsen i direktivet art. 25s svakhet, og den kunne vært klarere definert. I avhandlingen har vi drøftet hovedregelen om overføring til tredjeland, men det kan hende at unntakene i

¹⁵⁹ International Chamber of Commerce, « Privacy in the digital age », *Conference on Electronic Business: a roadmap for solutions* Budapest 29-30. October 1998.
http://www.iccwbo.org/home/conferences/reports/electronic_business_budapest/session2_budapest.asp

Se også Swire, Peter P. og Litan, Robert E. *None of your business – world data flows, electronic commerce and the European privacy directive*, The Brookings institute press, Washington D.C. 1998:189

direktivet art. 26 blir viktigere i praksis. Særlig muligheten til å inngå avtaler innenfor direktivets rammer vil kunne bidra til effektivitet samtidig som personvernet holdes i hevd. Faren ved bruk av unntakshjemler er imidlertid en uthuling av hovedregelen, og et mindre oversiktlig rettsbilde. Det internasjonale handelskammer (ICC) har utviklet en kontraktsmal for godkjenning etter direktivet art. 26 nr. 4 som er fremlagt for EU-Kommisjonen.¹⁶⁰ Hvorvidt denne vil få noen større utstrekning er for tidlig å si noe om. EU vil nok strekke seg langt for å godkjenne tredjeland, og man må håpe at det ikke går på bekostning av det vern direktivet ønsker å gi slik at det oppfattes som en papirtiger. Individenes rettigheter må ikke glemmes i vurderingen, for økonomiske hensyn kan lett for fremtredende. Man må imidlertid forvente at Kommisjonens tolking av direktivet art. 25 vil bli påvirket av politiske hensyn, og ikke være en ren juridisk vurdering. Den vurdering som behandlingsansvarlig og andre rettsanvendere skal foreta etter direktivet art. 25 må derimot bygge på en juridisk tolking.

Direktivets markering av personvern kan få en viktig verdi som incitament overfor andre stater til å regulere personvern. Fokus på beskyttelsen av individene kan øke bevisstheten hos myndigheter, kommersielle aktører og individer, og på sikt bidra til å styrke personvernet. Uansett vil direktivet ha effekt fordi det har startet en debatt, og har medført at flere stater har måttet vurdere sitt forhold til personvern og dermed ta et standpunkt. Verdens handelsorganisasjon kan også bli brukt som forhandlingsbord for fremtidige drøftelser om personvern i global skala.¹⁶¹

¹⁶⁰ International Chamber of Commerce, « Privacy in the digital age », *Conference on Electronic Business: a roadmap for solutions* Budapest 29-30. October 1998.
http://www.iccwbo.org/home/conferences/reports/electronic_business_budapest/session2_budapest.asp

¹⁶¹ Swire, Peter P. og Litan, Robert E. *None of your business – world data flows, electronic commerce and the European privacy directive*, The Brookings institute press, Washington D.C. 1998:189

ETTERORD

Denne avhandlingen ble ferdigstilt 15. september 1999, og vi vil her gi en kort oversikt over endringer i rettskildebildet siden den gang i Norge, EU og Japan.

Norge

Den norske personopplysningsloven av 14. april 2000¹⁶² trådte i kraft 1. januar 2001 med tilhørende forskrift.¹⁶³ Bestemmelsene vedrørende overføring til utlandet står uendret i forhold til lovforslaget som ble lagt til grunn i avhandlingen. Personopplysningsforskriften regulerer mer detaljert forholdet til beslutninger fra Kommisjonen vedrørende tredjelandets beskyttelsesnivå. Det fremkommer av forskriften § 6-2 at Datatilsynet skal sørge for at EU-kommisjonens beslutninger om at tredjeland har eller ikke har et tilfredsstillende beskyttelsesnivå for personvern etterleves, med mindre Norge har reservert seg mot beslutningen som nevnt i kapittel 4.4.3.2.

EU

Status for implementeringen av personverndirektivet

I kapittel 3.2.4 er det nevnt at Kommisjonen i juli 1999 avga en grunnlagt uttalelse til ni medlemsland fordi implementeringen av direktivet ikke var gjennomført. I januar 2000 ble Frankrike, Luxemburg, Nederland, Tyskland og Irland stevnet for EU-domstolen av Kommisjonen for manglende informasjon om fremdriften i implementeringsarbeidet.¹⁶⁴ Per august 2002 har Irland og Luxemburg ennå ikke gjennomført implementeringen.

¹⁶² Lov om behandling av personopplysninger av 14. april 2000 nr. 13
<http://www.lovdata.no/all/nl-20000414-031.html> (16. august 2002)

¹⁶³ Forskrift til personopplysningsloven av 15. desember 2000 nr. 1265 Arbeids- og administrasjonsdepartementet <http://www.lovdata.no/for/sf/aa/aa-20001215-1265.html> (16. august 2002)

¹⁶⁴ Data protection: Commission takes five member states to court, 11. januar 2000
http://www.europa.eu.int/comm/internal_market/en/dataprot/news/2k-10.htm (15. august 2002)

Godkjenning av tredjelandets beskyttelsesnivå

Som nevnt i kapittel 4.4.3 kan Kommisjonen foreta vurdering av et tredjelandets beskyttelsesnivå og godkjenne dette etter art. 25 nr. 6. Kommisjonen har foretatt slik vurdering for Sveits¹⁶⁵ og Ungarn¹⁶⁶ i juli 2000, og funnet deres beskyttelsesnivå tilstrekkelig. Dette innebærer at medlemslandene må følge disse beslutningene og tillate overføringer til tredjelandene med mindre det foreligger unntakssituasjoner hvor overføring allikevel kan nektes. Godkjennelsen kan endres dersom det foretas lovendringer i de aktuelle landene eller praksis viser at det allikevel ikke foreligger et tilstrekkelig beskyttelsesnivå.

I Norge følger det av personopplysningsforskriften § 6-2 at personopplysninger kan overføres til mottakere i Sveits og Ungarn. Datatilsynet kan forby overføringer for å beskytte den registrerte eller dersom det er overveiende sannsynlig at mottakeren ikke vil overholde mottakerlandets personvernregler og mottakerlandets myndigheter ikke vil behandle saken innen rimelig tid.

Den kanadiske *Personal information protection and electronic documents act* ble av Kommisjonen i desember 2001 ansett for å gi tilstrekkelig beskyttelse for enkelte typer overføringer.¹⁶⁷ Loven gjelder for organisasjoner underlagt føderal lovgivning som flyselskaper, jernbaner, shipping, banker, kringkasting, telefonselskaper m.fl. som innsamler og bruker personopplysninger om kunder og ansatte som del av sin økonomiske aktivitet. Omfattet er også organisasjoner som utleverer personopplysninger til vurdering utenfor en provins eller utenfor Canada. Fra 1. januar 2004 vil loven gjelde for alle kommersielle organisasjoner uavhengig av om de er underlagt føderal regulering eller ikke. Medlemsstatene er gjennom Kommisjonens beslutning bundet til å tillate overfø-

¹⁶⁵ Commission Decision 2000/518/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland - Official Journal L 215/1 of 25.8.2000
http://www.europa.eu.int/comm/internal_market/en/dataprot/adequacy/ch_00-518_en.pdf
 (15. august 2002)

¹⁶⁶ Commission Decision 2000/519/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary - O.J. L 215/4 of 25.8.2000
http://www.europa.eu.int/comm/internal_market/en/dataprot/adequacy/hu_00-519_en.pdf
 (15. august 2002)

¹⁶⁷ Commission Decision 2002/2/EC of 20.12.2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act - O.J. L 2/13 of 4.1.2002
http://www.europa.eu.int/comm/internal_market/en/dataprot/adequacy/canadadecisionen.pdf
 (15. august 2002)

ringer til nevnte organisasjoner i Canada.¹⁶⁸ Loven omfatter ikke offentlige organer eller ikke-kommersielle private organisasjoner, og overføring av personopplysninger til disse krever at den EU baserte behandleren sørger for sikkerhetsordninger før overføring skjer, for eksempel ved å bruke standardkontrakten utarbeidet av Kommisjonen.

Safe Harbour avtalen

EU-kommisjonen har gjennom forhandlinger med amerikanske myndigheter blitt enige om såkalte Safe Harbour-prinsipper som amerikanske virksomheter kan slutte seg til på frivillig basis. De vil i såfall anses for å ha et tilstrekkelig beskyttelsesnivå etter personvern direktivet. Denne avtalen har kommet istand fordi USA ikke har føderal personvernlovgivning som gjør det mulig å godkjenne USA etter art. 25 nr. 6. De virksomheter som undertegner Safe Harbour prinsippene vil være bundet av disse, og Federal Trade Commission og andre amerikanske offentlige organer vil ha tilsyn med at prinsippene overholdes.¹⁶⁹ Godkjennelsen av Safe Harbour prinsippene er imidlertid ikke en generell godkjennelse av personvernnivået i USA. På samme måte som ved godkjennelsen av Sveits og Ungarn må medlemsstatene tillate overføringer til virksomheter i USA som er tilsluttet Safe Harbour.

Det følger av personopplysningsforskriften § 6-3 at det kan foretas overføring av personopplysninger fra Norge til mottakere i USA selv om vilkårene i personopplysningsloven §§ 29 og 30 ikke er oppfylt dersom mottakeren forplikter seg til å oppfylle kravene i Kommisjonens beslutning som godkjenner Safe Harbour prinsippene. Også her kan Datatilsynet gripe inn og forby en overføring dersom bestemte situasjoner foreligger.

