

KOMMISJONSVEDTAK

2001/EØS/51/38

av 26. juli 2000

i henhold til europaparlaments- og rådsdirektiv 95/46/EF om tilstrekkeligheten av den beskyttelse som oppnås ved «trygg havn»-prinsippene for personvern og tilhørende vanlige spørsmål fra De forente stater handelsdepartement(*)

[meddelt under nummer K(2000) 2441]

(2000/520/EF)

KOMMISJONEN FOR DE EUROPEISKE FELLESKAP
HAR —

under henvisning til traktaten om opprettelse av Det europeiske fellesskap,

under henvisning til europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger⁽¹⁾, særlig artikkel 25 nr. 6, og

ut fra følgende betraktninger:

- 1) I henhold til direktiv 95/46/EF skal medlemsstatene sørge for at overføring av personopplysninger til en tredjestat kan finne sted bare dersom den aktuelle tredjestat sikrer et tilstrekkelig vernnivå og dersom medlemsstatenes lover for gjennomføring av andre bestemmelser i direktivet overholdes før overføringen finner sted.
- 2) Kommisjonen kan fastslå at en tredjestat sikrer et tilstrekkelig vernnivå. I så fall kan personopplysninger overføres fra medlemsstatene uten at ytterligere garantier er nødvendig.
- 3) I henhold til direktiv 95/46/EF skal vurderingen av vernnivået for personopplysninger foretas på bakgrunn av alle forhold som har innflytelse på en overføring eller på en type overføringer, og under overholdelse av fastsatte vilkår. Arbeidsgruppen for personvern i forbindelse med behandling av personopplysninger, som ble nedsatt ved nevnte direktiv⁽²⁾, har utarbeidet en veiledning for slike vurderinger⁽³⁾.
- 4) På grunn av tredjestaters ulike oppfatninger med hensyn til beskyttelse av personopplysninger bør vurderingen av om denne beskyttelsen er tilstrekkelig og enhver

avgjørelse i henhold til artikkel 25 nr. 6 i direktiv 95/46/EF, gjennomføres på en måte som ikke medfører vilkårlig eller uberettiget forskjellsbehandling av eller mellom tredjestater der lignende forhold råder, og som ikke utgjør noen skjult handelshindring, idet det tas hensyn til Fellesskapets gjeldende internasjonale forpliktelser.

- 5) Et tilstrekkelig vernnivå for overføring av opplysninger fra Fellesskapet til De forente stater i samsvar med dette vedtak, bør anses som nådd dersom organisasjonene overholder «trygg havn»-prinsippene om beskyttelse av personopplysninger som overføres fra en medlemsstat til De forente stater (heretter kalt «prinsippene») og de «vanlige spørsmål» (heretter kalt VS) som gir veiledning for gjennomføring av prinsippene som De forente staters regjering offentliggjorde 21. juli 2000. Videre bør organisasjonene offentliggjøre sine personvernprogrammer og være underlagt myndigheten til Federal Trade Commission (FTC) i henhold til avsnitt 5 i Federal Trade Commission Act som forbyr urimelig og villedende atferd eller praksis i forbindelse med handel, eller ethvert annet offentlig organ som effektivt kan sikre overholdelse av prinsippene som gjennomføres i samsvar med VS.
- 6) De områder og/eller den behandling av opplysninger som ikke er underlagt myndigheten til noen av de offentlige organene i De forente stater som er nevnt i vedlegg VII til dette vedtak, faller utenfor dette vedtaks virkeområde.
- 7) For å sikre riktig anvendelse av dette vedtak er det nødvendig at organisasjoner som har sluttet seg til prinsippene og VS, blir godkjent av berørte parter som de registrerte, dataoperatører og personvernmyndigheter. For dette formål bør De forente stater handelsdepartement, eller dets representant, påta seg å føre og offentliggjøre en liste over organisasjoner som erklærer sin tilslutning til prinsippene som gjennomføres i samsvar med VS, og som er underlagt myndigheten til minst ett av de offentlige organene nevnt i vedlegg VII til dette vedtak.
- 8) Av klarhetshensyn og for å gi medlemsstatenes vedkommende myndigheter mulighet til å sikre personvern i forbindelse med behandling av personopplysninger, må det i dette vedtak angis under

(*) Denne fellesskapsrettsakten, kunngjort i EFT L 215 av 25.8.2000, s. 7, er omhandlet i EØS-komiteens beslutning nr. 108/2000 av 30. november 2000 om endring av EØS-avtalens vedlegg XI (Telekommunikasjonstjenester), se EØS-tillegget til De Europeiske Fellesskaps Tidende nr. 8 av 15.2.2001, s. 47.

⁽¹⁾ EFT L 281 av 23.11.1995, s. 31.

⁽²⁾ Arbeidsgruppens nettsadresse er: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

⁽³⁾ Uttalelse 12/98, vedtatt av arbeidsgruppen 24. juli 1998: «overføring av personopplysninger til tredjestater: Anvendelse av artikkel 25 og 26 i direktivet om datasikring».

hvilke ekstraordinære omstendigheter det er berettiget å innstille visse overføringer av opplysninger, selv når vernnivået anses å være tilstrekkelig.

- 9) Det kan bli nødvendig å vurdere «trygg havn-ordningen», som er utformet på grunnlag av prinsippene og VS, på nytt i lys av erfaringer, utvikling innen personvern under forhold der teknologien gjør overføring og behandling av personopplysninger stadig lettere, og i lys av gjennomføringsrapporter utarbeidet av vedkommende myndigheter.
- 10) Arbeidsgruppen for personvern i forbindelse med behandling av personopplysninger nedsatt ved artikkel 29 i direktiv 95/46/EF har avgitt uttalelse om vernnivået i henhold til «trygg havn»-prinsippene i USA, som er tatt i betraktning ved utarbeidningen av dette vedtak⁽⁴⁾.
- 11) Tiltakene fastsatt i dette vedtak er i samsvar med uttalelse fra komiteen nedsatt ved artikkel 31 i direktiv 95/46/EF —

GJORT DETTE VEDTAK:

Artikkel 1

1. Med hensyn til artikkel 25 nr. 2 i direktiv 95/46/EF og for all virksomhet som faller inn under direktivets virkeområde, anses «trygg havn»-prinsippene (heretter kalt «prinsippene») som omhandlet i vedlegg I til dette vedtak, gjennomført i samsvar med veiledningen som gis i de «vanlige spørsmål» (heretter kalt VS), som ble utgitt av De forente staters handelsdepartement 21. juli 2000 og er oppført i vedlegg II til dette vedtak, å tilby et tilstrekkelig vernnivå for personopplysninger som overføres fra Fællesskapet til organisasjoner som er etablert i De forente stater, tatt i betraktning følgende dokumenter utgitt av De forente staters handelsdepartement:

- a) oversikt over gjennomføringen av «trygg havn»-prinsippene, vedlegg III,
- b) memorandum om erstatning for krenkelse av personvernet og uttrykkelige tillatelser i De forente staters lovgivning, vedlegg IV,

⁽⁴⁾ WP 15: Uttalelse 1/99 om vernnivået for personopplysninger i USA og de pågående drøftinger mellom Europakommisjonen og den amerikanske regjering.

WP 19: Uttalelse 2/99 om tilstrekkeligheten av de internasjonale «trygg havn»-prinsippene utarbeidet av De forente staters handelsdepartement 19. april 1999.

WP 21: Uttalelse 4/99 om vanlige spørsmål som skal offentliggjøres av De forente staters handelsdepartement i forbindelse med de foreslåtte «trygg havn»-prinsippene.

WP 23: Arbeidsdokument om de foreløpige resultatene av de pågående drøftingene mellom Europakommisjonen og De forente staters regjering om de internasjonale «trygg havn»-prinsippene.

WP 27: Uttalelse 7/99 om vernnivået for opplysninger som oppnås ved hjelp av «trygg havn»-prinsippene, som ble offentliggjort 15. og 16. november 1999 av De forente staters handelsdepartement sammen med vanlige spørsmål (VS) og andre tilhørende dokumenter.

WP 31: Uttalelse 3/2000 om dialogen mellom Den europeiske union og De forente stater om «trygg havn»-ordningen.

WP 32: Uttalelse 4/2000 om vernnivået som oppnås ved hjelp av «trygg havn»-prinsippene.

- c) brev fra Federal Trade Commission, vedlegg V,
- d) brev fra De forente staters transportdepartement, vedlegg VI.

2. I forbindelse med hver enkelt overføring av opplysninger skal følgende vilkår oppfylles:

- a) organisasjonen som mottar opplysningene skal utvetydig og offentlig ha forpliktet seg til å overholde prinsippene som gjennomføres i samsvar med VS, og
- b) organisasjonen skal være underlagt den lovfestede myndigheten til et av de De forente staters offentlige organer oppført i vedlegg VII til dette vedtak, som har myndighet til å behandle klager og sørge for oppreisning ved urimelig og villedende praksis samt erstatning for fysiske personer, uansett bostedsstat eller nasjonalitet, ved manglende overholdelse av prinsippene som gjennomføres i samsvar med VS.

3. Vilkårene oppført i nr. 2 anses for å være oppfylt av enhver organisasjon som har erklært sin tilslutning til prinsippene som gjennomføres i samsvar med VS, fra den dagen organisasjonen underretter De forente staters handelsdepartement, eller dets representant, om offentliggjøringen av forpliktelsen nevnt i nr. 2 bokstav a) og om navnet på det administrative organet som er nevnt i nr. 2 bokstav b).

Artikkel 2

Dette vedtaket gjelder bare spørsmålet om vernnivået i De forente stater er tilstrekkelig i henhold til prinsippene som gjennomføres i samsvar med VS med sikte på å oppfylle kravene i artikkel 25 nr. 1 i direktiv 95/46/EF, og berører ikke anvendelsen av andre bestemmelser i nevnte direktiv som gjelder behandling av personopplysninger i medlemsstatene, særlig artikkel 4.

Artikkel 3

1. Uten at det berører deres myndighet til å treffe tiltak for å sikre overholdelse av nasjonale bestemmelser vedtatt i henhold til andre bestemmelser enn artikkel 25 i direktiv 95/46/EF, kan medlemsstatenes vedkommende myndigheter utøve sin myndighet til å innstille overføring av opplysninger til en organisasjon som har erklært sin tilslutning til prinsippene som gjennomføres i samsvar med VS for å beskytte fysiske personer i forbindelse med behandling av deres personopplysninger i følgende tilfeller:

- a) når De forente staters offentlige organ nevnt i vedlegg VII til dette vedtak, eller en uavhengig klageinstans som nevnt i bokstav a) i vedlegg I til dette vedtak, har fastslått at organisasjonen overtrer prinsippene som gjennomføres i samsvar med VS, eller

- b) når det er svært sannsynlig at prinsippene overtres; når det er rimelig grunn til å tro at den berørte håndhevingsinstansen ikke i rett tid treffer eller ikke kommer til å treffe de passende tiltak som behøves for å avgjøre saken; når fortsatt overføring vil innebære en overhengende fare for alvorlig skade for de registrerte og når medlemsstatenes vedkommende myndigheter under de rådende omstendigheter har gjort en rimelig innsats for å varsle organisasjonen og gi den mulighet til å svare.

Innstillingen skal opphøre så snart prinsippene som gjennomføres i samsvar med VS overholdes og Fellesskapets vedkommende myndigheter er underrettet om dette.

2. Medlemsstatene skal omgående underrette Kommissjonen om tiltak som vedtas i henhold til nr. 1.

3. Medlemsstatene og Kommissjonen skal også underrette hverandre om tilfeller der tiltak truffet av organer med ansvar for at prinsippene som gjennomføres i samsvar med VS i De forente stater overholdes, ikke sikrer slik overholdelse.

4. Dersom opplysningene som er innhentet i samsvar med nr. 1, 2 og 3 viser at et organ med ansvar for at prinsippene som gjennomføres i samsvar med VS i De forente stater overholdes, ikke utfører oppgaven sin på en effektiv måte, skal Kommissjonen underrette De forente staters handelsdepartement og om nødvendig framlegge et utkast til tiltak etter framgangsmåten fastsatt i artikkel 31 i direktiv 95/46/EF med sikte på å oppheve eller midlertidig oppheve dette vedtak eller begrense dets virkeområde.