Standardkontrakt

Personvern direktivet artikkel 26 nr. 2 gir hjemmel for at medlemslandene kan tillate overføring til tredjeland uten tilstrekkelig beskyttelse dersom visse garantier er oppfylt. Slike garantier kan følge av avtale mellom den som innehar personopplysningene i EØS-landet og mottakeren i tredjelandet. EU-

¹⁶⁸ Data protection: Commission recognises adequacy of Canadian regime, 14. januar 2002 http://www.europa.eu.int/comm/internal_market/en/dataprot/news/02_46.htm (15. august 2002)

¹⁶⁹ Commission Decision 2000/520/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce - Official Journal L 215/7 of 25.8.2000 http://www.europa.eu.int/comm/internal_market/en/dataprot/adequacy/dec2000520ec.pdf (15. august 2002)

kommisjonen vedtok i desember 2001 en standardkontrakt som kan benyttes ved overføring av personopplysninger til mottaker i tredjeland som ikke har et tilstrekkelig beskyttelsesnivå.¹⁷⁰

Standardkontrakten gjelder kun beskyttelse av personopplysningene, mens eksportøren og importøren av opplysningene fritt kan legge til bestemmelser som vedrører kommersielle forhold mellom partene. Bestemmelsene anses for å gi passende garantier ved overføring med hensyn til de gunnleggende rettigheter som følger av personverndirektivet. Dette er kun anbefalinger slik at behandlingsansvarlig som skal overføre personopplysninger til tredjeland med utilstrekkelig beskyttelse ikke er pliktig til å benytte disse. Imidlertid vil den behandlingsansvarlige etter personverndirektivet artikkel 26 nr. 2 være forpliktet til å sørge for at mottaker i tredjelandet ivaretar personvernet, og dersom man benytter den standardkontrakten som er anbefalt av EU-kommisjonen vil man være sikker på at man oppfyller direktivets krav på dette punkt.¹⁷¹

Japan

Oppmerksomheten rundt personvern har i Japan blitt større de siste årene. Den tekniske utviklingen muliggjør en annen bruk av personopplysninger enn det dagens lovgivning regulerer og behovet for å regulere privat sektor har dermed økt. En ny lov *The act for the protection of personal data* ble godkjent av regjeringen 27. mars 2001. Lovforslaget er oversendt nasjonalforsamlingen hvor det fremdeles er til behandling, men det er forventet at loven vil tre i kraft i april 2003. Det foreligger ingen engelsk versjon av lovutkastet slik at vi ikke har kunnet foreta en nærmere vurdering, men basert på tilgjengelig informasjon om utkastet følger en oversikt over lovens innhold.¹⁷²

¹⁷⁰ Data protection: Standard contractual clauses to facilitate personal data transfers to third countries for processing Countries, 22. januar 2002
http://www.europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/02-16_da.pdf
 (15. august 2002)

¹⁷¹ Standardkontraktene er tilgjengelig for nedlast fra Datatilsynets nettsider
<http://www.datatilsynet.no>

¹⁷² Bill on data protection approved by Cabinet, *The Japan Times Online* 28. mars 2001
<http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20010328a3.htm> (15. august 2002)
 og Hiramatsu, Takemi: "New Japanese Proposed Legislation Regarding Protection of Personal Data" 7. mai 2001
http://www.haledorr.com/db30/cgi-bin/pubs/2001_05_IP_Session_Asahi.pdf

Loven skal omfatte all behandling av personopplysninger uavhengig av om behandlingen foretas i privat eller offentlig sektor basert på følgende prinsipper:

- Formålet med behandlingen må spesifiseres og behandlingen må holdes innenfor dette formålet.
- Innsamlingen av opplysningene må foretas på en lovlig måte
- Opplysningene skal være korrekte og oppdaterte.
- Det skal være adekvat informasjonssikkerhet ved behandling av personopplysningene.
- Den registrerte skal sikres innsyn og kan kreve retting eller sletting.
- Personopplysningene skal ikke utleveres til en tredjepart uten den registrertes samtykke eller hvor slik utlevering følger av lov.
- Behandler må ha et system for å motta og besvare klager.

Med unntak for bestemmelsene om innsamling av opplysninger er pressen samt bruk av personopplysninger for forskning, akademiske aktiviteter og religiøse og politiske aktiviteter unntatt fra loven.

Enkelte forvaltningsorganer vil ha kompetanse til å utstede retningslinjer for behandling av personopplysninger. Dersom behandlingsansvarlig bryter loven eller ikke følger pålegg kan det medføre fengselsstraff på inntil seks måneder eller bot inntil JPY 300.000.¹⁷³

Det er flere detaljer som vi ikke har kommet inn på, men lovutkastet fremstår som veldig likt personverndirektivet. Som nevnt avslutningsvis i kapittel 5 kan personverndirektivet være et incitament for andre stater til å gi vern for personopplysninger, og gjennom det japanske lovutkastet ser man at personverndirektivet ligger til grunn både for terminologi og prinsipper. Det vil ikke være overraskende dersom utformingen av lovteksten delvis er styrt av kravet til tilstrekkelig beskyttelse i personverndirektivet.

¹⁷³ JPY 300.000 tilsvarer ca. NOK 20000 per 15. august 2002.

BIBLIOGRAFI

- Akagawa, Roy K. «When the law is toothless» *Asahi evening news*, Tokyo 12.-13. juli 1997
- Arnesen, Finn; Borgli, Anneke B.; Bull, Henrik; Foyn, Stein; Rognstad; Ole-Andreas og Stemshaug; Helge *Oversikt over EØS-retten*, (1. utgave) Universitetet i Oslo, Oslo 1994
- Blekeli, Dag Ragnar og Selmer, Knut S *Data og personvern*, Universitetsforlaget, Oslo 1977
- Blume, Peter «Om den skandinaviske registrelovgivning» *Tidsskrift for rettsvitenskap* 2/87
- Chafee, Judy og Repeta, Lawrence *Japanese government information: New rules for access*, Japan information access project, Washington D.C. juni 1998
<http://www.nmjc.org/jiap/specrpts/joho.html> (13. september 1999)
- Cullen international (red) *A business guide to changes in European data protection legislation*, Kluwer law international, Den Haag 1999
- Dangelmaier, Wilhelm *Protection of personal data and privacy in Japan*, Heinz Nixdorf Institut
<http://hni.uni-paderborn.de/cim/datenschutz/seiten/Japan1.html> (28. mai 1999)
- Dean, Meryll (red) *Japanese legal system: Text and materials*, Cavendish publishing limited, London 1997
- Djønne, Eirik (red) *Datatilsynet – ti år som personvernets vokter*, Complex 4/90 TANO, Oslo 1990
- Djønne, Eirik; Grønn, Tove og Hafli, Tor *Personregisterloven med kommentarer*, TANO, Oslo 1987.
- Eckhoff, Torstein *Rettskildelære*, (3. utgave) TANO, Oslo 1993
- Franklin, Charles E. H. (red) *Business guide to privacy and data protection legislation*, Kluwer law international, Den Haag 1996
- Greenleaf, Graham «A proposed privacy code for Asia-Pacific cyberlaw» *Emerging law on the electronic frontier, Journal of computer mediated communication*, volume 2 nr. 1: Part 1 of a special issue June 1996, Harvard university program om information resources policy.
<http://jcmc.mssc.huji.ac.il/vol2/issue1/asiapac.html> (28. mai 1999)
- Greenleaf, Graham «European privacy directive and data exports» *Privacy law & policy reporter*, volume 2 nr. 6/1995.
Også publisert på

- <http://www.austlii.edu.au/au/other/plpr/Vol2No06/v02n06b.htm> (20. juli 1999)
- Greenleaf, Graham «The European privacy directive – completed» *Privacy law & policy reporter*, volume 2 nr. 5/1995.
Også publisert på
<http://www.austlii.edu.au/au/other/plpr/Vol2No06/v02n06b.htm> (20. juli 1999)
- Greenleaf, Graham «Towards an Asia-Pacific information privacy convention» *Privacy law & policy reporter*, volume 2 nr. 7/1995.
Også publisert på
<http://www.austlii.edu.au/do/disp.pl/au/other/plpr/Vol2No07/v02n07c.htm> (28. mai 1999)
- Grindin, Susan E. *As the cyber-world turns: The European Union's data protection directive and trans-border flow of personal data*, 24. januar 1998.
<http://www.info-law.com/eupriv.html> (28. mai 1999)
- Haley, J. O. «Sheathing the sword of justice in Japan: An essay on law without sanctions» Dean, Meryll (red) *Japanese legal system: Text and materials*, Cavendish publishing limited, London 1997:38-43
- Hiramatsu, Tsuyoshi «Telecommunication in Japan: Non-protection of privacy» *The international computer lawyer*, volume 1 nr. 3, februar 1993.
- Horibe, Masao «Access to information and privacy legislation in Japan» *Transnational data and communications report*, 14TRD nr. 6, november/desember 1991.
- Horibe, Masao «Making Freedom of information laws in Japan – an academic lawyer's experience» *Hitotsubashi journal of law and politics* 20/1992 s. 33-45.
- Horibe, Masao «The information society and privacy: Current state of personal data protection in Japan» *JIPDEC Informatization Quarterly: The information society and privacy* JIQ nr. 115/1998:3-15
- Horibe, Masao *The protection of privacy and personal data in Japan*, presentert ved Privacy protection in a global networked society – an OECD workshop, Paris 16.-17. februar 1998
- Japan almanac 1999*, Asahi shimbun, Tokyo 1998
- Jarbekk, Eva I. E. Personvern og overføring av personopplysninger til utlandet, Complex 4/96 TANO, Oslo 1996
- Johansen, Per Anders «Nektet å utveksle beviser», *Aftenposten (Morgen)* 18. desember 1998:2
- Kagge, Gunnar «... men Kevin tjener bare 60-70 kr», *Aftenposten (Morgen)* 9. september 1999:41