Artikkel 4

1. Dette vedtak kan til enhver tid endres i lys av de erfaringer som er gjort ved anvendelsen av det og/eller dersom

det i amerikansk lovgivning stilles krav til minst samme vernenivå som det som oppnås ved hjelp av prinsippene og VS.

Kommissjonen skal i alle tilfeller på grunnlag av tilgjengelige opplysninger vurdere gjennomføringen av dette vedtak tre år etter at det er meddelt medlemsstatene og underrette komiteen nedsatt i artikkel 31 i direktiv 95/46/EF om enhver relevant iakttakelse, herunder ethvert forhold som kan ha innvirkning på vurderingen i artikkel 1 i dette vedtak av at beskyttelsen er tilstrekkelig i henhold til artikkel 25 i direktiv 95/46/EF, og ethvert forhold som viser at dette vedtak blir gjennomført på en måte som innebærer forskjellsbehandling.

2. Kommissjonen skal om nødvendig framlegge et utkast til tiltak etter framgangsmåten nevnt i artikkel 31 i direktiv 95/46/EF.

Artikkel 5

Medlemsstatene skal treffe alle nødvendige tiltak for å etterkomme dette vedtak innen 90 dager etter at det er meddelt dem.

Artikkel 6

Dette vedtak er rettet til medlemsstatene.

Utferdiget i Brussel, 26. juli 2000.

For Kommissjonen

Frederik BOLKESTEIN

Medlem av Kommissjonen

VEDLEGG I

«TRYGG HAVN»-PRINSIPPER

utstedt av De forente staters handelsdepartement 21. juli 2000

Den europeiske unions omfattende personvernlovgivning («personverndirektivet») trådte i kraft 25. oktober 1998. I henhold til direktivet skal overføring av personopplysninger finne sted bare til tredjestater som sørger for et tilstrekkelig vernnivå. Både De forente stater og Den europeiske union arbeider for å forbedre personvernet for sine borgere, men De forente stater har valgt en annen tilnærming enn Den europeiske union. De forente stater anvender en sektorvis tilnærming som forener lovgivning, regulering og selvregulering. Denne forskjellen i tilnærming har ført til at mange amerikanske organisasjoner er usikre på betydningen av EU-kravet om «tilstrekkelig vernnivå» for overføring av personopplysninger fra Den europeiske union til De forente stater.

For å minske denne usikkerheten og fastsette en mer forutsigbar ramme for slik overføring av personopplysninger har De forente staters handelsdepartement utstedt dette dokumentet («prinsippene») samt «Vanlige spørsmål» (VS) i henhold til sin lovfestede myndighet til å støtte, fremme og utvikle internasjonal handel. Prinsippene er utviklet i samarbeid med næringslivet og offentligheten for å lette handelen mellom De forente stater og Den europeiske union. Prinsippene skal anvendes bare av amerikanske organisasjoner som mottar personopplysninger fra Den europeiske union, for at de skal oppfylle kravene i «trygg havn»-ordningen og dra fordel av den formodningen om et «tilstrekkelige vernnivå» som er fastsatt der. Siden prinsippene ble utviklet utelukkende for dette formål, kan de ikke uten videre anvendes til andre formål. Prinsippene kan ikke anvendes i stedet for nasjonale gjennomføringsbestemmelser for direktivet som gjelder behandling av personopplysninger i medlemsstatene.

En organisasjon bestemmer selv om den vil slutte seg til «trygg havn»-ordningen, og det finnes flere måter å kvalifisere seg på. Organisasjoner som bestemmer seg for å slutte seg til prinsippene, må overholde dem for å oppnå og beholde fordelene ved «trygg havn»-ordningen, og de må offentlig erklære dette. Dersom en organisasjon for eksempel slutter seg til et personvernprogram basert på selvregulering som overholder prinsippene, kvalifiserer organisasjonen for «trygg havn»-ordningen. En organisasjon kan også utvikle sine egne personvernprogrammer basert på selvregulering, forutsatt at de er i samsvar med prinsippene. Dersom overholdelsen av prinsippene er basert helt eller delvis på selvregulering, og organisasjonen ikke overholder selvreguleringen, skal organisasjonen holdes ansvarlig i henhold til avsnitt 5 i Federal Trade Commission Act som forbyr urimelige og villedende praksis, eller annen lov som forbyr slik praksis. (Se vedlegget for liste over amerikanske lovfestede organer som er godkjent av EU.) I tillegg kan organisasjoner som er underlagt lovbestemmelser eller forskrifter (eller regler) som sikrer en effektiv beskyttelse av personopplysninger, også dra fordel av «trygg havn»-ordningen. I alle disse tilfellene er «trygg havn»-fordelene garantert fra og med den datoen da organisasjonen erklærer sin tilslutning til «trygg havn»-prinsippene overfor De forente staters handelsdepartement (eller dets representant) i samsvar med retningslinjene beskrevet i VS om egensertifisering.

Overholdelsen av prinsippene kan begrenses a) til det nivå som er tilstrekkelig for å oppfylle kravene i forbindelse med nasjonal sikkerhet, offentlighetens interesse og håndheving av loven, b) av lover, administrative bestemmelser eller rettspraksis som skaper motstridende forpliktelser eller uttrykkelige tillatelser, forutsatt at organisasjonen ved anvendelse av slike tillatelser kan vise at den overtrer prinsippene bare i det omfang som er nødvendig for å ivareta de overordnede, rettmessige interesser som slike tillatelser skal fremme, eller c) dersom direktivet eller medlemsstatenes lovgivning tillater unntak eller fravikelser, såfremt slike unntak eller fravikelser anvendes i tilsvarende sammenhenger. Organisasjonene bør i samsvar med målet om bedre personvern, søke å gjennomføre disse prinsippene på en fullstendig og oversiktlig måte, noe som innebærer at de i sine personvernprogrammer angir i hvilke tilfeller unntak fra prinsippene i henhold til bokstav b) over får alminnelig anvendelse. Når prinsippene og/eller amerikansk lovgivning gir mulighet til å velge, forventes det av samme årsak at organisasjonene om mulig velger et høyere vernnivå.

Organisasjoner kan av praktiske eller andre årsaker ønske å anvende prinsippene i all sin databehandling, men de er bare forpliktet til å anvende dem på opplysninger som overføres etter at de har sluttet seg til «trygg havn»-ordningen. En organisasjon som ønsker å kvalifisere seg til «trygg havn»-ordningen, er ikke

forpliktet til å anvende prinsippene på behandling av personopplysninger i manuelle registre. Organisasjoner som ønsker å dra fordel av «trygg havn»-ordningen for å motta opplysninger fra manuelle registre i EU, må anvende prinsippene på alle slike opplysninger som overføres etter at de har sluttet seg til «trygg havn»-ordningen. En organisasjon som ønsker å utvide «trygg havn»-ordningen til også å omfatte personopplysninger om menneskelige ressurser som overføres fra EU til bruk innenfor rammen av et ansettelsesforhold, må opplyse om dette ved egensertifisering til De forente staters handelsdepartement (eller dets representant), og må oppfylle kravene beskrevet i VS om egensertifisering. En organisasjon kan også stille de nødvendige garantier i henhold til direktivets artikkel 26 dersom den anvender prinsippene på grunnleggende bestemmelser om personvern i skriftlige avtaler med parter som overfører opplysninger fra EU, når de øvrige bestemmelser om slike standardavtaler er blitt godkjent av Kommissjonen og medlemsstatene.

Amerikansk lovgivning får anvendelse på spørsmål om fortolkning og overholdelse av «trygg havn»-prinsippene (herunder VS) og «trygg havn»-organisasjonenes relevante personvernbestemmelser, unntatt når organisasjonen har forpliktet seg til å samarbeide med europeiske personvernmyndigheter. Alle bestemmelser i «trygg havn»-prinsippene og VS får anvendelse når de er relevante, med mindre noe annet er fastsatt.

«Personopplysninger» er opplysninger om en identifisert eller identifiserbar person som hører inn under direktivets virkeområde, mottatt av en amerikansk organisasjon fra Den europeiske union og registrert på en hvilken som helst måte.

MELDEPLIKT

En organisasjon må opplyse personer om formålene med innsamlingen og bruken av opplysningene om dem, hvordan de kan ta kontakt med organisasjonen dersom de har forespørsler eller klager, hvilken kategori av tredjemenn opplysningene viderefremmes til og hvilke muligheter og midler organisasjonen tilbyr personene når det gjelder å begrense bruken og viderefremmingen av opplysningene. Meldingen skal være klar og tydelig. Den skal gis første gang en person blir bedt om å gi personopplysninger til organisasjonen eller så snart som mulig etter det, men under alle omstendigheter før organisasjonen bruker slike opplysninger for andre formål enn dem de opprinnelig ble innsamlet eller behandlet for av den organisasjon som har overført opplysningene, eller før den viderefremmer dem for første gang til tredjemann⁽¹⁾.

VALGFRIHET

En organisasjon må gi registrerte personer muligheten til å velge om personopplysninger om dem skal kunne (a) viderefremmes til tredjemann⁽¹⁾ eller (b) brukes for et formål som er uforenlig med de formål opplysningene opprinnelig ble innsamlet for eller som den registrerte på et senere tidspunkt har godkjent. Registrerte personer skal tilbys klare, forståelige, lett tilgjengelige og økonomisk overkommelige ordninger for å utøve slik valgfrihet.

Ved følsomme opplysninger (for eksempel opplysninger om helse, rasemessig eller etnisk opprinnelse, politisk oppfatning, religiøs eller filosofisk overbevisning, fagforeningsmedlemskap eller opplysninger om seksuell liv) skal den registrerte uttrykkelig ha gitt sitt samtykke dersom slike opplysninger skal viderefremmes til tredjemann eller brukes for andre formål enn dem de opprinnelig ble innsamlet for, eller formål som vedkommende på grunnlag av valgfriheten senere har godkjent. Organisasjonen skal under alle omstendigheter behandle enhver opplysning som mottas fra tredjemann som følsom dersom tredjemann betegner og behandler den som sådan.

VIDERE OVERFØRING

En organisasjon må anvende prinsippene om meldeplikt og valgfrihet for å kunne viderefremme opplysninger til tredjemann. Dersom organisasjonen ønsker å overføre opplysninger til en tredjemann som fungerer som mellommann, som beskrevet i fotnoten, må den først bekrefte at tredjemann overholder «trygg havn»-prinsippene eller omfattes av direktivet eller en annen ordning som sikrer et tilstrekkelig vernnivå, eller den må inngå en skriftlig avtale med tredjemann, der denne forplikter seg til å sørge for

⁽¹⁾ Prinsippene om meldeplikt og valgfrihet får ikke anvendelse når opplysninger viderefremmes til tredjemann som fungerer som mellommann og utfører oppgaver på vegne av organisasjonen og i samsvar med organisasjonens instruksjoner. Derimot får prinsippet om videre overføring anvendelse i slike tilfeller.

minst samme vernnivå som kreves i de relevante prinsippene. Dersom organisasjonen imøtekommer disse kravene, skal den ikke holdes ansvarlig (med mindre den avtaler noe annet) dersom tredjemann som den overfører opplysninger til behandler dem på en måte som strider mot eventuelle begrensninger eller tillatelser, med mindre organisasjonen visste eller burde ha visst at tredjemann ville behandle opplysningene på en slik måte og organisasjonen ikke har truffet de nødvendige tiltak for å forhindre slik behandling.

SIKKERHET

Organisasjoner som oppretter, vedlikeholder, bruker eller sprer personopplysninger, må treffe rimelige tiltak for å beskytte opplysningene mot tap eller misbruk, ulovlig tilgang, videreformidling, endring eller ødeleggelse.

DATAINTEGRITET

I henhold til prinsippene må personopplysninger være relevante for de formål de skal brukes til. En organisasjon skal ikke behandle personopplysninger på en måte som er uforenlig med de formål de ble innsamlet for eller formål som den registrerte senere har godkjent. En organisasjon skal i den grad det er nødvendig treffe hensiktsmessige tiltak for å sikre at opplysningene er pålitelige i forhold til tiltenkte formål, samt at de er nøyaktige, fullstendige og ajourførte.