- Kapteyn, P. J. G. og Verloren van Themaat, P. *Introduction to the law of the European Communities – After the coming into force of the Single European act*, (2. utgave) Kluwer law and taxation publishers, Deventer 1989
- Kawashima, T «Japanese way of legal thinking» Dean, Meryll (red) *Japanese legal system: Text and materials*, Cavendish publishing limited, London 1997:163-165
- Knudsen, Håkon *Kommentarer til personregisterloven*, Student Karnov – norsk kommentert lovsamling, (utgave 19) Karnovs forlag AS, Oslo 1996:bind 2 s. 1801 flg.
- Kvilesjø, Svend Ole «330000 norske e-postkasser åpne på nettet i går» *Aftenposten (Morgen)* 31. august 1999:2
- Lassen, Birger Stuevold (red) *Knophs oversikt over Norges rett*, (10. utgave) Universitetsforlaget, Oslo 1993
- Management and Coordination Agency *Summary of the 1996 Annual report*, Tokyo <http://www.somucho.go.jp/soumu/eha000.htm> (19. august 1999)
- Matsumoto, Tsumo *The development and future challenges of self-regulation in Japan, with special regard to electronic commerce*, revised version of paper presented at 25th anniversary conference of the Advertising standards authority of New Zealand, Wellington april 1998.
<http://www.law.kyushu-u.ac.jp/~luke/ecommerce.html> (28. mai 1999)
- Matsushita, M «International trade and competition law in Japan» Dean, Meryll (red) *Japanese legal system: Text and materials*, Cavendish publishing limited, London 1997:194-204
- Ministry of International Trade and Industry «Handbook concerning protection of personal data» *JIPDEC Informatization Quarterly: The information society and privacy* JIQ nr. 115/1998:33-61
- Ministry of International Trade and Industry «Privacy mark award system» *JIPDEC Informatization Quarterly: The information society and privacy* JIQ nr. 115/1998:27-32
- Noda, Yosiyuki *Introduction au droit japonais*, Libraire Dalloz, Paris 1966
- Noda, Yosiyuki *Introduction to Japanese law*, University of Tokyo Press, Tokyo 1976
- NTB Nessa kartlegger leger som utfører abortinnngrep 26. juni 1999
- Oda, Hiroshi *Japanese law*, Butterworth & Co, London 1992
- Petersson, Roger og Reinholdsson, Klas *Personuppgiftslagen i pratiken*, Nordstedts Juridik AB, Stockholm 1998
- Swire, Peter P. og Litan, Robert E. None of your business – world data flows, electronic commerce and the European privacy directive, The Brookings institute press, Washington D.C. 1998
- Uten navn «Amazon avslører lesevaner» VG 3. september 1999
<http://www.vg.no/pub/vgart.hbs?artid=2748580> (6. september 1999).

Uten navn «Privacy of personal data assured – Kanagawa ordinance on protecting personal data formulated» *The Kanagawan*, volume 37 nr. 1, april/mai 1990.

Uten navn «Rights to send and receive information freely to be recognizes as fundamental human rights» *Telecom tribune* volume 10 issue 12, februar 1996. Også publisert på
<http://www.telecomtribune.com/1996issues/TT9602/TT11A.HTM>
(23. august 1999)

Vassnes, Hanne Borgen «- Leger kan få ei kule i nakken» *Dagbladet* 27. juli 1999

Young, Michael K «Administrative guidance in the courts: A case study in doctrinal adaption» Fujikura, Koichiro (red) *Japanese law and legal theory*, Dartmouth publishing compant limited, Aldershot 1996:143-175

Utredninger og uttalelser

European Commission Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: Test of the method on several categories of transfer (final report), Tender nr. XV/97/18/D, Edinburgh september 1998
<http://europa.eu.int/comm/dg15/en/media/dataprot/studies/adequat.htm>
(1. juni 1999)

EØS-komiteens beslutning nr. 83/1999 av 25. juni 1999 om endring av EØS-avtalens protokoll 37 og vedlegg XI (Telekommunikasjonstjenester)

Ministry of post and telecommunication Privacy and information security: Report from the Japanese study group on electronic information and network utilisation, MPT News, volume 6 nr. 13, Tokyo oktober 1995

NOU 1997:19 Et bedre personvern – forslag til lov om behandling av personopplysninger

Ot. prp. nr. 92 (1998-99) om lov om behandling av personopplysninger

SOU 1997:39 Integritet, offentlighet, informasjonsteknik. Betänkande av Datalagskommittén, Stockholm 1997

Working party on the protection of individuals with regard to the processing of personal data:

- *Avis 5/99 Concernant le niveau de protection des données à caractère personnel en Suisse*, DG XV 5054/99 WP22, Brussel 7. juni 1999
<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp22fr.pdf> (12. august 1999)
- Discussion document: First orientation on transfers of personal data to third countries – possible ways forward in assessing adequacy, DG XV D/5020/97 WP4, Brussel 26. juni 1997
<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp4en.htm> (1. juni 1999)
- Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government, Brussel 26. januar 1999
<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp15en.htm> (28. mai 1999)
- Opinion 2/99 on the Adequacy of the «International Safe Harbor Principles» issued by the US Department of Commerce on 19th April 1999, Brussel 3. mai 1999
<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp19en.htm> (1. juni 1999)
- Working document: Judging industry self-regulation – when does it make a meaningful contribution to the level of data protection in a third country? DG XV D/5057/97 final WP7, Brussel 14. januar 1998
<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp7en.htm> (1. juni 1999)
- Working document: Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries, DG XV D/5005/98 WP9, Brussel 22. april 1998
<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp9en.htm> (1. juni 1999)
- *Working document: Processing of personal data on the Internet*, Brussel 23. februar 1999
<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp16en.htm> (28. mai 1999)
- Working document: Transfers of personal data to third countries – applying articles 25 and 26 of the EU data protection directive, DG XV D/5025/98 WP12, 24. juli 1998
<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp12en.htm> (1. juni 1999)

Lover og retningslinjer m.m.

Act for the protection of computer processed personal data held by administrative organs, 16. desember 1988 nr. 95

Avtale mellom EFTA-statene om opprettelse av et Overvåkingsorgan og en Domstol (ODA-avtalen) av 2. mai 1992

Avtale om Det europeiske økonomiske samarbeidsområde (EØS-avtalen) av 2. mai 1992

Council of Europe *Convention for the protection of individuals with regard to automatic processing of personal data 108/81*

<http://www.coe.fr/neg/legaltxt/108e.htm> (15. juli 1999)

Cyber business association *Guidelines for protecting personal information in cyber business*, Tokyo 17. desember 1997

<http://www.iiijnet.or.jp/fmmc/501e.html> (28. mai 1999)

Electronic commerce promotion council *Guidelines concerning the protection of personal data in electronic commerce in the private sector*, Tokyo mars 1998 http://ecom.ecom.or.jp/eng/output/wg12/privacy_guideline.htm (1. juni 1999)

Electronic network consortium *Guideline for protecting personal data in electronic network management*, Tokyo 3. desember 1997

<http://www.nmda.or.jp/enc/privacy-rev-english.html> (2. juni 1999)

Europa-parlamentets og rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling af personopplysninger og om fri udveksling af sådanne opplysninger

http://europa.eu.int/eur-lex/da/lif/dat/1995/da_395L0046.html (9. juli 1999)

Japanese Bankers Association *Privacy protection, Personal credit information center*, Tokyo <http://www.zenginkyo.or.jp/en/pcic/pcic05.htm> (8. juli 1999)

Japan information service industry association *Guidelines concerning the protection of computer processed personal data in the information service industry in Japan*, Tokyo 26. november 1997

<http://www.jisa.or.jp/statistics/JISAprivacyguideline-e.htm> (21. september 1998)

Konsolideret udgave af Traktaten om opprettelse af det Europæiske Fællesskab (Romatraktaten),

Europæiske Fællesskabers Tidende C 340 av 10. november 1997 s. 173-308
http://europa.eu.int/eur-lex/da/treaties/Datatilsynet/e_cons_treaty_da.pdf (9. september 1999)

Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven) av 27. november 1992 nr. 102

Lov om personregistre m.m av 9. juni 1978 nr. 48
<http://www.datatilsynet.no/lov/loven/LOVEN.htm> (9. juli 1999)

Ministry of International Trade and Industry *Guidelines concerning the protection of computer processed personal data in the private sector*, Notification nr. 98 av 4. mars 1997
<http://hni.uni-paderborn.de/cim/datenschutz/seiten/Japan2.html> (8. juli 1999)

Ministry of Post and Telecommunications *Guidelines on the protection of personal data in telecommunications business*, Tokyo 2. desember 1998
http://www.mpt.go.jp/whatsnew/guideline_privacy-e.html (29. mai 1999)

Organisation of Economic Co-operation and Development *Guidelines concerning the protection of privacy and transborder flows of personal data*, 23. september 1980
<http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM> (9. juli 1999)

Annet

Advanced Information and Telecommunications Society Promotion Headquarters Report of working group on electronic commerce: A Japanese initiative in promoting electronic commerce (provisional translation), Tokyo juni 1998

Cyber Business Association Notice from the Privacy and security working group report: Creation of Guidelines for protecting personal information in cyber business, Tokyo 17. desember 1997
<http://www.ijnet.or.jp/fmmc/501e.html> (28. mai 1999)

Director General XV *Data protection: Background information*, Brussel 3. november 1998
<http://europa.eu.int/comm/dg15/en/media/dataprot/backinfo/info.htm> (28. mai 1999)

Director General XV *Directive on personal data protection enters into effect*, Brussel 23. oktober 1998

<http://europa.eu.int/comm/dg15/en/media/dataprot/925.htm> (29. mai 1999)

Director General XV *EU considers draft US «safe harbor» principles*, Brussel 30. april 1999

<http://europa.eu.int/comm/dg15/en/media/dataprot/news/harbor.htm> (28. mai 1999)

Director General XV *Status of implementation of Directive 95/46*, Brussel 12. mai 1999.

<http://europa.eu.int/comm/dg15/en/media/dataprot/law/impl.htm> (29. mai 1999)

Director General XV *Technical briefing for journalists on data protection – EU/US dialogue*, Brussel 10. desember 1998

<http://europa.eu.int/comm/dg15/en/media/dataprot/backinfo/euus.htm> (28. mai 1999)

Electronic Commerce Promotion Council *Report from the working group on privacy issues*, Tokyo

<http://www.ilpf.org/confer/present/sakusa2.htm> (28. mai 1999)

Electronic Network Consortium *Revision of Guildelines for protecting personal data in electronic network management – For network management in the internet age*, Tokyo 3. desember 1997

<http://kasumi.nmda.or.jp/enc/privacy-press-english.html> (oktober 1998)

International Chamber of Commerce «Privacy in the digital age», *Conference on Electronic Business: a roadmap for solutions* Budapest 29-30. oktober 1998

http://www.iccwbo.org/home/conferences/reports/electronic_business_budapest/session2_budapest.asp (10. september 1999)

Ministry of post and telecommunications *Public comment for the revised version of Guidelines on the protection of personal data in telecommunications business (draft)*, Tokyo 3. september 1998

<http://www.mpt.go.jp/pressrelease/english/telecomm/news980903.html> (april 1999)

Ministry of post and telecommunication *Report of Study group on privacy protecting in telecommunications services (an outline)*, Tokyo 26. oktober 1998

http://www.mpt.go.jp/policyreports/english/group/telecommunications/privacy_protect981026.html (29. mai 1999)

THE ACT FOR PROTECTION OF COMPUTER-PROCESSED PERSONAL DATA HELD BY ADMINISTRATIVE ORGANS

10 October 1989

Chapter 1 General Provisions

Article 1 Purpose

The purpose of this Act is, in view of the development of computer processing of personal data in administrative organs, to protect the rights and interests of individuals while insuring the proper and smooth operation of public administration, by providing for basic rules concerning the handling of computer-processed personal data held by administrative organs.

Article 2 Definitions

For the purpose of this Act, the meaning of the terms set forth in the following subparagraphs shall be provided for in the said paragraphs:

1) the term "administrative organs" means:

(a) a national administrative organ as provided for in Article 3 paragraph 2 of the National Government Organisation Law (Law No. 120 of 1948) and an organ established under the jurisdiction of the Cabinet under the provision of law (unless the organ established is considered an extraordinary organisation as designated by the Cabinet Order referred to in (b) below, then it shall be excluded).

(b) an organisation designated by Cabinet Order from among the extraordinary organisations as referred to in Article 8-3 of the National Government Organisation Law;

2) the term "personal data" means data which relate to a living individual and ones where the individual can be identified from a name, date of birth or other descriptions contained in the data or from a number, symbol or other mark assigned to the individual (including data where the individual cannot

be identified from the information alone, but may be identified by easily collating the data with other information). They exclude however, data concerning directors of a corporation or other organisation as contained in the data recorded with regard to corporations or other organisations.

3) The term "computer processing" means the inputting, storage, editing, working, modifying, updating, retrieval, erasure and outputting of data or any other similar processing by means of computer operations. It excludes, however, such processing solely for the purpose of preparing the text of documents or for recording the contents of documents and pictures and any other processing as designated by Cabinet Order.

4) The term "personal data file" means a group of personal data compiled systematically for accomplishing the aim of certain functions, which should be recorded in a magnetic tape, magnetic disk or any other similar medium capable of keeping certain items securely recorded (hereinafter referred to as "magnetic tape etc.") for the purpose of computer processing.

5) The term "processed data" means personal data recorded in a personal data file.

6) The term "data subject of the processed data" means an individual whose identity can be retrieved in computer processing without referring to any other individual's name, date of birth, other descriptions, or numbers, symbols, other marks assigned to another individual, among individuals identified by the processed data.

Article 3 Exclusion

The provisions of this law shall not apply to personal data collected for compiling the designated statistics as provided for in Article 2 of the Statistics Law (Law No. 18 of 1947), and to personal data collected by the statistical survey which was notified to the Director-General of the Management and Coordination Agency under the provision of Article 8 paragraph 1 of the same Law, and those obtained by collection of statistical reports (limited to the part relating to items as used solely for compiling statistics, and mentioned in the application form provided for in Article 4, paragraph 2 of the Statistical Reports Coordination Law (Law No. 148 of 1952)) which were approved by the Director-General of the Management and Coordination Agency under the provisions of the same Law.

Chapter 2 Computer Processing of Personal Data

Article 4 Holding of personal data files

(1) An administrative organ shall, in holding a personal data file (meaning the compiling or obtaining and maintaining of a personal data file for use or its own function, including entrusting all or part of computer processing of personal data to others, and not including the case where it does so by being entrusted by others. The same shall apply hereinafter), confine itself to the extent necessary to perform the competent function provided for by law, and specify the purpose of such holding as much as possible.

(2) The extent of items to be recorded in the personal data files (hereinafter referred to as "file record items") and the extent of individuals to be recorded in the personal data files as the subject of the processed data (hereinafter referred to as "file record extent") shall not exceed the limit necessary for accomplishing the purpose of holding the personal data file as specified by the preceding paragraph (hereinafter referred to as "file-holding purpose").

Article 5 Security etc. of personal data

(1) When an administrative organ conducts computer processing of personal data, or punching or other preparatory work for inputting data or keeping magnetic tapes etc. (hereinafter referred to as "computer processing etc. of personal data"), the head of the administrative organ (meaning the person designated by Cabinet Order (b) of Article 2 subparagraph 1. The same shall apply hereinafter) shall strive to take measures necessary for prevention of leakage, loss, destruction of personal data or other proper measures (hereinafter referred to as "measures for security").

(2) The head of an administrative organ which holds a personal data file (hereinafter referred to as "holding organ") shall strive to ensure that the processed data should correspond with past or present facts within the extent necessary for the fileholding purpose.

Article 6 Prior notification with regard to holding a personal data file etc.

(1) When an administrative organ intends to hold a personal data file, the head of the administrative organ shall notify in advance the Director-General of the Management and Coordination Agency of the matters set forth in the following subparagraphs. When it intends to modify the notified matter, the head of the administrative organ shall also notify in advance the Direc-

tor-General of the Management and Coordination Agency of the matter to be modified:

- 1) the name of the personal data file;
- 2) the name of the holding organ and the name of the organisation which is in charge of the function for which the personal data file is used;
- 3) the purpose of the file-holding,
- 4) items in the file record and the extent of the file record;
- 5) the method of collecting the processed data;
- 6) when it provides routinely the processed data to any person other than the holding organ, the name of the person to whom the data are provided;
- 7) with regard to a personal data file which is entered in the personal data files directory, the name and location of the organisation which accepts the requests under the provision of the first clause of Article 13 paragraph 1, under the provision of paragraph 1 of the following Article (excluding ones which are set forth in the provision of Article 13 paragraph 1 and ones that are of processed data of which the first clause of Article 13 paragraph 1 is not to be applied to all of the processed data under the provision of Article 19);
- 8) when it decides under the provisions of paragraph 2 of the following article not to enter in the personal data files directory parts of the file record items or items set forth in subparagraph 5 or 6, or when it decides under the provision of paragraph 3 of the same article not to enter in the personal data files directory a personal data file, the description to that effect;
- 9) in the case of a personal data file to which requests under the first sentence of Article 13 paragraph I cannot be made because it shall fall under the provision of paragraph 1 of Article 13, the description to that effect;
- 10) in accordance with the provisions of other laws or orders thereunder, when all or part of the contents of the processed data appear in a licence, permit, notice or other document, and it has already been issued to the data subject of the processed data, when all or parts of the contents of the processed data have been published or made available i.e. for public inspection, when the data subject of the processed data may make a request that he/she shall be informed, or when, as to the processed data to which the first clause of Article 13 paragraph 1 applies, a special procedure concerning correction, addition or deletion (hereinafter referred to as "correction etc.") of all or part of the contents of the processed data is provided for, the description to that effect and the title of the said law or order;
- 11) other matters designated by Cabinet Order.

(2) The preceding paragraph shall not apply to the personal data files set forth in the following subparagraphs;

- 1) a personal data file which records matters concerning security of the State, diplomatic secrecy, and other matters involving significant interests of the State;
- 2) a personal data file which is compiled, or obtained for the purpose of criminal investigation, investigation of infraction cases under the provisions of taxation laws or instituting or maintaining of prosecutions;
- 3) a personal data file concerning employees or former employees of an administrative organ, and which solely record items concerning personnel management, salary or welfare or items corresponding to them (including a personal data file concerning entrance examination of personnel conducted by an administrative organ);
- 4) a personal data file which is solely used for experimental computer processing;
- 5) a personal data file which records all or part of the processed data in the personal data file notified under the provision of the preceding paragraph, and whose file-purpose, file record items and file record extent are confined within the extent of those notified matters;
- 6) a personal data file which records only processed data to be erased within one year;
- 7) a personal data file recording processed data which are used for sending materials or other goods or moneys or for ex officio necessary correspondence, and which records only addressees' names, addresses or other items necessary for such sending or correspondence;
- 8) a personal data file which is compiled by an employee by himself/herself solely for the purpose of performing his/her duties within the holding organ;
- 9) a personal data file which is compiled or obtained by an employee on his/her own initiative for use in academic research and processed data which are used solely for the purpose of the said academic organ;
- 10) a personal data file in which the number of the data subjects of the processed data is less than the number provided for by Cabinet Order, and the processed data which are not expected to be provided to any person other than the holding organs;
- 11) a personal data file which is provided for by Cabinet Order as corresponding to any personal data file set forth in subparagraph 3 of the preceding subparagraph.