INNSYN

Registrerte personer skal ha tilgang til personopplysninger som en organisasjon er i besittelse av om dem, og de skal ha mulighet til å rette, endre eller slette uriktige opplysninger, med mindre arbeidet eller kostnadene ved å gi tilgang, er uforholdsmessig store i forhold til risikoen for den registrertes personvern, eller med mindre det medfører at en annen persons rettigheter blir krenket.

HÅNDHEVING

Effektivt personvern forutsetter ordninger som sikrer at «trygg havn»-prinsippene blir overholdt, som sikrer klageadgang for registrerte personer som berøres av overtredelser samt at det får følger for en organisasjon dersom den ikke overholder prinsippene. Slike ordninger skal minst omfatte a) lett tilgjengelige, økonomisk overkommelige og uavhengige klageadgangsordninger som gjør det mulig å undersøke og avgjøre hver registrert persons klage eller tvist under henvisning til prinsippene samt å yte erstatning når gjeldende lovgivning eller initiativer gjennom den private sektor gir mulighet for det, b) framgangsmåter for oppfølging for å kontrollere at de forsikringer og bekreftelser organisasjonene gir om sin personvernpraksis er riktige og at denne praksis faktisk blir fulgt, og c) plikt til å avhjelpe problemer som oppstår når en organisasjon som har erklært sin tilslutning til «trygg havn»-ordningen, overtrer prinsippene, samt sanksjoner overfor slike organisasjoner. Sanksjonene skal være tilstrekkelig strenge til å sikre at organisasjonene overholder prinsippene.

Vedlegg

Liste over amerikanske lovfestede organer som er godkjent av Den europeiske union

Den europeiske union godkjenner følgende amerikanske offentlige organers myndighet til å behandle klager og sørge for oppreisning ved urimelig eller villedende praksis og å gi erstatning til berørte personer ved overtredelse av prinsippene som gjennomføres i samsvar med VS:

- Federal Trade Commission på grunnlag av den myndighet organet er tillagt i henhold til avsnitt 5 i Federal Trade Commission Act,
 - De forente staters transportdepartement på grunnlag av den myndighet det er tillagt i henhold til kapittel 49 avsnitt 41712 i United States Code.
-

VEDLEGG II

VANLIGE SPØRSMÅL (VS)

VS 1 – Følsomme opplysninger

Spørsmål: *Skal en organisasjon alltid gi uttrykkelig valgfrihet i forbindelse med følsomme opplysninger?*

Svar: Nei, slik valgfrihet kreves ikke dersom behandlingen 1) er nødvendig for å verne den registrertes eller en annen persons vitale interesser, 2) er nødvendig for å gjøre gjeldende et rettslig krav eller for forsvar, 3) kreves for medisinsk behandling eller diagnose, 4) utføres av en stiftelse, sammenslutning eller annen ideell organisasjon med politiske, filosofiske, religiøse eller fagforeningsmessige formål, som ledd i organisasjonens rettmessige virksomhet og under forutsetning av at behandlingen utelukkende gjelder organisasjonens medlemmer eller personer som på grunn av organisasjonens formål har regelmessig kontakt med den, og at opplysningene ikke videreføres til tredjemann uten de registrertes samtykke, 5) er nødvendig for å oppfylle organisasjonens forpliktelser på det arbeidsrettslige område, eller 6) gjelder opplysninger som den registrerte uttrykkelig har offentliggjort.

VS 2 – Unntak for journalistiske formål

Spørsmål: *Får «trygg havn»-prinsippene anvendelse på personopplysninger som blir innsamlet, lagret eller spredt i journalistisk øyemed, tatt i betraktning De forente staters forfatningsmessige beskyttelse av pressefriheten og direktivets unntak for journalistisk materiale?*

Svar: Når pressefriheten, som er nedfelt i første tillegg til den amerikanske grunnloven, kommer i konflikt med personvernet, skal disse interessene avveies i henhold til første tillegg når det dreier seg om amerikanske personers eller organisasjoners virksomhet. Personopplysninger som er innsamlet med tanke på offentliggjøring, kringkasting eller andre former for offentlig formidling av journalistisk materiale, enten det blir brukt eller ikke, samt opplysninger fra tidligere offentliggjort materiale som spres fra pressearkiver, er ikke underlagt «trygg havn»-prinsippene.

VS 3 – Sekundært ansvar

Spørsmål: *Er internettleverandører, teleselskaper eller andre organisasjoner ansvarlige i henhold til «trygg havn»-prinsippene når de på vegne av en annen organisasjon utelukkende overfører, ruter, svitsjer eller lagrer opplysninger som kan stride mot disse prinsippene?*

Svar: Nei. Verken direktivet eller «trygg havn»-prinsippene gir grunnlag for sekundært ansvar. Når en organisasjon fungerer utelukkende som kanal for opplysninger som overføres av tredjemann, og ikke fastlegger formålene med eller metodene for behandlingen av personopplysningene, kan organisasjonen ikke holdes ansvarlig.

VS 4 – Investeringsbanker og revisorer

Spørsmål: *Investeringsbankers og revisorers virksomhet kan omfatte behandling av personopplysninger uten at den registrerte er blitt underrettet eller har gitt sitt samtykke. Under hvilke omstendigheter er dette tillatt i henhold til prinsippene om meldeplikt, valgfrihet og innsynsrett?*

Svar: Investeringsbanker og revisorer kan behandle personopplysninger uten den registrertes viten bare i det omfang og i det tidsrom som er nødvendig for å oppfylle lovfestede krav eller ivareta offentlige interesser samt under andre omstendigheter der anvendelse av disse prinsippene ville skade organisasjonens rettmessige interesser. Disse rettmessige interessene omfatter overvåking av at foretak overholder sine rettslige forpliktelser og rettmessige regnskapsvirksomhet, og behovet for fortrolighet når det gjelder mulige overtakelser, fusjoner, fellesforetak eller lignende transaksjoner som utføres av investeringsbanker eller revisorer.

VS 5 – Personvernmyndighetenes rolle

Spørsmål: *Hvordan vil foretak som forplikter seg til å samarbeide med personvernmyndigheter i EU, oppfylle disse forpliktelsene, og hvordan vil de bli gjennomført?*

Svar: I henhold til «trygg havn»-prinsippene skal amerikanske organisasjoner som mottar personopplysninger fra EU, forplikte seg til å innføre effektive ordninger som setter dem i stand til å overholde «trygg havn»-prinsippene. Som fastsatt i prinsippet om håndheving skal slike ordninger omfatte a) klageadgang for de registrerte, b) framgangsmåter for oppfølging for å kunne kontrollere at de forsikringer og bekreftelser organisasjonene gir om sin personvernpraksis er riktige og c) plikt til å avhjelpe problemer som oppstår ved overtredelse av prinsippene samt sanksjoner overfor slike organisasjoner. En organisasjon kan oppfylle bokstav a) og c) i prinsippet om håndheving dersom den oppfyller kravene i dette VS om samarbeid med personvernmyndighetene.

En organisasjon kan forplikte seg til å samarbeide med personvernmyndighetene ved at den i sin egsertifisering til De forente staters handelsdepartement (se VS 6 om egsertifisering) bekrefter at den

1. velger å oppfylle kravene i bokstav a) og c) i «trygg havn»-prinsippet om håndheving ved å forplikte seg til å samarbeide med personvernmyndighetene,
2. vil samarbeide med personvernmyndighetene om å undersøke og avgjøre eventuelle klager som mottas innenfor rammen av «trygg havn»-ordningen,
3. vil følge eventuelle anbefalinger fra personvernmyndighetene når disse er av den oppfatning at organisasjonen må treffe særlige tiltak for å overholde «trygg havn»-prinsippene, herunder utbedringstiltak eller betaling av skadeserstatning til registrerte personer som er blitt berørt av at prinsippene ikke overholdes, og at organisasjonen vil gi personvernmyndighetene skriftlig bekreftelse på at slike tiltak er truffet.

Personvernmyndighetenes samarbeid skjer i form av informasjon og anbefalinger på følgende måte:

- Anbefalinger fra personvernmyndighetene vil bli formidlet gjennom et uformelt panel av personvernmyndigheter opprettet på europeisk plan, som blant annet vil bidra til en enhetlig og sammenhengende tilnærming.
- Panelet vil gi anbefalinger til berørte amerikanske organisasjoner med hensyn til uavgjorte klager fra registrerte personer om behandling av personopplysninger som er blitt overført fra EU innenfor rammen av «trygg havn»-ordningen. Disse anbefalingene skal være av en slik art at de sikrer at «trygg havn»-prinsippene anvendes riktig, og skal omfatte opplysninger om den klageadgang berørte personer har og som personvernmyndighetene finner passende.
- Panelet vil gi slike anbefalinger når det får henvist en sak fra de berørte organisasjoner og/eller mottar klager fra enkeltpersoner mot organisasjoner som har forpliktet seg til å samarbeide med personvernmyndighetene innenfor rammen av «trygg havn»-ordningen, og det vil oppfordre og om nødvendig hjelpe slike personer til i første omgang å bruke de interne klagemuligheter som vedkommende organisasjon tilbyr.
- Anbefalinger vil bli gitt først etter at begge parter i en tvist har hatt rimelig anledning til å komme med merknader og framlegge de eventuelle bevis de finner relevant. Panelet vil søke å gi sine anbefalinger så snart som mulig innenfor rammen av en riktig saksbehandling. Normalt vil panelet gi sin anbefaling senest 60 dager etter at klage eller henvisning er mottatt, og om mulig enda raskere.
- Panelet vil offentliggjøre resultatene av sin behandling av klagene, dersom det finner det formålstjenlig.
- Verken panelet eller de enkelte personvernmyndigheter kan holdes ansvarlig for panelets anbefalinger.

Som angitt over, må organisasjoner som velger denne typen tvisteløsning, forplikte seg til å etterkomme personvernmyndighetenes anbefalinger. Dersom en organisasjon ikke har etterkommet anbefalingen senest 25 dager etter at den ble avgitt, og ikke har gitt noen

tilfredsstillende forklaring på forsinkelsen, underretter panelet om at det har til hensikt å henvise saken til the Federal Trade Commission eller et annet amerikansk føderalt organ eller delstatsorgan med lovfestet myndighet til å treffe tvangstiltak i tilfeller av villedende praksis og uriktige opplysninger, eller til å beslutte at det foreligger et alvorlig brudd på samarbeidsavtalen, som dermed skal anses som ugyldig. I sistnevnte tilfelle vil panelet underrette handelsdepartementet (eller dets representanter), for å få endret listen over «trygg havn»-deltakere. Ethvert mislighold av forpliktelsen til å samarbeide med personvernmyndighetene og enhver overtredelse av «trygg havn»-prinsippene, kan forfølges rettslig som villedende praksis i henhold til avsnitt 5 i Federal Trade Commission Act eller tilsvarende lovgivning.

Organisasjoner som velger dette alternativ, vil bli avkrevd en årsavgift som skal dekke panelets driftskostnader, og de kan i tillegg bli bedt om å dekke eventuelle oversettelseskostnader som oppstår som følge av panelets behandling av henvisninger eller klager mot organisasjonene. Årsavgiften skal ikke være høyere enn 500 USD og vil være lavere for mindre bedrifter.

Organisasjoner som slutter seg til «trygg havn»-ordningen, vil i et tidsrom på tre år ha mulighet til å samarbeide med personvernmyndighetene. Dersom altfor mange amerikanske organisasjoner velger denne ordningen, vil personvernmyndighetene vurdere ordningen på nytt ved slutten av dette tidsrommet.

VS 6 – Egensertifisering

Spørsmål: *Hvordan skal en organisasjon sertifisere at den overholder «trygg havn»-prinsippene?*

Svar: En organisasjon kan dra fordel av «trygg havn»-ordningen fra og med den dagen den erklærer sin tilslutning til prinsippene ved egensertifisering overfor De forente staters handelsdepartement (eller dets representant) i samsvar med retningslinjene nedenfor.

En organisasjon kan slutte seg til «trygg havn»-ordningen ved egen sertifisering ved å sende et brev til De forente staters handelsdepartement (eller dets representant), som skal være undertegnet av en ledende medarbeider på vegne av organisasjonen som slutter seg til «trygg havn»-ordningen, og skal inneholde minst følgende opplysninger:

1. organisasjonens navn, postadresse, e-postadresse, telefon- og faksnummer,
2. en beskrivelse av organisasjonens virksomhet med hensyn til personopplysninger mottatt fra EU, og
3. en beskrivelse av organisasjonens personvernprogram med hensyn til slike personopplysninger, herunder a) hvordan programmet skal gjøres tilgjengelig for offentligheten, b) hvilken dato det trer i kraft, c) en kontaktadresse for klager, anmodninger om innsyn og andre spørsmål som kan oppstå i forbindelse med «trygg havn»-ordningen, d) hvilket lovfestet organ som har myndighet til å behandle klager mot organisasjonen på grunn av urimelig eller villedende praksis og brudd på lover eller bestemmelser om personvern (oppført i vedlegget til prinsippene), e) navnet på enhver personvernordning som organisasjonen deltar i, f) kontrollordninger (intern kontroll, tredjemannskontroll)⁽¹⁾ og g) uavhengige klageinstanser som kan behandle uløste saker.

Dersom en organisasjon ønsker at «trygg havn»-ordningen også skal gjelde for opplysninger om menneskelige ressurser som overføres fra EU for å bli brukt innenfor rammene av et arbeidsforhold, kan den det dersom det finnes et lovfestet organ med myndighet til å behandle klager mot organisasjonen som gjelder opplysninger om menneskelige ressurser som står oppført i vedlegget til prinsippene. I tillegg må organisasjonen angi dette i egensertifiseringsbrevet, og erklære at den forplikter seg til å samarbeide med vedkommende EU-myndigheter i samsvar med VS 9 og 5 samt at den akter å følge disse myndighetenes anbefalinger.

De forente staters handelsdepartement (eller dets representant) vil føre en liste over alle organisasjoner som har sendt inn egensertifiseringsbrev, og som dermed har rett til å nyte godt av «trygg havn»-fordelene, og vil ajourføre denne listen på grunnlag av de brev og meldinger det mottar hvert år i samsvar med VS 11. Slike egensertifiseringsbrev bør sendes inn minst én

⁽¹⁾ Se VS 7 om kontroll.

gang i året. I motsatt fall vil organisasjonen bli strøket fra listen og ikke lenger nyte godt av «trygg havn»-fordelene. Både listen og organisasjonenes egensertifiseringsbrev vil bli offentliggjort. Alle organisasjoner som ved egensertifisering slutter seg til «trygg havn»-ordningen, skal også i sine offentliggjorte personvernprogrammer angi at de følger «trygg havn»-prinsippene.

Forpliktelsen til å følge «trygg havn»-prinsippene er ikke tidsbegrenset for opplysninger mottatt i det tidsrom organisasjonen nyter godt av «trygg havn»-prinsippene. Forpliktelsen innebærer at organisasjonen må fortsette å anvende prinsippene på slike opplysninger så lenge den lagrer, bruker eller videreformidler dem, selv om organisasjonen av en eller annen grunn senere skulle forlate ordningen.

En organisasjon som som følge av fusjon eller overtakelse vil opphøre som eget rettssubjekt, må melde dette på forhånd til De forente staters handelsdepartement (eller dets representant). I meldingen skal det også angis om den enhet som overtar, eller den enhet som oppstår ved fusjonen, 1) fortsatt vil være bundet av «trygg havn»-prinsippene i henhold til de lovbestemmelser som gjelder for overtakelsen eller fusjonen, eller 2) velger ved egensertifisering å slutte seg til «trygg havn»-prinsippene eller treffer andre vermetiltak, for eksempel en skriftlig avtale som sikrer at «trygg havn»-prinsippene overholdes. Dersom verken 1) eller 2) får anvendelse, må alle opplysninger som er mottatt under «trygg havn»-ordningen, umiddelbart slettes.

En organisasjon trenger ikke å anvende «trygg havn»-prinsippene på alle personopplysninger, men den må anvende prinsippene på personopplysninger som den mottar fra EU etter at den har sluttet seg til «trygg havn»-ordningen.

En organisasjon som gir uriktige opplysninger til offentligheten med hensyn til organisasjonens tilslutning til «trygg havn»-prinsippene, kan bringes inn for Federal Trade Commission eller et annet offentlig organ. Uriktige opplysninger til De forente staters handelsdepartement (eller dets representant) kan medføre rettslig forfølgning i henhold til False Statements Act (USC 18, §1001).

VS 7 – Kontroll

Spørsmål: Hvilke framgangsmåter for oppfølging bruker organisasjoner for å kontrollere at de forsikringer og bekreftelser de har avgitt om sine personverniltak er sanne og at disse tiltakene gjennomføres som beskrevet og i samsvar med «trygg havn»-prinsippene?

Svar: For å oppfylle kravet om kontroll i prinsippet om håndheving kan en organisasjon kontrollere slike forsikringer og bekreftelser enten gjennom egenvurdering eller ekstern samsvars kontroll.

Ved egenvurdering skal det kontrolleres om organisasjonens offentliggjorte personvernprogram med hensyn til personopplysninger mottatt fra EU er riktig, dekkende, om det i tilstrekkelig grad er blitt offentliggjort, er fullt ut iverksatt og tilgjengelig. Det må også framgå at personvernprogrammet er i samsvar med «trygg havn»-prinsippene, at personer blir underrettet om eventuelle interne ordninger for behandling av klager samt om uavhengige klageinstanser, at det finnes framgangsmåter for å gi ansatte opplæring i hvordan de skal gjennomføre programmet og for å gripe inn dersom programmet ikke følges, samt at organisasjonen har interne framgangsmåter for regelmessig og objektiv kontroll av at ovenstående etterleves. En ledende medarbeider eller en annen representant med fullmakt i organisasjonen skal minst én gang i året undertegne en erklæring om at det er foretatt egenvurdering, og denne erklæringen skal gjøres tilgjengelig på anmodning, eller i forbindelse med en undersøkelse eller en klage over manglende overholdelse.

Organisasjoner skal dokumentere iverksettingen av sine personvernprogrammer under «trygg havn»-ordningen, og på anmodning, i forbindelse med undersøkelser eller klager over manglende overholdelse, gjøre slik dokumentasjon tilgjengelig for den ansvarlige klageinstans eller for den instans som har ansvar for saker om urimelig eller villedende praksis.

Dersom en organisasjon velger ekstern samsvars kontroll, skal kontrollen påvise at organisasjonens personvernprogram med hensyn til personopplysninger mottatt fra EU, er i samsvar med «trygg havn»-prinsippene, at programmet følges og at personer blir underrettet om klageinstanser. Kontrollmetodene kan uten begrensning omfatte revisjon, stikkprøver, bruk av falske opplysninger som «lokkemat» eller av andre teknologiske verktøy som måtte passe. Kontrolløren, en ledende medarbeider eller en annen representant i organisasjonen med

fullmakt skal minst én gang i året undertegne en erklæring om at det er foretatt ekstern samsvarskontroll, og denne erklæringen skal gjøres tilgjengelig på anmodning eller i forbindelse med en undersøkelse eller klage over manglende overholdelse.

VS 8 – Innsyn

Innsynsprinsippet:

Registrerte personer skal ha tilgang til personopplysninger som en organisasjon er i besittelse av om dem, og de skal ha mulighet til å rette, endre eller slette uriktige opplysninger, med mindre arbeidet eller kostnadene ved å gi tilgang, er uforholdsmessig store i forhold til risikoen for privatpersonens personvern, eller med mindre det medfører at en annen persons rettigheter blir krenket.

1. Spørsmål: *Er retten til innsyn uinnskrenket?*

1. Svar: Nei. I samsvar med «trygg havn»-prinsippene er innsynsretten av avgjørende betydning for personvernet. Særlig gir den personer mulighet til å kontrollere at opplysningene om dem er riktige. Likevel er en organisasjons plikt til å gi innsyn i de personopplysninger den har om en person, underlagt forholdsmessighets- og rimelighetsprinsippet, og må i visse tilfeller tilpasses. Det framgår klart av de forklarende merknader til OECDs retningslinjer av 1980 om personvern (Explanatory Memorandum to the 1980 OECD Privacy Guidelines) at en organisasjons plikt til å gi innsyn, ikke er absolutt. Organisasjonen er ikke forpliktet til å undersøke like grundig som for eksempel ved en stevning, og det kreves heller ikke at organisasjonen gir tilgang til organisasjonens ulike lagringsmedier for opplysninger.

Erfaringen har snarere vist at når en person anmoder om innsyn, bør organisasjonen først og fremst spørre seg hvilke grunner personen har. Dersom for eksempel en anmodning om innsyn er vag eller for omfattende, kan organisasjonen innlede en dialog med personen for bedre å forstå bakgrunnen for anmodningen og dermed lettere finne de relevante opplysningene. Organisasjonen kan spørre om hvilken del eller hvilke deler av organisasjonen personen har vært i kontakt med, og/eller hvilken art opplysninger (eller hvilket formål) anmodningen gjelder. En person trenger imidlertid ikke å begrunne en anmodning om innsyn i opplysninger om seg selv.

Kostnader og arbeidsbyrde er viktige faktorer som det må tas hensyn til, men de er ikke avgjørende for om det er rimelig å gi innsyn. Dersom for eksempel opplysningene er grunnlag for avgjørelser som er av vesentlig betydning for den enkelte (for eksempel avslag på eller tildeling av viktige fordeler som forsikring, lån eller ansettelse), må organisasjonen i samsvar med de øvrige bestemmelsene i VS gi innsyn i slike opplysninger, selv om det medfører stor arbeidsbyrde eller høye kostnader.

Dersom opplysningene det anmodes om ikke er følsomme eller ikke vil være grunnlag for avgjørelser av vesentlig betydning for den registrerte (for eksempel ikke-følsomme markedsføringsopplysninger som brukes for å avgjøre om den registrerte skal få tilsendt en katalog), men er lett tilgjengelige og det ikke medfører store kostnader å stille dem til rådighet, må organisasjonen gi innsyn i de faktiske opplysninger den har om den registrerte. Disse opplysningene kan inneholde fakta innsamlet fra den registrerte selv i forbindelse med en transaksjon, eller fakta mottatt fra andre, men som gjelder den registrerte.

I henhold til selve innsynsprinsippet skal organisasjoner alltid være velvillige med hensyn til å gi innsyn. Dersom for eksempel visse opplysninger skal beskyttes og lett kan skilles fra andre opplysninger som det anmodes om innsyn i, skal organisasjonen redigere bort de følsomme opplysningene og gi innsyn i de øvrige. Dersom organisasjonen i særlige tilfeller avgjør at innsyn ikke kan gis, skal den begrunne avgjørelsen overfor den registrerte og opplyse om hvor vedkommende kan henvende seg for nærmere opplysninger.

2. Spørsmål: *Hva er fortrolige forretningsopplysninger, og kan organisasjoner nekte innsyn for å beskytte slike opplysninger?*

2. Svar: Fortrolige forretningsopplysninger (slik begrepet brukes i Federal Rules of Civil Procedure on discovery) er opplysninger som en organisasjon har truffet tiltak for å beskytte fordi videreformidling ville være til fordel for en konkurrent i markedet. Hvilket

dataprogram en organisasjon bruker, for eksempel et modelleringsprogram eller detaljer ved dette programmet, kan være fortrolige forretningsopplysninger. Dersom forretningsopplysninger lett kan skilles fra andre opplysninger som det anmodes om innsyn i, skal organisasjonen redigere bort de fortrolige forretningsopplysningene og gi innsyn i de øvrige. En organisasjon kan nekte eller begrense innsyn dersom den ved å gi innsyn risikerer å avsløre sine egne fortrolige forretningsopplysninger som definert ovenfor, for eksempel de markedsføringskonsepter og -klassifiseringer den har utarbeidet, eller andres fortrolige forretningsopplysninger som i henhold til en avtaleforpliktelse skal behandles fortrolig, når en slik forpliktelse til fortrolighet er vanlig eller pålagt.