(3) The head of the holding organ (meaning the person designated by Cabinet Order as referred to in Amide 5 paragraph 1, in the case of an extraordinary organisation provided for by Cabinet Order as referred to in Amide 2 subparagraph 1 (b). The same shall apply hereinafter) shall notify without undue delay the Director-General of the Management and Coordination Agency to that effect, when the holding organ has ceased to hold the personal data file whose records provided for in paragraph 1 were notified or when the personal data file has fallen within the purview of subparagraph 10 of the preceding paragraph.

Article 7 Compiling of and public access to the personal data file directory

(1) In accordance with the provisions of Cabinet Order, the head of a holding organ shall compile a directory of all holding personal data files (except those set forth in the subparagraphs of paragraph 2 of the preceding amide), which respectively describes the matters set forth in subparagraph 1 to 7, 9 and 10 of paragraph 1 of the preceding article (hereinafter referred to as "personal data file directory"), and make it available for public access.

(2) Notwithstanding the preceding paragraph, when the head of the holding organ finds that the proper performance of functions relating to the file-holding purpose is likely to be greatly obstructed by describing in the personal data files directory a part of the file record items or matters set forth in subparagraph 5 or 6 of paragraph 1 of the preceding article, he/she may withhold entering the part of the file record items or matters.

(3) Notwithstanding paragraph 1, when the head of the holding organ finds, with regard to the personal data file used for one of the functions set forth in the following subparagraphs, that the proper performance of functions relating to the file-holding purpose is likely to be greatly obstructed by entering in the personal data files directory the personal data files, he/she may withhold entering it in the personal data files directory,

- 1) the function concerning prevention of crime;
- 2) the function concerning international assistance in criminal investigation;
- 3) the function concerning execution of detention, correction or rehabilitation of criminal offenders;
- 4) the function concerning control over the entry into or departure from Japan of all persons or recognition of refugee status of granting of visas;
- 5) the function concerning assessment or collection of tax;

6) the function provided for by Cabinet Order as corresponding to any function set forth in the subparagraph above.

Article 8 Public notice of personal data files

(1) The Director-General of the Management and Coordination Agency shall make public in the Official Gazette at least once a year the matters set forth in subparagraphs 1 to 7, 9 and 10 of Amide 6 and paragraph 1, with regard to the personal data files notified under the provision of paragraph 1 of the same amide. This shall not apply, however, to the personal data files notified under the provision of paragraph 3 of the same amide.

(2) Notwithstanding the preceding paragraph, with regard to the personal data files set forth in the following subparagraphs, the Director-General of the Management and Coordination Agency shall not make public part of the file record items or the matters set forth in the said subparagraph:

1) a personal data file in which some of the items or matters in the file record as set forth in subparagraph 5 or G were entered in the personal data files directory under the provision of paragraph 2 of the preceding Amide-the said part of the file record items or the matter decided not to be entered;

2) the personal data file which was decided not to be entered in the personal data files directory under the provision of paragraph 3 of the preceding amide the matters provided for in the preceding paragraph.

(3) Notwithstanding paragraph 1, when there was no notification of the matters to be modified under the provision of Amide G paragraph 1 since the previous publication, the Director-General of the Management and Coordination Agency may withhold publication of paragraph 1 with regard to the personal data file.

(4) When the Director-General of the Management and Coordination Agency receives notification under the provision of Amide G paragraph 3 after the previous publication, with regard to the personal data file made public under the provision of paragraph 1, he/she shall also make public the content of the notification, on the occasion of the publication made under the provision of paragraph 1.

Article 9 Restrictions of use and providing of processed data

(1) Processed data shall not be used or provided for any purpose other than the fileholding purpose, except when they shall be used within the holding

organ or provided to a person other than the holding organ in accordance with the provisions of law.

(2) Notwithstanding the preceding paragraph, when the head of the holding organ recognises that any of the following subparagraphs shall apply, he/she may use or provide the processed data for a purpose other than the file-holding purpose. This shall not apply to such cases, however, where it is recognised that the rights and interests of the data subject of the processed data or third parties are likely to be improperly infringed upon by the use of providing of the processed data for a purpose other than the fileholding purpose:

- 1) when there is a consent of the data subject of the processed data, or when they are provided by him/her;
- 2) where the holding organ uses processed data within the organ to the extent necessary to perform the competent functions provided for by law, with a reasonable motive to use them;
- 3) where processed data are provided to an administrative organ other than the holding organ, a local government or a corporation created directly by law or a corporation set up by the special act of establishment in accordance with the provisions of a special law (excluding corporations which are not applied to Article 4 paragraph 11 of the Establishment Law of the Management and Coordination Agency (Law No. 79 of 1983). Hereinafter referred to as "special public corporation"), and when the person to whom the processed data are provided (hereinafter referred to as "recipient") uses them to the extent necessary to perform the functions or businesses provided for by law, and there is a reasonable motive for the recipient to use them;
- 4) besides the cases set forth in the three subparagraphs above, when processed data are provided solely for the purpose of compiling statistics for academic research, when it is clearly of benefit to the subject of the processed data to provide them to a person other than the subject of the processed data or when there is any other special reason for providing the processed data.

(3) The preceding paragraph shall not preclude application of the provisions of other laws which restrict use or providing of processed data.

(4) The head of the holding organ shall, when he/she recognises it especially necessary to protect the rights and interests of individuals, restrict the use of processed data within the holding organ for a purpose other than the file-holding purpose to specified departments and organisations.

Article 10 Duties of the recipient to take necessary measures

(1) The head of a holding organ shall, in the case where he/she provides processed data to the person set forth in subparagraph 3 or 4 of paragraph 2 of the preceding Article under the provision of paragraph 2 of the same Article, when he/she deems it necessary, place restrictions on the purpose or use or other necessary limits on the recipient or request it to take measures for security of the processed data provided.

(2) The head of the holding organ shall, on the occasion of placing the restrictions of the person set forth in subparagraph 3 of paragraph 2 of the preceding Article or requesting it to take measures by the provision of the preceding paragraph, take care not to obstruct improperly the performance of its functions or business.

Article 11 Obligation of person entrusted with computer processing etc. of personal data

Article 5 paragraph 1 shall apply, mutatis mutandis, to the case where a person entrusted with computer processing etc. of personal data by an administrative organ conducts the entrusted businesses.

Article 12 Duty of a person engaged in computer processing etc. of personal data

An employee or former employee of an administrative organ who conducts computer processing etc. of personal data, a person who is engaged in or formerly engaged in the entrusted businesses of the preceding article, shall not divulge or use for an improper purpose the contents of personal data which have come to his/her knowledge in the performance of his/her duties.

Chapter 3 Disclosure and Correction etc. of Processed Data

Article 13 Disclosure of processed data

(1) Any person may request in writing to the head of a holding organ the disclosure (including the information that these are not the processed data. The same shall apply hereinafter) of the processed data of which he/she is the data subject (excluding ones recorded in the personal data file which was not entered in the personal data files directory and the file record items which was decided not to describe in the personal data file directory under the pro-

vision of Article 7 paragraph 2). This shall not apply, however, to a personal data file which records items concerning school records or entrance examinations in schools provided for in the School Education Law (Law No. 26 of 1947), a personal data file which records items concerning diagnosis and treatment in a hospital, clinic or maternity clinic, and a personal data file which records items concerning trials of criminal cases or depositions given by public prosecutors, public prosecutor's assistants, officers of the court, police officials or on the execution of sentences.

(2) A legal representative of a minor or a person to be judged incompetent may make a request for disclosure under the terms of the preceding paragraph (hereinafter referred to as "request for disclosure") on behalf of the data subject.

(3) When a request for disclosure is made, the head of the holding organ shall disclose the processed data concerned with the request in writing to the person who has made the request (hereinafter referred to as "request for disclosure") except in the cases set forth in paragraph 1 of the following article. When consent is given by the person requesting disclosure, however, he/she may disclose by means other than in writing.

Article 14 Non-disclosure of processed data

(1) Where the head of the holding organ finds that results in any of the following subparagraphs fall under the disclosure of processed data concerned with the request for disclosure, he/she is not permitted to disclose all or part of the said processed data:

- 1) Hindering the proper performance of any of the following functions:
 - (a) the functions set forth in subparagraphs 1 to 5 of Article 7 paragraph 3;
 - (b) a function concerning criminal investigation, investigation of infraction cases under the provisions of taxation laws, or instituting or maintaining public prosecutions;
 - (c) a function concerning execution of entry and inspection or other powers of inquiry under the provision of law;
 - (d) a function concerning examination of knowledge and skill, review of qualifications etc., assessment of compensation of benefit etc., or other estimate or judgement corresponding to them;
 - (e) a function provided for by Cabinet Order as corresponding to any function set forth in (a) to (d).

- 2) In the case where the processed data are concerned with the data obtained from a third party, impairing a cooperative relationship or reliant relationship between the holding organ and the third party;
- 3) Injuring an individual's life, body, property or other interests.

(2) When the head of the holding organ decides not to disclose all or part of the processed data under the provision of the preceding paragraph (hereinafter referred to as a "non-disclosure decision"), he/she shall deliver a document which sets out that decision and the reasons) to the person that requested the disclosure.