3. Spørsmål: *Er det tilstrekkelig at organisasjonen formidler personopplysningene til den registrerte fra sine databaser, eller skal det gis tilgang til selve databasen?*

3. Svar: En organisasjon kan gi innsyn ved å formidle de relevante opplysningene til den registrerte, som dermed ikke skal ha tilgang til organisasjonens database.

4. Spørsmål: *Må en organisasjon omstrukturere sine databaser for å kunne gi innsyn?*

4. Svar: En organisasjon skal gi innsyn bare i den grad den lagrer opplysningene. Innsynsprinsippet innebærer ikke plikt til å oppbevare, vedlikeholde, omorganisere eller omstrukturere registre med personopplysninger.

5. Spørsmål: *Av disse svarene framgår det at innsyn kan nektes i visse tilfeller. I hvilke andre tilfeller kan en organisasjon nekte personer innsyn i personopplysninger om dem selv?*

5. Svar: Slike tilfeller er svært begrensede, og det må gis en konkret begrunnelse for å nekte innsyn. En organisasjon kan nekte innsyn i opplysninger dersom videreformidling antas å vanskeliggjøre vern av viktige offentlige interesser som for eksempel nasjonal sikkerhet, forsvar eller offentlig sikkerhet. I tillegg kan innsyn nektes når personopplysninger behandles utelukkende for statistiske formål eller forskningsformål. Innsyn kan også nektes eller begrenses i tilfeller der

- a. innsyn vanskeliggjør gjennomføring eller håndheving av loven, herunder forebygging, undersøkelser eller oppklaring av lovovertridelser eller retten til rettferdig rettergang,
- b. innsyn vanskeliggjør private søksmål, herunder forebygging, undersøkelse eller oppklaring av rettslige krav eller retten til rettferdig rettergang,
- c. innsyn medfører at personopplysninger om andre personer, som ikke kan redigeres bort, blir videreformidlet,
- d. innsyn er et brudd på lovbestemte eller yrkesmessige rettigheter eller plikter,
- e. innsyn er et brudd på den nødvendige fortrolighet i forbindelse med framtidige eller nåværende forhandlinger, for eksempel med hensyn til overtakelse av børsnoterte selskaper,
- f. innsyn vanskeliggjør sikkerhetsundersøkelser av arbeidstakere eller behandling av klager,
- g. innsyn er til skade for den fortrolighet som kan være nødvendig i begrensede tidsrom i forbindelse med personalplanlegging og omstrukturering,
- h. innsyn er til skade for den fortrolighet som kan være nødvendig i forbindelse med overvåking, inspeksjon eller regulerende funksjoner som hører med til en god økonomiforvaltning,
- i. innsyn under andre omstendigheter medfører en uforholdsmessig stor arbeidsbyrde eller store kostnader eller at andre personers legitime rettigheter eller interesser blir krenket.

En organisasjon som påberoper seg et unntakstilfelle, må bevise at et slikt unntakstilfelle faktisk foreligger (slik det vanligvis er tilfellet). Som angitt over skal personer som har anmodet om innsyn, opplyses om begrunnelsene for at innsyn nektes eller begrenses, samt om hvor de kan henvende seg for nærmere opplysninger.

6. Spørsmål: *Kan en organisasjon kreve gebyr for å dekke kostnader ved å gi innsyn?*
6. Svar: Ja. OECD-retningslinjene gir organisasjoner rett til å kreve gebyr såfremt det ikke er uforholdsmessig høyt. Dermed kan organisasjonene kreve et rimelig gebyr for innsyn. Innkreving av gebyr kan bidra til å forhindre gjentatte og useriøse anmodninger om innsyn.
- Organisasjoner som selger offentlig tilgjengelig opplysninger kan dermed kreve sitt ordinære gebyr ved anmodninger om innsyn. Den registrerte kan også søke om innsyn i opplysninger om seg selv hos den organisasjonen som opprinnelig samlet inn opplysningene.
- Dersom den registrerte tilbyr seg å dekke kostnadene, kan innsyn ikke nektes av kostnadsgrunner.
7. Spørsmål: *Er en organisasjon forpliktet til å gi innsyn i personopplysninger som stammer fra offentlige registre?*
7. Svar: Offentlige registre er registre som forvaltes av offentlige organer eller enheter på ulike nivåer som er tilgjengelige for offentligheten. Det er ikke nødvendig å anvende innsynsprinsippet på slike opplysninger med mindre de kombineres med andre personopplysninger, unntatt når små mengder opplysninger fra registre som ikke er offentlig tilgjengelige brukes til å indeksere eller organisere opplysninger fra offentlige registre. Vilkår for innsyn fastsatt av vedkommende myndighet skal imidlertid overholdes. Når opplysninger fra offentlige registre kombineres med andre opplysninger som ikke er offentlig tilgjengelige (andre enn dem som er nevnt særskilt ovenfor), skal en organisasjon imidlertid gi innsyn i alle disse opplysningene såfremt de ikke omfattes av andre unntak.
8. Spørsmål: *Må innsynsprinsippet anvendes på offentlig tilgjengelige personopplysninger?*
8. Svar: På samme måte som med opplysninger fra offentlige registre (se spørsmål 7), er det ikke nødvendig å gi innsyn i opplysninger som allerede er offentlig tilgjengelige, så lenge de ikke er kombinert med ikke-offentlige opplysninger.
9. Spørsmål: *Hvordan kan en organisasjon beskytte seg mot gjentatte og useriøse anmodninger om innsyn?*
9. Svar: En organisasjon er ikke forpliktet til å svare på slike anmodninger om innsyn. Derfor kan organisasjonene kreve et rimelig gebyr og fastsette en passende grense for hvor mange ganger de vil behandle anmodninger om innsyn fra én person innenfor et gitt tidsrom. Når de fastsetter slike begrensninger, må organisasjonene ta hensyn til faktorer som hvor ofte opplysningene ajourføres, for hvilket formål de anvendes og arten av opplysninger det dreier seg om.
10. Spørsmål: *Hvordan kan en organisasjon beskytte seg mot svikaktige anmodninger om innsyn?*
10. Svar: En organisasjon er ikke forpliktet til å gi innsyn med mindre den mottar tilstrekkelige opplysninger til å bekrefte identiteten til den personen som anmoder om innsyn.
11. Spørsmål: *Er det noen frist for behandlingen av anmodninger om innsyn?*
11. Svar: Ja, organisasjonene bør svare uten unødige forsinkelser og innenfor en rimelig frist. Som det framgår av de forklarende merknadene til OECDs retningslinjer av 1980, kan dette kravet oppfylles på ulike måter. For eksempel kan en behandlingsansvarlig som regelmessig sender opplysninger til de registrerte, være fritatt for plikten til omgående å besvare individuelle anmodninger.

VS 9 – Menneskelige ressurser

1. Spørsmål: *Gjelder «trygg havn»-ordningen for personopplysninger som er innsamlet i forbindelse med arbeidsforhold, og som overføres fra EU til USA?*
1. Svar: Ja, «trygg havn»-ordningen gjelder når et selskap i EU overfører personopplysninger om sine ansatte (nåværende eller tidligere), som er innsamlet i forbindelse med arbeidsforholdet, til en tjenesteyter i USA, det være seg et morselskap, et tilknyttet eller et ikke-tilknyttet foretak, som er tilsluttet «trygg havn»-ordningen. I slike tilfeller skal

innsamlingen og behandlingen av opplysningene før overføring til USA være i samsvar med den nasjonale lovgivningen i den EU-staten der de ble innsamlet, og alle vilkår eller begrensninger for overføring i henhold til denne lovgivning skal overholdes.

«Trygg havn»-prinsippene er relevante bare ved overføring av eller innsyn i individuelt identifiserbare opplysninger. Statistikkrapporter som bygger på samlede ansettelsesopplysninger og/eller bruk av opplysninger som er gjort anonyme eller pseudonyme, utgjør ikke noe problem for personvernet.

2. Spørsmål: *Hvordan får prinsippene om meldeplikt og valgfrihet anvendelse på slike opplysninger?*

2. Svar: En amerikansk organisasjon som har mottatt ansettelsesopplysninger fra EU innenfor rammen av «trygg havn»-ordningen, kan videreformidle dem til tredjemann og/eller bruke dem for andre formål bare dersom det skjer i samsvar med prinsippene om meldeplikt og valgfrihet. Dersom en amerikansk organisasjon for eksempel har til hensikt å bruke personopplysninger som er samlet inn i forbindelse med et ansettelsesforhold til formål som ikke gjelder ansettelsesforholdet, for eksempel markedsføring, må organisasjonen først gi de berørte personene en valgmulighet, med mindre de allerede har gitt samtykke til slik bruk av opplysningene. De ansattes valg må heller ikke føre til at deres yrkeskarriere begrenses eller til straffetiltak mot dem.

Det bør bemerkes at visse vilkår som får alminnelig anvendelse på overføringer fra visse medlemsstater kan utelukke annen bruk av slike opplysninger, selv etter overføring til land utenfor EU, og slike vilkår skal oppfylles.

I tillegg skal arbeidsgivere bestrebe seg på å imøtekomme arbeidstakerens ønsker om personvern. Dette kan for eksempel innebære at det gis bare begrenset innsyn i opplysninger, at visse opplysninger anonymiseres eller at det brukes koder eller pseudonymer, dersom de virkelige navnene ikke er nødvendige for formålet med opplysningene.

En organisasjon er ikke forpliktet til å anvende prinsippene om meldeplikt og valgfrihet i det omfang og i det tidsrom det er nødvendig for ikke å skade organisasjonens rettmessige interesser i forbindelse med forfremmelser, ansettelser eller lignende personalsaker.

3. Spørsmål: *Hvordan anvendes innsynsprinsippet?*

3. Svar: I VS om innsyn gis en veiledning om årsaker til å nekte innsyn eller gi begrenset innsyn i opplysninger om menneskelige ressurser. Arbeidsgivere i EU må naturligvis overholde nasjonale bestemmelser og sørge for at arbeidstakere i EU har tilgang til slike opplysninger i samsvar med lovgivningen i sine hjemstater, uansett hvor opplysningene behandles og lagres. «Trygg havn»-ordningen forutsetter at en organisasjon som behandler slike opplysninger i USA, vil samarbeide for å gi innsyn enten direkte eller gjennom arbeidsgiveren i EU.

4. Spørsmål: *Hvordan vil «trygg havn»-prinsippene bli håndhevet med hensyn til ansettelsesopplysninger?*

4. Svar: Såfram opplysningene anvendes bare innenfor rammen av arbeidsforholdet, er det selskapet i EU som har hovedansvaret for opplysningene overfor arbeidstakeren. Det vil si at når europeiske arbeidstakere klager over brudd på sine personvernrettigheter, og ikke er tilfreds med utfallet av framgangsmåtene for internkontroll, klage eller anke (eller en hvilken som helst annen framgangsmåte for klage etter avtale med en fagforening), skal de henvises til vedkommende nasjonale myndigheter for personvern eller arbeid der vedkommende arbeider. Dette omfatter også saker der den påståtte feilbehandlingen av opplysninger har funnet sted i De forente stater, og ansvaret ligger hos den amerikanske organisasjonen som har mottatt opplysningene fra arbeidsgiveren, og ikke hos arbeidsgiveren, noe som snarere innebærer et eventuelt brudd på «trygg havn»-prinsippene enn på nasjonale lovbestemmelser som gjennomfører personverndirektivet. Dette vil være den mest effektive framgangsmåten for å håndtere de ofte overlappende rettigheter og forpliktelser som er fastsatt i nasjonal arbeidsrett og arbeidsavtaler samt i personvernlovgivningen.