Article 15 Time limit for disclosure etc.

(1) Disclosure under Article 13 paragraph 3 or a non-disclosure decision (referred to as "disclosure etc." in this Article) shall be made within 30 days beginning with the day when the request for the disclosure was received.

(2) When unable to make the disclosure etc. within the period provided for in the preceding paragraph because of difficulty in dealing with the task or any other proper reason, the head of the holding organ shall, within the period provided for, notify in writing to the person requesting the disclosure, the reason why the disclosure cannot be made etc. within the period and the time limit of the disclosure etc.. Upon being able to make the disclosure, he/she should do so without undue delay.

(3) A person requesting disclosure may consider that a nondisclosure decision has been made when a disclosure etc. has not been made within the period provided for in paragraph I (until the said time limit in the case where the time limit of the disclosure etc. was notified under the provision of the preceding paragraph).

Article 16 Fees etc.

(1) A person who makes a request for disclosure shall pay fees in accordance with the provisions of Cabinet Order.

(2) A person who makes a request for disclosure may, except in the cases provided for by Cabinet Order, request mailing of the written disclosure provided for in Article 13 paragraph 3 by paying postage in addition to the fees of the preceding paragraph.

Article 17 Correction etc. of processed data

(1) When an application for correction etc. of the disclosed processed data has been made in writing by the person who received disclosure by the provision of Article 13 paragraph 3, the head of the holding organ shall make an investigation without undue delay to the extent necessary for accomplishing the file-holding purpose and notify in writing the result to the person who made the application, except in the case where a special procedure for the applied correction etc. of the contents of the processed data is provided for under the provisions of other law or order.

(2) The person who made the application for correction etc. under the provision of the preceding paragraph may, when he/she is dissatisfied with the contents of the notification of the same paragraph, make an application for reinvestigation to the head of the holding organ.

(3) Paragraph 1 shall apply, mutatis mutandis, to the case where the application of the preceding paragraph was made.

Article 18 Delegation to Cabinet Order

Items to be written in the documents under the provisions of Article 13 paragraph 1, Article 14 paragraph 2, Article 15 paragraph 2 and paragraph 1 of the preceding article, documents necessary for a request for disclosure from a legal representative under the provision of Article 13 (2), procedures necessary to identify that a requester for disclosure is the data subject of the processed data, and other matters necessary for a request for disclosure, methods of disclosure and correction etc. of the processed data shall be provided for by Cabinet Order.

Article 19 Relation with other laws

When all or parts of the contents of the processed data appear in a licence, permit, notice or other document, and it has already been issued to the data subject, when all or part of the contents of the processed data have been published or made available for inspection, or when the data subject makes a request that shall be informed, in accordance with the provisions of other law or order thereunder, the first clause of Article 13 paragraph I shall not apply to all or part of the said processed data.

Chapter 4 Miscellaneous Provisions

Article 20 Handling of complaints

The head of the holding organs shall strive to deal properly and promptly with complaints concerning use, providing or disclosure of the processed data or applications for correction etc. of the processed data or other complaints with regard to dealing with the processed data.

Article 21 Requests for submission of materials and explanations

The Director-General of the Management and Coordination Agency may request the head of the administrative organ to submit materials and to give an explanation, when he/she finds it necessary to do so, with regard to the operation of functions concerning computer processing etc. of the personal data in the administrative organ.

Article 22 Statement of an opinion

The Director-General of the Management and Coordination Agency may give an opinion to the Prime Minister or the head of an administrative organ with regard to dealing with computer-processed personal data held by the administrative organ, when he/she finds it necessary in order to achieve the purpose of this Act.

Article 23 Delegation of powers and functions

The head of a holding organ may delegate to employees of the holding organ the powers and functions provided for in Article 9 paragraph 2, Article 10 paragraph 1, Articles 13 and 14, Article 15 paragraph 2 and Article 17 paragraph 1, under the provision of Cabinet Order (in the case of an organ established under the jurisdiction of the Cabinet, an order of the said organ).

Article 24 Delegation to Cabinet Order

In addition to the provisions of this Act, matters necessary for implementation of this Act shall be provided for by Cabinet Order.

Article 25 Penalty

A person who has obtained disclosure by the provision of Article 13 paragraph 3 by deceit or other unjust means shall be liable to a correctional fine of not more than 100,000 yen.

Article 26 Measures of local government

Where a local government conducts computer processing etc. of personal data, it shall, taking into account the national measures under the provisions of this Act, strive to take necessary measures to secure proper dealing with personal data, and to implement them.

Article 27 Actions to be taken by public corporations

Where a public corporation conducts computer processing etc. of personal data, it shall, taking into account the national measures under the provisions of this Act, strive to take necessary actions to secure proper dealing with personal data.

Supplementary Provisions

Article 1 Commencement

This Act shall come into force from the day fixed by Cabinet Order within not more than one year beginning with the day of promulgation. The provisions of Chapter 3 and Article 23 (excluding the part concerned with Article 9 paragraph 2 and Article 10 paragraph 1 within the same article) shall, however, come into force on the day fixed by Cabinet Order within not more than two years beginning with the day of promulgation.

Article 2 Transitional measures

With regard to the application of the provisions of Article G paragraph 1 and Article 8 paragraph 1 as to the personal data files held by an administrative organ at the time of commencement of this Act, "intends to hold" in Article G paragraph 1 shall be "holds"; "in advance" in the same provision shall be "without undue delay after commencement of this Act"; and "at least once a year" in Article 8 paragraph 1 shall be "without undue delay after receiving the notification".

Article 3

(1) The provisions of this Act shall not apply to the existing statistical reports provided for in Article 2 paragraph 1 of the supplementary provisions of the Law to Amend the Parts of the Statistics Law and the Statistical Reports Coordination Law (Law No. 96 of 1988. Hereinafter referred to as "the Amended Statistics Law"), (including ones deemed to be the existing statistical reports by

the provision of paragraph 3 of the same article) until the end of one year beginning with the day of commencement of this Act. With regard to the application of the preceding article in this case, "without undue delay after commencement of this Act" shall be "without undue delay after the end of the one year beginning with the day of commencement of this Act".

(2) The provisions of this Act shall not apply to the statistical reports (limited to the part relating to items used solely for compiling statistics) notified under the provision of Article 2 paragraph 1 of the supplementary provisions of the Amended Statistics Law.

Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector

Ministry of International Trade and Industry
Notification nr. 98 04.03.1997

Chapter 1. Purpose of Guidelines

Article 1. Purpose

The purpose of these guidelines is to protect adequately personal data handled by enterprises in the private sector. These guidelines help business organizations to establish guidelines for each industry sector according to the status of the operations of member enterprises, with a view to supporting and promoting the enterprises' establishment of a compliance program aimed at protecting personal data according to the activities of enterprises.

Chapter 2. Definitions

Article 2. Definitions

For the purposes of these guidelines, the meaning of the terms set forth in the following subparagraphs shall be provided for in the said subparagraphs.

- 1 The term "personal data" means data which relate to an individual, and ones that the individual can be identified from name, date of birth or other descriptions or from number, symbol, other mark, image or sound assigned to the individual contained in the data (including data that the individual can not be identified only from the data, but be

identified by easily collating with other data). They exclude, however, such data concerning directors of a corporation or other organization as contained in the data recorded with regard to the corporaion or other organization.

- 2 The term "manager" means a person designated by the representative of enterprises who has authority to determine the purpose, method, etc. of collection, use and disclosure of personal data.
- 3 The term "recipient" means a person or an enterprise that personal data are disclosed to.
- 4 The term "consent of data subject" means the declaration of intent, by the data subject, to give consent to the handling of personal data concerning him through an explicit response given through a signed and sealed statement or oral agreement. However, in the case of actions including transactions, applications, subscriptions, etc. not associated with contract procedures through the issue of documents, etc. this shall include the tacit declaration of intent, in which opposition is not expressed, given in the procedures associated with the actions.

Chapter 3. Scope of Application of Guidelines

Article 3. Personal Data to which Guidelines Apply

These guidelines shall apply to personal data processed, either wholly or in part, using electronic computers, optical information processing devices or other automatic processing systems within enterprises, including personal data processed in document form for the purpose of processing by an automatic processing system. This shall not apply, however, to personal data collected by an individual for personal uses.

Article 4. Extension of Guidelines

Provisions to these guidelines may be added or revised according to the activities of the industry sector or enterprises in so far as these additions or revisions are in line with the purpose of adequately protecting personal data.

Chapter 4. Measures Concerning Collection of Personal Data

Article 5. Limitation on Collection of Personal Data

The collection of personal data shall specify clearly the purpose of the collection within the limit of legitimate business of enterprises and shall be conducted to the extent necessary to achieve the purpose.

Article 6. Limitation on Methods of Collection

The collection of personal data shall be conducted by lawful and fair means.

Article 7. Prohibition against Collection of Specific Personal Data of a Delicate Nature

Personal data which include the following types of data shall not be collected, used or disclosed. This shall not apply, however, in the case where the data subject has given explicit consent to the collection, use or disclosure of the data, or where there are special provisions in laws, or where it is necessary for the judicial procedures to collect, use or disclosure the data.

- Race or ethnicity

- Family origin or legal domicile (not including data relating to prefectures of current residence)
- Religion (including ideology and beliefs), political opinions or trade-union membership
- Health, medical treatment or sex life

Article 8. Measures for Collection of Personal Data Directly from Data Subject

When personal data are collected directly from the data subject, the consent of the data subject concerning the collection, use and disclosure of the personal data shall be obtained through written notification of at least the information given below, or of equivalent information. This shall not apply, however, in the case where it is clear that the data subject has been notified in writing of the information given below, or where personal data are collected from data made public by the data subject to a large number of unspecified persons.

- 1 The name or title, department and telephone number or address, etc. of the manager or his agent concerned with personal data within enterprises.
- 2 Purpose of the collection and the use of personal data.
- 3 If there is a plan to disclose personal data, the purpose thereof, the recipient of the personal data or the type and character of the recipient's organization, and whether or not a contract has been concluded concerning the handling of personal data.
- 4 The voluntariness of the data subject concerning provision or non-provision of personal data and the result not to provide personal data.
- 5 The existence of the right to request access to personal data and the right to request correction or deletion thereof if the personal data are found to be erroneous following

the access, and the specific method by which the right is to be exercised.

Article 9. Measures for Indirect Collection of Personal Data Other than from Data Subject

When personal data are collected indirectly from a source other than the data subject, the consent of the data subject concerning the collection, use and disclosure of the personal data shall be obtained through written notification of at least the information given in (1) through (3) and (5) of the preceding Article. This shall not apply, however, in the case given in (1) through (4) below.

- 1 If personal data are collected from enterprises that have obtained the data subject's consent to disclose the personal data in accordance with (3) of the preceding Article when the personal data were collected from the data subject
- 2 If personal data are collected and disclosed from enterprises with a guarantee that personal data are handled in a manner equivalent to that of the enterprises through conclusion of a contract stipulating the obligation to maintain confidentiality, the prohibition against re-disclosure and the assignment of responsibility when accidents occur in respect of personal data disclosed.
- 3 If it is clear that the data subject has been notified of the information given in (1) through (5) of the preceding Article, and if personal data are collected from data made public by the data subject to a large number of unspecified persons.
- 4 If personal data are collected in the case where it is not likely to infringe on the interests of the data subject worthy of protection within the limit of legitimate business of enterprises.

Chapter 5. Measures Concerning Use of Personal Data

Article 10. Limitation on Use of Personal Data

The use of personal data shall, in principle, be limited within the scope of the purpose of the collection.

Article 11. Measures for Use of Personal Data within the Scope of the Purpose

The use of personal data within the scope of the purpose of the collection shall be done solely in the case given in (1) through (6) below.

- If the data subject has given consent.
- If the use is necessary to permit the data subject to prepare for or to perform a contract to which he is a party.
- If the use is necessary for compliance with legal obligations to which enterprises are subject.
- If the use is necessary in order to protect the vital interests of the data subject including life, health, property, etc.
- If the use is necessary for protecting the public interest or for exercising authority under laws by enterprises or a third party that personal data are disclosed to.
- If the use is necessary for the legitimate interests of enterprises, or a third party or other parties that the personal data are disclosed to, in so far as the interests of the data subject are not infringed.

Article 12. Measures for Use of Personal Data beyond the Scope of the Purpose

When the use of personal data exceeds the scope of the purpose of the collection, or when the use of personal data is done in the

cases other than any of the cases given in (1) through (6) of the preceding Article, it shall be carried out with the prior acknowledgment of the data subject secured by obtaining the prior consent of the data subject or by giving the data subject an opportunity to refuse prior to use, through written notification of at least the information given in (1) through (3) and (5) of Article 8.

Chapter 6. Measures Concerning Disclosure of Personal Data

Article 13. Limitation on Disclosure of Personal Data

The disclosure of personal data shall, in principle, be limited within the scope of the purpose of the collection.

Article 14. Measures for Disclosure of Personal Data within the Scope of the Purpose

The disclosure of personal data within the scope of the purpose of the collection shall be carried out with the prior acknowledgment of the data subject secured by obtaining the prior consent of the data subject or by giving the data subject an opportunity to refuse prior to disclosure, through written notification of at least the information given in (1) through (3) and (5) of Article 8. This shall not apply, however, in the case given in (1) through (4) below.

- If personal data are disclosed to the recipient that the data subject has given consent to disclose the personal data to in accordance with (3) of Article 8 when the personal data were collected from the data subject.
- If personal data are disclosed to the recipient with a guarantee that personal data are handled in a manner equivalent to

that of enterprises that disclose the personal data through conclusion of a contract stipulating the obligation to maintain confidentiality, the prohibition against re-disclosure and the assignment of responsibility when accidents occur in respect of personal data disclosed.

- If it is clear that the recipient is to take measures to obtain the data subject's consent through notification of the information given in (1) through (3) and (5) of Article 8 concerning the personal data.
- If personal data are disclosed in the case where it is not likely to infringe on the interests of the data subject worthy of protection within the limit of legitimate business of enterprises.

Article 15. Measures for Disclosure of Personal Data beyond the Scope of the Purpose

When the disclosure of personal data exceeds the scope of the purpose of the collection, or when the disclosure of personal data is done in cases other than any of the cases given in (1) through (4) of the preceding Article, the consent of the data subject shall be obtained through written notification of at least the information corresponding to (1) through (3) and (5) of Article 8 concerning the recipient of the personal data. In such cases, "enterprises" given in (1) of Article 8 shall be amended to read "recipient", and "disclose" given in (3) of Article 8 shall be amended to read "re-disclose". This shall not apply, however, in the case where it is clear that the data subject has been notified of the information and has given blanket consent.

Chapter 7. Obligation to Manage Personal Data Properly

Article 16. Ensuring the Accuracy of Personal Data

Personal data shall be kept accurate and up-to-date to the extent necessary for the purpose of the use.

Article 17. Ensuring Security in Use of Personal Data

Reasonable security measures shall be taken through both technical and organizational means against such risks as unauthorized access to personal data or as loss, destruction, alteration, leakage, etc. of personal data.

Article 18. Obligation of Employees to Maintain Confidentiality of Personal Data

Persons within enterprises engaged in the collection, use and disclosure of personal data shall perform, using sufficient care, the obligation to maintain the confidentiality of personal data in accordance with the provisions of laws, or regulations and instructions specified by the manager of the enterprises.

Article 19. Measures Concerning Entrustment of Personal Data

In the case where enterprises entrust personal data to an outside enterprise, they shall select one that can handle the personal data at a sufficient level of protection, and shall guarantee, through conclusion of a contract or other legal measure, that the instructions of the manager of the enterprises are observed, that the confidentiality of personal data is maintained, that the re-disclosure of personal data is prohibited, and that responsibility

when accidents occur is assigned, and shall maintain the contract, etc. as written documents or magnetically-stored records for the period that the personal data are managed by the outside enterprise.

Article 20. Rights Concerning Own Personal

Data Requests for access to personal data by the data subject shall, in principle, be accepted within a reasonable period of time. If the personal data is found to be erroneous following the access, requests for correction or deletion of the personal data shall, in principle, be accepted within a reasonable period of time. In such cases, recipients of the personal data shall be notified to the extent possible.

Article 21. Right to Refuse Use or Disclosure of Own Personal Data

Refusals of the use or the disclosure, by the data subject, of personal data managed by enterprises shall be accepted. This shall not apply, however, in the case where the use or the disclosure is necessary for protecting the public interest, or for exercising authority or performing obligations under laws by the enterprises or a third party that the personal data are disclosed to.

Chapter 9. Organization and Implementation Accountability

Article 22. Designation of Manager by the Representative

The representative of enterprises shall designate from within the enterprises a person who understands the contents of these guide-

lines and has the capacity to put them into practice, and shall cause the person to function as the manager of personal data.

Article 23. Duties of Manager

The manager of personal data within enterprises shall understand and observe the provisions of these guidelines, and shall accept responsibility for causing employees to understand and observe these guidelines by providing training, establishing internal regulations, implementing security measures, establishing a compliance program and taking measures to ensure that the program is made known to everyone.

Chapter 10. Other Provisions

Article 24. Notification when Magnetically-Stored Records are Transmitted and

Received Using Communication Networks In the case where magnetically-stored records are transmitted and received using a communication network, enterprises that collect personal data concerning the sender or receiver of the records using a communication network can notify the data subject, who is the sender or receiver, through transmission of magnetically-stored records rather than through written notification of the data subject, as provided for in Article 8, Article 9, Article 12, Article 14, and Article 15 of these guidelines.

TIDLIGERE UTGITT I COMPLEX-SERIEN

CompLex er Institutt for rettsinformatikk skriftserie. Serien startet i 1981, og det har blitt utgitt mer enn hundre titler. Bøkene i CompLex-serien kan bestilles fra GnistAkademika (se bestillingsskjema bak i boken eller www.gnist.no).