En amerikansk organisasjon som deltar i «trygg havn»-ordningen, og som bruker opplysninger om menneskelige ressurser overført fra EU innenfor rammene av et arbeidsforhold, og som ønsker at slike overføringer skal komme inn under «trygg

havn»-ordningen, må derfor i slike tilfeller forplikte seg til å samarbeide ved undersøkelser som foretas av vedkommende EU-myndigheter, og følge deres anbefalinger. De personvernmyndighetene som har sagt seg villig til å samarbeide på denne måten, skal underrette Europakommisjonen og De forente staters handelsdepartement. Dersom en amerikansk organisasjon som deltar i «trygg havn»-ordningen, ønsker å overføre opplysninger om menneskelige ressurser fra en medlemsstat som ikke har sagt seg villig til slikt samarbeid, gjelder bestemmelsene i VS 5.

VS 10 – Artikkel 17-avtaler

Spørsmål: *Når opplysninger overføres fra EU til De forente stater utelukkende for behandlingsformål, er det da nødvendig med en avtale, selv om databehandleren deltar i «trygg havn»-ordningen?*

Svar: Ja. De behandlingsansvarlige i EU skal alltid inngå en avtale når opplysninger overføres utelukkende for behandling, uansett om behandlingen foregår innenfor eller utenfor EU. Formålet med avtalen er å beskytte den behandlingsansvarliges interesser, dvs. den person eller enhet som fastsetter formålet med behandlingen og midlene som skal anvendes, og som bærer det fulle ansvar overfor den eller de berørte personer. Det skal dermed framgå av avtalen hvilken type behandling som skal foretas og hvilke tiltak som er nødvendige for å sikre at opplysningene beskyttes.

Det er derfor ikke nødvendig for en amerikansk organisasjon som deltar i «trygg havn»-ordningen, og som mottar personopplysninger fra EU utelukkende for behandlingsformål, å anvende prinsippene på slike opplysninger, fordi den behandlingsansvarlige i EU bærer ansvaret overfor den registrerte i samsvar med relevante EU-bestemmelser (som kan være strengere enn de tilsvarende «trygg havn»-prinsippene).

Fordi deltakere i «trygg havn»-ordningen sørger for et tilstrekkelig vernnivå, kreves det ikke forhåndsgodkjenning av avtaler med slike deltakere om overføring av opplysninger for behandlingsformål (eller medlemsstatene gir automatisk slik godkjenning), slik det kreves for avtaler med mottakere som ikke deltar i «trygg havn»-ordningen, eller som på annet vis ikke kan sørge for tilstrekkelig vern.

VS 11 – Tvisteløsning og håndheving

Spørsmål: *Hvordan skal kravene til tvisteløsning fastsatt i håndhevingsprinsippet gjennomføres, og hva skjer når en organisasjon gjentatte ganger overtrer prinsippene?*

Svar: I håndhevingsprinsippet er det fastsatt hvordan «trygg havn»-prinsippene skal håndheves. I VS 7 om kontroll er det fastsatt hvordan kravene i prinsippets bokstav b) skal overholdes. Dette VS 11 omhandler bokstav a) og c), som begge stiller krav til uavhengige klageadgangsordninger. Klageadgangsordningene kan være av ulik art, men de må oppfylle kravene i håndhevingsprinsippet. Organisasjoner kan oppfylle kravene på følgende måter: 1) ved å overholde personvernprogrammer som er utviklet innenfor den private sektor, der «trygg havn»-prinsippene er innlemmet, og som omfatter effektive håndhevingsordninger tilsvarende kravene beskrevet i håndhevingsprinsippet, 2) ved å underkaste seg de tilsynsmyndigheter som er opprettet ved lov eller administrativt, og som ivaretar behandling av individuelle klager og tvisteløsning, eller 3) ved å forplikte seg til å samarbeide med personvernmyndigheter innenfor EU eller deres godkjente representanter. Denne listen er veiledende og ikke uttømmende. Den private sektor kan innføre andre håndhevingsordninger, såfremt kravene i håndhevingsprinsippet og i «Vanlige spørsmål» oppfylles. Det bør bemerkes at kravene i håndhevingsprinsippet kommer i tillegg til kravene i avsnitt 3 i innledningen til prinsippene, om at organisasjoner som baserer seg på selvregulering, skal kunne holdes ansvarlige i henhold til avsnitt 5 i Federal Trade Commission Act eller tilsvarende lovgivning.

Klageadgangsordninger

Forbrukere skal oppfordres til å klage til den berørte organisasjon, før de henvender seg til uavhengige klageinstanser. Det finnes ulike kjennetegn på en uavhengig klageinstans, for eksempel mulighet til innsyn i sammensetning og finansiering eller dokumentert erfaring. Som håndhevingsprinsippet krever, skal klageadgangsordningene være lett tilgjengelige og økonomisk overkommelige for den registrerte. Tvisteløsningsinstanser skal undersøke hver

klage som mottas fra registrerte personer, med mindre klagen åpenbart er ubegrunnede eller useriøse. Dette utelukker ikke at organisasjoner som har opprettet klageadgangsordninger, innfører kriterier for hvilke klager som skal behandles, men slike kriterier må være klare og begrunnede (for eksempel kriterier for å utelukke klager som faller utenfor programmets virkeområde eller som bør behandles av en annen instans) og skal ikke føre til at plikten til å undersøke rettmessige klager forsømmes. I tillegg bør klageinstansene gi vedkommende som framsetter en klage fullstendige og lett tilgjengelige opplysninger om framgangsmåten for tvisteløsning. Slike opplysninger skal omfatte en beskrivelse av instansens personvernpraksis, i samsvar med «trygg havn»-prinsippene⁽²⁾. Instansene bør også delta i samarbeidet om å utvikle hjelpemidler, som for eksempel standardiserte klageskjemaer, som skal gjøre det enklere å behandle klager.

Klageadgang og sanksjoner

Klageadgang overfor tvisteløsningsinstansene bør føre til at organisasjonen så langt det lar seg gjøre opphever eller utbedrer følgene av overtredelsen og at organisasjonens framtidige behandling av opplysninger skjer i samsvar med prinsippene, samt eventuelt at behandlingen av personopplysninger om den person som har framsatt klagen, opphører. Sanksjonene må være tilstrekkelig strenge til å sikre at organisasjonene følger prinsippene. En rekke sanksjoner av ulik strenghetsgrad vil gi tvisteløsningsinstansene muligheten til å reagere på passende måte på ulike grader av manglende overholdelse. Slike sanksjoner bør omfatte både offentliggjøring av overtredelser og krav om i visse tilfeller å slette opplysninger⁽³⁾. Andre mulige sanksjoner er midlertidig oppheving eller tilbaketrekking av en godkjenning, erstatning til registrerte personer for tap som følge av overtredelse av prinsippene og forbud. Organer for tvisteløsning og selvregulering i den private sektor skal underrette vedkommende offentlige organ eller domstolene om «trygg havn»-organisasjoner som ikke retter seg etter deres avgjørelser, samt underrette De forente staters handelsdepartement (eller dets representant).

Tiltak fra Federal Trade Commission (FTC)

FTC har forpliktet seg til først og fremst å behandle saker om påståtte overtredelser som det får henvist fra selvreguleringsorganisasjoner på personvernområdet, for eksempel BBBOnline og TRUSTe, og fra EU-medlemsstatene, for å fastslå om det foreligger brudd på avsnitt 5 i Federal Trade Commission Act, som forbyr urimelig og villedende atferd eller praksis innenfor handel. Dersom FTC kommer til at det sannsynligvis foreligger brudd på avsnitt 5, kan den saken løses ved å søke å oppnå et administrativt forbud mot vedkommende praksis eller ved å framsette en klage til en føderal domstol, som kan resultere i en dom med samme virkning dersom klageren får medhold. FTC kan oppnå sivilrettslige sanksjoner ved overtredelse av et administrativt forbud, og kan innlede sivilrettslige eller strafferettslige saker ved unnlatelse av å etterkomme føderale rettsavgjørelser. FTC vil underrette De forente staters handelsdepartement om alle slike tiltak. Handelsdepartementet oppfordrer andre offentlige organer til å underrette departementet om den endelige avgjørelsen i slike saker, eller andre avgjørelser om overholdelse av «trygg havn»-prinsippene.

Gjentatte overtredelser av prinsippene

Dersom en organisasjon gjentatte ganger unnlater å overholde prinsippene, har den ikke lenger rett til å nyte godt av «trygg havn»-fordelene. Gjentatte overtredelser av prinsippene foreligger når en organisasjon som har foretatt egensertifisering overfor handelsdepartementet (eller dets representant), nekter å etterkomme den endelige avgjørelsen fra et selvreguleringsorgan eller et offentlig organ, eller når et slikt organ fastslår at en organisasjon overtrer prinsippene så ofte at den ikke lenger er troverdig når den påstår at den overholder dem. I slike tilfeller skal organisasjonen umiddelbart underrette De forente staters handelsdepartement (eller dets representant) om dette. Dersom organisasjonen unnlater å gjøre dette, kan det gi grunnlag for rettslig forfølgning i henhold til False Statements Act (18 USC §1001).

(2) Tvisteløsningsinstanser er ikke forpliktet til å overholde håndhevingsprinsippet. De kan også fravike prinsippene når det i forbindelse med deres spesifikke oppgaver oppstår forpliktelser eller gis uttrykkelige tillatelser.

(3) Tvisteløsningsinstanser kan anvende slike sanksjoner etter eget skjønn. Ved vurdering av krav om at opplysninger skal slettes, må det tas i betraktning hvor følsomme de berørte opplysningene er, og om organisasjonen har innsamlet, brukt eller videreformidlet opplysninger på en måte som åpenbart strider mot prinsippene.

Departementet (eller dets representant) vil føre opp på den offentlige listen over organisasjoner som tiltrer «trygg havn»-ordningen ved egensertifisering, alle meldinger det mottar om gjentatte overtredelser, uansett om de er mottatt fra organisasjonen selv, et selvreguleringsorgan eller et offentlig organ, men etter først å ha gitt vedkommende organisasjon en tretti (30) dagers frist og en mulighet til å svare. Det vil altså klart framgå av den offentlige listen som føres av handelsdepartementet (eller dets representant) hvilke organisasjoner som er anerkjent som «trygg havn»-organisasjoner, og hvilke som ikke lenger er det.

En organisasjon som søker om å bli underlagt et selvreguleringsorgan for på nytt å kvalifisere seg for «trygg havn»-ordningen, må gi dette organet alle opplysninger om sin tidligere deltaking i «trygg havn»-ordningen.

VS 12 – Valgfrihet og tidsfrister for å reservere seg

Spørsmål: *Gir prinsippet om valgfrihet en person mulighet til å velge bare i begynnelsen av et registreringsforhold, eller når som helst?*

Svar: Formålet med prinsippet om valgfrihet er i alminnelighet å sikre at personopplysninger brukes og videreformidles i samsvar med den registrertes forventninger og ønsker. Derfor skal registrerte personer til enhver tid ha mulighet til å reservere seg mot at personopplysninger om dem brukes i direkte markedsføring, innenfor rimelige tidsfrister som organisasjonen fastsetter, for eksempel for at den skal få tid til å iverksette den enkeltes valg. En organisasjon kan også kreve tilstrekkelige opplysninger til å kunne fastslå identiteten til den person som ønsker å reservere seg. I De forente stater kan registrerte personer utøve denne valgfriheten gjennom en sentral ordning for dette formål, for eksempel Direct Marketing Association's Mail Preference Service. Organisasjoner som deltar i Direct Marketing Association's Mail Preference Service, skal opplyse forbrukere som ikke ønsker å motta reklame, om denne tjenesten. Under alle omstendigheter skal registrerte personer gis mulighet til på en lett tilgjengelig og økonomisk overkommelig måte å utøve denne valgmuligheten.

En organisasjon kan også bruke opplysninger til visse direkte markedsføringsformål, når det i praksis ikke er mulig å gi den registrerte muligheten til å reservere seg før opplysningene brukes, dersom organisasjonen samtidig (og når som helst, på anmodning) gir den registrerte mulighet (kostnadsfritt) til å reservere seg mot å motta ytterligere direkte markedsføring, og dersom organisasjonen retter seg etter personens ønsker.

VS 13 – Reiseopplysninger

Spørsmål: *Når kan opplysninger om plassereservasjon for flypassasjerer og andre reiseopplysninger, for eksempel opplysninger om hyppige flyreiser, bestilling av hotellrom eller om særlige behov, for eksempel måltider tilberedt etter visse religiøse retningslinjer eller fysisk assistanse, overføres til organisasjoner utenfor EU?*

Svar: Slike opplysninger kan overføres i en rekke ulike sammenhenger. I henhold til direktivets artikkel 26 kan «overføring av personopplysninger til en tredjestat som ikke sikrer et tilstrekkelig vernnivå i henhold til artikkel 25 nr. 2» finne sted dersom 1) overføringen er nødvendig for å kunne yte de tjenester kunden ber om eller for å oppfylle vilkårene i en avtale, for eksempel en avtale om hyppige flyreiser, eller 2) kunden utvilsomt har gitt sitt samtykke. Amerikanske organisasjoner som deltar i «trygg havn»-ordningen, gir tilstrekkelig vern av personopplysninger og kan derfor motta opplysninger fra EU uten å oppfylle disse vilkårene eller andre vilkår i direktivets artikkel 26. Siden «trygg havn»-ordningen inneholder særlige regler for følsomme opplysninger, skal slike opplysninger (for eksempel om en passasjers behov for fysisk assistanse) inngå i opplysninger som overføres til «trygg havn»-deltakere. Likevel må organisasjonen som overfører opplysningene, under alle omstendigheter følge lovgivningen i den EU-medlemsstaten der den utøver sin virksomhet, noe som bl. a. kan medføre særlige vilkår for behandling av følsomme opplysninger.

VS 14 – Legemidler

1. Spørsmål: *Når personopplysninger blir innsamlet innenfor EU og overført til De forente stater for legemiddelforskning og/eller andre formål, er det da medlemsstatens lover eller «trygg havn»-prinsippene som gjelder?*

1. Svar: Medlemsstatens lovgivning får anvendelse på innsamlingen av personopplysninger og på all behandling som finner sted før opplysningene overføres til De forente stater. «Trygg havn»-prinsippene får anvendelse først etter at opplysningene er blitt overført til De forente stater. Opplysninger som anvendes til legemiddelforskning og andre formål, bør om nødvendig gjøres anonyme.
2. Spørsmål: *Personopplysninger som framkommer gjennom særlig medisinsk forskning eller legemiddelforskning, er ofte viktige for framtidig vitenskapelig forskning. Når personopplysninger som er innsamlet i forbindelse med en undersøkelse, overføres til en amerikansk organisasjon innenfor «trygg havn»-ordningen, kan denne organisasjonen da anvende opplysningene til ny vitenskapelig forskning?*
2. Svar: Ja, dersom prinsippene om meldeplikt og valgfrihet ble fulgt fra begynnelsen. Slik melding skal inneholde opplysninger om enhver framtidig spesifisert bruk av opplysningene, for eksempel regelmessig oppfølging, beslektede undersøkelser eller markedsføring. Det er ikke mulig å opplyse om all framtidig bruk av opplysningene, siden ny innsikt i opprinnelige opplysninger, nye medisinske oppdagelser og framskritt samt utvikling innenfor folkehelse og lovgivning kan føre til ny bruk av forskningen. I meldingen skal det derfor eventuelt opplyses om at personopplysningene kan bli brukt i framtidig, medisinsk og farmasøytisk forskningsvirksomhet som ikke kan forutses. Dersom slik ny bruk ikke er i samsvar med de alminnelige forskningsformål som opplysningene opprinnelig ble innsamlet for, eller som den registrerte i ettertid har samtykket i, må det innhentes nytt samtykke.
3. Spørsmål: *Hva skjer med opplysningene om en person dersom en deltaker bestemmer seg for å trekke seg fra et klinisk forsøk, enten etter eget ønske eller på anmodning fra en sponsor?*
3. Svar: Deltakerne kan når som helst selv bestemme seg for eller bli oppfordret til å trekke seg fra et klinisk forsøk. Alle opplysninger som er blitt innsamlet før de trekker seg, kan fremdeles behandles på samme måte som andre opplysninger som blir innsamlet i forbindelse med forsøket, men bare dersom deltakeren ble opplyst om dette i meldingen da vedkommende sa seg villig til å delta.
4. Spørsmål: *Selskaper som framstiller legemidler eller medisinsk utstyr, har med henblikk på regulering og kontroll lov til å formidle personopplysninger fra kliniske forsøk utført innenfor EU, til reguleringsmyndigheter i De forente stater. Er tilsvarende overføringer lov til andre enn reguleringsmyndighetene, for eksempel foretak eller andre forskere?*
4. Svar: Ja, i samsvar med prinsippene om meldeplikt og valgfrihet.
5. Spørsmål: *For å gjøre kliniske forsøk så objektive som mulig, får deltakerne og til tider forskerne ikke tilgang til opplysninger om den behandling hver deltaker får. Slik tilgang kan sette undersøkelsens og resultatenes gyldighet på spill. Vil deltakere i slike kliniske forsøk (ofte kalt «blindundersøkelser») få tilgang til opplysninger om sin behandling under forsøket?*
5. Svar: Nei, en deltaker må ikke gis slik tilgang dersom denne begrensningen ble forklart da vedkommende sa seg villig til å delta i forsøket, og dersom videreformidling av slike opplysninger vil være til skade for forskningsforsøkets integritet. Samtykke til å delta i forsøket på disse vilkårene anses som ensbetydende med at vedkommende frasier seg retten til innsyn. Når forsøket er avsluttet og resultatene analysert, skal deltakere gis innsyn i opplysninger om seg selv dersom de ber om det. De bør først henvende seg til den lege eller behandler som behandlet dem under det kliniske forsøket, og deretter eventuelt til selskapet som sponset forsøket.
6. Spørsmål: *Må et selskap som framstiller legemidler eller medisinsk utstyr, anvende «trygg havn»-prinsippene om meldeplikt, valgfrihet, videre overføring og innsyn i sin virksomhet med hensyn til produktsikkerhet og effektivitetsmåling, herunder rapporter om uheldige forhold og registrering av pasienter/personer som bruker visse legemidler eller et visst medisinsk utstyr (for eksempel pacemaker)?*
6. Svar: Nei, ikke når overholdelse av prinsippene kolliderer med overholdelsen av lovbestemte forskrifter. Dette gjelder både for rapporter, for eksempel fra tjenesteytere innenfor helsetjenesten til selskaper som framstiller legemidler eller medisinsk utstyr, og for

rapporter fra slike selskaper til offentlige organer, som De forente Staters Food and Drug Administration.

7. Spørsmål: *Som regel koder den ansvarlige forskeren forskningsopplysningene ved kilden, for ikke å avsløre den enkeltes identitet. Legemiddelselskaper som sponser slik forskning, mottar ikke nøkkelen. Det er bare forskeren som har tilgang til den unike nøkkelkoden, slik at han eller hun under visse omstendigheter kan identifisere den enkelte deltaker (for eksempel dersom det skulle bli behov for medisinsk oppfølging). Vil en overføring fra EU til De forente stater av opplysninger kodet på denne måten utgjøre en overføring av personopplysninger som er underlagt «trygg havn»-prinsippene?*

7. Svar: Nei. Dette ville ikke utgjøre en overføring av personopplysninger underlagt «trygg havn»-prinsippene.

VS 15 – Offentlige registre og offentlig tilgjengelige opplysninger

Spørsmål: *Er det nødvendig å anvende prinsippene om meldeplikt, valgfrihet og videre overføring på opplysninger fra offentlige registre eller på offentlig tilgjengelige opplysninger?*

Svar: Det er ikke nødvendig å anvende prinsippene om meldeplikt, valgfrihet og videre overføring på opplysninger fra offentlige registre, såfremt de ikke kombineres med opplysninger fra registre som ikke er offentlige, og såfremt eventuelle vilkår for innsyn fastsatt av vedkommende myndighet oppfylles.

Det er heller ikke nødvendig å anvende prinsippene om meldeplikt, valgfrihet og videre overføring på offentlig tilgjengelige opplysninger, med mindre den europeiske avsenderen av opplysningene oppgir at de skal være underlagt begrensninger som krever at organisasjonen anvender prinsippene for de formål opplysningene skal brukes til. Organisasjoner er ikke ansvarlige for hvordan slike opplysninger brukes av dem som innhenter slike opplysninger fra offentliggjort materiale.

Dersom det viser seg at en organisasjon med hensikt har offentliggjort personopplysninger i strid med prinsippene, slik at den eller andre kan dra nytte av disse unntakene, vil organisasjonen bli utelukket fra «trygg havn»-ordningen.

VEDLEGG III

Oversikt over håndhevingen av «trygg havn»-ordningen**Føderal og delstatlig myndighet med hensyn til urimelig og villedende praksis og personvern**

I dette memorandum gis en oversikt over den myndighet Federal Trade Commission (FTC) har i henhold til avsnitt 5 i Federal Trade Commission Act (15 USC §§ 41-58, som endret) til rettslig å forfølge dem som unnlater å beskytte personopplysninger slik de har erklært eller forpliktet seg til. Det omhandler også unntak fra FTCs myndighet og andre føderale og delstatlige myndigheters muligheter til å gripe inn der FTC ikke har myndighet⁽¹⁾.

FTCs myndighet med hensyn til urimelig eller villedende praksis

I henhold til avsnitt 5 i Federal Trade Commission Act er «urimelig eller villedende atferd eller praksis i forbindelse med handel», ulovlig (15 USC § 45(a)(1)). Avsnitt 5 gir FTC uinnskrenket myndighet til å forhindre slik atferd og praksis (15 USC § 45(a)(2)). Følgelig kan FTC, etter å ha gjennomført en formell høring, nedlegge forbud eller påbud for å stanse den ulovlige atferden (15 USC § 45(b)). Dersom det er i offentlighetens interesse, kan FTC også anmode en amerikansk førsteinstansdomstol om midlertidig påbud eller midlertidig eller varig forbud (15 USC § 53(b)). I tilfeller der urimelig eller villedende atferd eller praksis utgjør et alminnelig atferdsmønster, eller der FTC allerede har nedlagt forbud eller påbud, kan FTC fastsette en administrativ bestemmelse som forbyr den aktuelle atferd eller praksis (15 USC § 57a).

Enhver som ikke retter seg etter FTCs avgjørelser, kan idømmes en bot på inntil 11 000 USD, og hver dag overtredelsen fortsetter vil bli betraktet som en særskilt overtredelse⁽²⁾ (15 USC § 45(1)). På samme måte kan enhver som med vitende og vilje bryter en FTC-bestemmelse, bøtelegges med 11 000 USD for hver overtredelse (15 USC § 45(m)). Gjennomføringstiltak kan treffes av De forente staters justisdepartement, eller dersom det avstår fra dette, av FTC (15 USC § 56).

FTCs myndighet og personvern

Ved utøvelsen av sin myndighet i samsvar med avsnitt 5 anser FTC at uriktige opplysninger om årsaken til og formålet med innsamling av opplysninger fra kunder utgjør villedende praksis⁽³⁾. I 1998 innklaget FTC for eksempel GeoCities for å ha videreformidlet opplysninger foretaket hadde samlet inn på sitt nettsted, til tredjemann for salgsfremmende formål, uten forhåndssamtykke, i strid med sine erklæringer om personvern⁽⁴⁾. FTCs personale har også uttalt at innsamling av personopplysninger fra barn samt salg og videreformidling av slike opplysninger uten foreldrenes samtykke, sannsynligvis utgjør urimelig praksis⁽⁵⁾.

⁽¹⁾ Vi redegjør ikke her for alle de ulike føderale lovbestemmelser om personvern i ulike sammenhenger, eller for de delstatslover eller den sedvanerett som får anvendelse. Lover på føderalt plan som regulerer innsamling og bruk av personopplysninger for kommersielle formål, omfatter blant andre Cable Communications Policy Act (47 USC § 551), Driver's Privacy Protection Act (18 USC § 2721), Electronic Communications Privacy Act (18 USC § 2701 *et seq.*), Electronic Funds Transfer Act (15 USC §§ 1693, 1693m), Fair Credit Reporting Act (15 USC § 1681 *et seq.*), Right to Financial Privacy Act (12 USC § 3401 *et seq.*), Telephone Consumer Protection Act (47 USC § 227) og Video Privacy Protection Act (18 USC § 2710). Mange delstater har tilsvarende lovgivning på disse områdene. Se for eksempel Mass. Gen. Laws ch. 167B, § 16 (som forbyr finansinstitusjoner å videreformidle kunders finansielle opplysninger til tredjemann uten enten kundens samtykke eller en rettsavgjørelse), N.Y. Pub. Health Law § 17 (som begrenser bruk og videreformidling av opplysninger om pasienters fysiske eller mentale helse, og som gir pasienter rett til innsyn i egne opplysninger).