2002

- 1/02 Koblingshandel og forholdet til fysisk og teknologisk integrasjon i relasjon til EØS-avtalens art.54(d)**
Ole Jacob Garder NOK 180,-
- 2/02 To opphavsrettslige arbeider:**
Bjarte Aambø – Opphavsrettslige rettsmangler
Erlend Rignes Efskind – Skjermbildets rettslige natur
Aambo / Rignes Efskind..... NOK 201,-
- 3/02 Arbeidstakeroppfinnelser ved universiteter og høyskoler. Innstilling fra et utvalg oppnevnt av universitets- og høyskolerådet 31 januar 2000. Avgitt til universitets- og høyskolerådet i oktober 2001**
..... NOK 213,-
- 4/02 Utøvende kunstners direkteoverføringer på Internett – med hovedvekt på kringkastingsbegrepet**
Irina Eidsvold Tøien..... NOK 225,-
- 5/02 Administrasjon av radiofrekvensspekteret. Rettslige problemstillinger knyttet til telemyndighetenes forvaltning av frekvensressursene**
Øyvind Haugen..... NOK 177,-

2001

- 1/01 **Internet and Choice-of-Law – The International Sale of Digitised Products through the Internet in a European Context**
Peter Lenda..... NOK 275,-
- 2/01 **Internet Domain Names and Trademarks**
Tonje Røste Gulliksen NOK 227,-
- 3/01 **Internasjonal jurisdiksjon ved elektronisk handel – med Lugano-konvensjonen art 5 (5) og elektroniske agenter som eksempel**
Joakim S. T. Øren NOK 204,-
- 4/01 **Legal issues of maritime virtual organisations**
Emily M. Weitzenböck..... NOK 164,-
- 5/01 **Cyberspace jurisdiction in the U.S. – The International Dimension of Due Process**
Henrik Spang-Hanssen..... NOK 685,-
- 6/01 **Norwegian border control in a Europe without Internal Frontiers – Implications for Data Protection and civil liberties**
Stephen Kabera Karanja..... NOK 252,-

2000

- 1/00 **Klassikervernet i norsk åndsrett**
Anne Beth Lange..... NOK 268,-
- 2/00 **Adgangen til å benytte personopplysninger. Med vekt på det opprinnelige behandlingsformålet som begrensningsfaktor**
Claude A. Lenth NOK 248,-
- 3/00 **Innsyn i personopplysninger i elektroniske markedsplasser.**
Line Coll..... NOK 148,-

1999

- 1/99 International regulation and protection of Internet domain and trademarks**
Tonje Røste Gulliksen NOK 248.-
- 2/99 Betaling via Internett**
Camilla Julie Wollan..... NOK 268.-
- 3/99 Internett og jurisdiksjon**
Andreas Frølich Fuglesang & Georg Philip Krog NOK 198.-

1998

- 1/98 Fotografiske verk og fotografiske bilder, åndsverkloven § 1 og § 43 a**
Johan Krabbe-Knudsen..... NOK 198.-
- 2/98 Straffbar hacking, straffelovens § 145 annet ledd**
Guru Wanda Wanvik NOK 238.-
- 3/98 Interconnection – the obligation to interconnect telecommunications networks under EC law**
Katinka Mahieu..... NOK 198.-

1997

- 1/97 Eksemplarframstilling av litterære verk til privat bruk**
Therese Steen..... NOK 158.-
- 2/97 Offentlige anskaffelser av informasjonsteknologi**
Camilla Sivesind Tokvam..... NOK 175.-
- 3/97 Rettslige spørsmål knyttet til Oppgaveregisteret**
Eiliv Berge Madsen..... NOK 170.-
- 4/97 Private pengespill på Internett**
Halvor Manshaus NOK 160.-

- 5/97 **Normative Structures in Natural and Artificial Systems**
Christen Krogh..... NOK 255.-
- 6/97 **Rettslige aspekter ved digital kringkasting**
Jon Bing..... NOK 178.-
- 7/97 **Elektronisk informasjonsansvar**
Tomas Myrbostad NOK148.-
- 8/97 **Avtalelisens etter åndsverksloven § 36**
Ingrid Mauritzen NOK 120.-
- 9/97 **Krav til systemer for forvaltning av immaterielle rettigheter**
Svein Engebretsen..... NOK 168.-
- 10/97 **American Telephony: 120 Years on the Road to Full-blown Competition**
Jason A. Hoida..... NOK 140.-
- 11/97 **Rettslig vern av databaser**
Harald Chr Bjelke NOK 358.-

1996

- 1/96 **Innsynsrett i elektronisk post i offentlig forvaltning**
Knut Magnar Aanestad og Tormod S. Johansen..... NOK 218.-
- 2/96 **Public Policy and Legal regulation of the Information Market in the Digital Network Enviroment**
Stephen John Saxby..... NOK 238.-
- 3/96 **Opplysning på spill**
Ellen Lange..... NOK 218.-
- 4/96 **Personvern og overføring av personopplysninger til utlandet**
Eva I. E. Jarbekk..... NOK 198.-
- 5/96 **Fjernarbeid**
Henning Jakhell..... NOK 235.-

- 6/96 A Legal Advisory System Concerning Electronic Data Inter-
change within the European Community**
Andreas Mitrakas NOK 128.-
- 7/96 Elektronisk publisering: Utvalgte rettslige aspekter**
Jon Bing og Ole E. Tokvam NOK 186.-
- 8/96 Fjernsynsovervåking og personvern**
Finn-Øyvind H. Langfjell NOK 138.-

1995

- 1/95 Rettslige konsekvenser av digitalisering: Rettighetsadministra-
sjon og redaktøransvar i digitale nett**
Jon Bing NOK 368.-
- 2/95 Rettslige spørsmål i forbindelse med utvikling og bruk av stan-
darder innen telekommunikasjon**
Sverre Sandvik NOK 178.-
- 3/95 Legal Expert Systems: Discussion of Theoretical Assumptions**
Tina Smith NOK 278.-
- 4/95 Personvern og straffeansvar – straffelovens § 390**
Ole Tokvam NOK 198.-
- 5/95 Juridisk utredning om filmen «To mistenkelige personer»**
Johs. Andenæs NOK 138.-
- 6/95 Public Administration and Information Technology**
Jon Bing and Dag Wiese Schartum NOK 348.-
- 7/95 Law and Liberty in the Computer Age**
Vittorio Frosini NOK 158.-

1994

- 1/94 **Deon'94, Second International Workshop on Deontic Logic in Computer Science**
Andrew J. I. Jones & Mark Sergot (ed)..... NOK 358.-
- 2/94 **Film og videogramrett. TERESA (60)**
Beate Jacobsen NOK 318.-
- 3/94 **Elektronisk datutveksling i tollforvaltningen – Rettslige spørsmål knyttet til TVINN**
Rolf Risnæs..... NOK 225.-
- 4/94 **Sykepenger og personvern – Noen problemstillinger knyttet til behandlingen av sykepenger i Infotrygd**
Mari Bø Haugestad..... NOK 148.-
- 5/94 **EØS, medier og offentlighet. TERESA (103)**
Mads Andenæs, Rolf Høyer og Nils Risvand NOK 148.-
- 6/94 **Offentlige informasjonstjenester: Rettslige aspekter**
Jon Bing..... NOK148.-
- 7/94 **Sattelittfjernsyn og norsk rett. MERETE (3) IV**
Nils Eivind Risvand..... NOK 138.-
- 8/94 **Videogram på forespørsel. MERETE (14) IV**
Beate Jacobsen (red) NOK 158.-
- 9/94 **«Reverse engineering» av datamaskinprogrammer. TERESA (92) IV**
Bjørn Bjerke..... NOK 198.-
- 10/94 **Skattemessig behandling av utgifter til anskaffelse av datamaskinprogrammer. TERESA (75)**
Gjert Melsom NOK 198.-

1993

- 1/93 **Artificial Intelligence and Law. Legal Philosophy and Legal Theory**
Giovanni Sartor..... NOK 148.-
- 2/93 **Erstatningsansvar for informationstjenester, særlig ved databaseydelser**
Connie Smidt..... NOK 138.-
- 3/93 **Personvern i digitale telenett**
Ingvild Hanssen-Bauer..... NOK 178.-
- 4/93 **Consumers Purchases through Telecommunications in Europe. – Application of private international law to cross-border contractual disputes**
Joachim Benno..... NOK 198.-
- 5/93 **Four essays on: Computers and Information Technology Law**
Morten S. Hagedal..... NOK 218.-
- 6/93 **Sendetidsfordeling i nærradio MERETE (3) III**
Marianne Rytter Evensen..... NOK 148.-
- 7/93 **Essays on Law and Artificial Intelligence**
Richard Susskind..... NOK 158.-

1992

- 1/92 **Avskrivning av mikrodatamaskiner med tilbehør – en nordisk studie TERESA (87)**
Beate Hesselvedt..... NOK 138.-
- 2/92 **Kringkastingsbegrepet TERESA (78)**
Nils Kr. Einstabland..... NOK 208.-
- 3/92 **Rettskilderegistre i Helsedirektoratet NORIS (94) I & II**
Maria Strøm..... NOK 228.-

- 4/92 Softwarepatent – Imaterialrettens enfant terrible. En redegjørelse for patenteringen af softwarerelaterede opfindeiser i amerikansk og europæisk ret**
Ditlev Schwanenfügel NOK 158.-
- 5/92 Abonnementskontrakter fro kabelfjernsyn TERESA (78II)**
Lars Borchgrevink Grindal NOK 248.-
- 6/92 Implementing EDI – a proposal for regulatory form**
Rolf Riisnæs NOK 118.-
- 7/92 Deponering av kildekode«escrow»-klausuler TERESA (79)**
Morten S. Hagedal NOK 128.-
- 8/92 EDB i juridisk undervisning – med en reiserapport fra England og USA**
Ola-Kristian Hoff NOK 228.-
- 9/92 Universitetets ansvar for bruk av datanett TERESA (94)**
Jon Bing & Dag Elgesem NOK 198.-
- 10/92 Rettslige sider ved teletorg**
Andreas Galtung NOK 148.-

BESTILLING

Jeg bestiller herved følgende CompLex-utgivelser:

Nummer / årgang: _____

Tittel: _____

Nummer / årgang: _____

Tittel: _____

Nummer / årgang: _____

Tittel: _____

Nummer / årgang: _____

Tittel: _____

Nummer / årgang: _____

Tittel: _____

Navn: _____

Adresse: _____

Postadresse: _____

Telefon: _____

Bestillingsskjemaet sendes pr.post eller telefaks til:



Fagbokhandelen i Oslo

Avd. juridisk litteratur Aulabygningen

Karl Johansgt. 47, 0162 Oslo

Telefon: 22 42 54 50

Telefaks: 22 41 17 08

Complex kan også bestilles via nettbokhandelen www.gnist.no