⁽²⁾ I slike saker kan amerikanske førsteinstansdomstoler også nedlegge forbud eller gi rimelig oppreisning, for å håndheve FTCs avgjørelse (15 USC § 45(1)).

⁽³⁾ «Villedende praksis» defineres som en framstilling, utelatelse eller praksis som antas å kunne villedende normalt aktsomme forbrukere på en avgjørende måte.

⁽⁴⁾ Se www.ftc.gov/opa/1998/9808/geocities.htm.

⁽⁵⁾ Se skriv til Center for Media Education, www.ftc.gov/os/1997/9707/cenmed.htm. Children's Online Privacy Protection Act av 1998 gir i tillegg FTC myndighet til å regulere nettstedsoveratørers og direktekoblede tjenesteyteres innsamling av personopplysninger fra barn (se 15 USC §§ 6501-6506). Særlig pålegges slike operatører og tjenesteytere å underrette foreldrene og innhente deres samtykke som skal kunne etterprøves, før personopplysninger fra barn innsamles, brukes eller videreformidles (*id.*, § 6502(b)). Loven gir også foreldrene innsynsrett og rett til å nekte tillatelse til fortsatt bruk av opplysningene (*id.*).

Lederen i FTC, Robert Pitofsky, har i et brev til generaldirektør John Mogg ved Europakommisjonen redegjort for at begrensningene i FTCs myndighet med hensyn til personvern er begrenset når det ikke er avgitt uriktige opplysninger (eller ingen opplysninger i det hele tatt) om hvordan innsamlede opplysninger vil bli brukt (se brev fra FTCs leder Pitofsky til John Mogg av 23. september 1998). Foretak som vil dra nytte av den foreslåtte «trygg havn»-ordningen, må imidlertid garantere at de vil beskytte de innsamlede opplysningene i samsvar med de foreskrevne retningslinjene. Når et foretak garanterer at det vil beskytte slike personopplysninger, og deretter ikke gjør det, vil det bli betraktet som avgivelse av uriktige opplysninger og dermed utgjøre «villedende praksis» i henhold til avsnitt 5.

Siden FTCs myndighet omfatter urimelig og villedende atferd eller praksis «i forbindelse med handel», har ikke FTC myndighet når det gjelder innsamling og bruk av personopplysninger for ikke-kommersielle formål, for eksempel pengeinnsamling til veldedige formål (se brev fra Pitofsky, s. 3). Derimot vil bruk av personopplysninger i en hvilken som helst forretningsmessig transaksjon høre inn under FTCs myndighet. Dermed vil for eksempel en arbeidsgivers salg av personopplysninger om arbeidstakere til et foretak som driver med direkte markedsføring, være omfattet av avsnitt 5.

Unntak i avsnitt 5

I avsnitt 5 er det fastsatt unntak fra FTCs myndighet med hensyn til urimelig eller villedende atferd eller praksis i følgende virksomhetssektorer:

- finansinstitusjoner, herunder banker, spare- og utlånsforetak og kredittforeninger,
- offentlige teleselskaper og offentlige mellomstatlige transportører,
- luftfartsselskaper og
- emballeringsbedrifter og kjøttvareprodusenter,

Se 15 USC § 45 a) 2). Hvert unntak og hvilke reguleringsmyndigheter som trer inn i stedet for FTC, beskrives nedenfor.

Finansinstitusjoner⁽⁶⁾

Det første unntaket gjelder «banker, spare- og utlånsinstitusjoner beskrevet i avsnitt 18 f) 3) (15 USC § 57 a) f) 3))» og «føderale kredittforeninger beskrevet i avsnitt 18 f) 4) (15 USC § 57 a) f) 4))»⁽⁷⁾. Disse finansinstitusjonene er i stedet underlagt bestemmelser vedtatt av henholdsvis Federal Reserve Board, Office of Thrift Supervision⁽⁸⁾ og National Credit Union Administration Board (15 USC § 58 a) f)). Disse reguleringsorganene har som oppgave å vedta de bestemmelser som er nødvendige for å hindre urimelig og villedende praksis fra disse finansinstitusjonenes side⁽⁹⁾, og skal opprette en egen avdeling som skal behandle klager fra forbrukere (15 USC § 57 a) f) 1)). Gjennomføringsmyndigheten er fastsatt i avsnitt 8 i Federal Deposit Insurance Act (12 USC § 1818) for banker og spare- og utlånsforetak, og i avsnitt 120 og 206 i Federal Credit Union Act for føderale kredittforeninger (15 USC §§ 57 a) f) 2)-4)).

Selv om forsikringsselskapene ikke er nevnt uttrykkelig i listen over unntak i avsnitt 5, overlater McCarran-Ferguson Act (15 USC § 1011) *et seq.* som regel reguleringen av forsikringsvirksomhet til de

⁽⁶⁾ President Clinton underskrev Gramm-Leach-Bliley Act (Pub. L 106-102, konsolidert i 15 USC § 6801 og følgende) 12. november 1999. Loven begrenser finansinstitusjonenes videreformidling av personopplysninger om sine kunder. Loven krever at finansinstitusjoner bl. a. skal underrette alle kunder om sine programmer og sin praksis med hensyn til personvern innen rammen av videreformidling av personopplysninger til tilknyttede eller ikke-tilknyttede foretak. Loven gir FTC, de føderale bankmyndigheter og andre myndigheter rett til å vedta regler for gjennomføring av de tiltak som loven krever for personvern. De berørte offentlige organer har framlagt forslag til regler for dette formål.

⁽⁷⁾ Dette unntaket er formulert slik at det ikke gjelder for verdipapirer. Meglere og verdipapirforhandlere og andre innenfor verdipapirhandel kommer derfor inn under den konkurrerende jurisdiksjonen til Securities and Exchanges Commission og FTC med hensyn til urimelig og villedende atferd eller praksis.

⁽⁸⁾ Unntaket i avsnitt 5 viste opprinnelig til Federal Home Loan Bank Board som ble nedlagt ved Financial Institutions Reform, Recovery and Enforcement Act av 1989. Organets funksjoner ble overført til Office of Thrift Supervision og til Resolution Trust Corporation, Federal Deposit Insurance Corporation og Housing Finance Board.

⁽⁹⁾ Samtidig som finansinstitusjoner fjernes fra FTCs ansvarsområde, fastsettes det i avsnitt 5 at hver gang FTC fastsetter en regel med hensyn til urimelig og villedende atferd eller praksis, bør reguleringsmyndighetene for finansinstitusjoner, vedta tilsvarende bestemmelser innen 60 dager (15 USC § 57 a) f) 1)).

ulike delstatene⁽¹⁰⁾. I henhold til avsnitt 2b) i McCarran-Ferguson Act kan ingen føderal lov dessuten oppheve, svekke eller fortrenge delstatenes regelverk «med mindre en slik lov uttrykkelig gjelder forsikringsvirksomhet» (15 USC § 1012 b)). Bestemmelsene i FTC Act får likevel anvendelse på forsikringssektoren «i den grad slik virksomhet ikke er regulert av delstatene» (id.) Det bør også bemerkes at McCarran-Ferguson Act fortrenses av delstatslovgivningen bare når det gjelder «forsikringsvirksomhet». FTC har derfor fortsatt myndighet i saker om forsikringsselskapers urimelige eller villedende praksis i forbindelse med virksomhet utenfor forsikringssektoren. Dette kan f.eks. omfatte tilfeller der forsikringsselskaper selger personopplysninger om sine forsikringstakere til selskaper som driver direkte markedsføring av annet enn forsikringsprodukter⁽¹¹⁾.

Offentlige transportører

Det andre unntaket under avsnitt 5 gjelder de offentlige transportørene som er «underlagt lover som skal regulere handelen» (15 USC § 45 a 2)). I dette tilfellet tilsvarer «lover som skal regulere handelen» underkapittel IV i kapittel 49 i United States Code og Communications Act av 1934 (47 USC § 151 *et seq.*) (15 USC § 44).

Underkapittel IV i kapittel 49 (mellomstatlig transport) omfatter jernbaneselskaper, veitransportselskaper, vannveitransportselskaper, befraktere, speditører og rørledningstransportselskaper (49 USC § 10101 *et seq.*). Disse ulike offentlige transportørene er underlagt regelverket til Surface Transportation Board, et uavhengig organ under transportdepartementet (49 USC §§ 10501, 13501 og 15301). Transportøren har under ingen omstendigheter lov til å videreformidle opplysninger om fraktens art, bestemmelsessted og andre egenskaper som kan anvendes til skade for avsender (49 USC §§ 11904, 14908 og 16103). Det bemerkes at disse bestemmelser viser til opplysninger om avsenders frakt og ser dermed ikke ut til å gjelde personopplysninger om avsender som ikke er knyttet til den aktuelle frakten.

I Communications Act er det fastsatt at «mellomstatlig og internasjonal handel med kommunikasjon via kabel og radio» er underlagt Federal Communications Commission (FCC) (47 USC §§ 151 og 152). Communications Act anvendes ikke bare på offentlige teleforetak, men også på andre foretak som fjernsyns- og radioselskaper og kabeltjenesteleverandører som ikke er offentlige transportører, og som dermed ikke er omfattet av unntaket i avsnitt 5 i FTC Act. FTC har derfor myndighet til å undersøke om disse foretakene driver en urimelig og villedende praksis, mens FCC har konkurrerende myndighet til å utøve sin uavhengige myndighet på dette området, som beskrevet under.

I henhold til Communications Act er «ethvert teleselskap», herunder de lokale sentralene, forpliktet til å beskytte private opplysninger om kunder⁽¹²⁾. (47 USC § 222 a)). I tillegg til denne alminnelige personvernbestemmelsen har Communications Act blitt endret ved Cable Communications Policy Act av 1984 (kalt «Cable Act») (47 USC § 521 *et seq.*), for å pålegge kabelnettoperatorene å beskytte «personlige, identifiserbare opplysninger» om kabelnettabonnenter (47 USC § 551)⁽¹³⁾. Cable Act begrenser kabelnettoperatorenes innsamling av personopplysninger og krever at de underretter abonnentene om hva slags opplysninger som er samlet inn og hvordan de skal brukes. Den gir abonnenter rett til innsyn i opplysninger som gjelder dem og pålegger kabelnettoperatorene å tilintetgjøre disse opplysningene når de ikke lenger er nødvendige.

Communications Act gir FCC myndighet til å gjennomføre disse to personvernbestemmelsene på eget initiativ eller som følge av en klage utenfra⁽¹⁴⁾ (47 USC §§ 205, 403; *id.* § 208). Dersom FCC fastslår at

⁽¹⁰⁾ «Forsikringsvirksomhet og alle personer som utøver slik virksomhet, skal være underlagt de ulike delstatenes lover med hensyn til regulering og beskatning av slik virksomhet» (15 USC § 2012 a)).

⁽¹¹⁾ FTC har utøvet sin myndighet over forsikringsselskapene i ulike sammenhenger. I ett tilfelle traff FTC tiltak overfor et foretak som FTC har utøvet sin myndighet over forsikringsselskapene i ulike sammenhenger. I ett tilfelle traff FTC tiltak overfor et foretak som hadde drevet villedende reklame i en delstat der det ikke hadde tillatelse til å drive virksomhet. FTCs myndighet bygde på det faktum at det ikke fantes noe virkningsfullt regelverk på delstatsplan siden foretaket faktisk var utenfor den berørte delstatens rekkevidde. *Se* FTC mot Travelers Health Association, 362 US 293 (1960).

Når det gjelder delstatene, har 17 vedtatt modellen om vern av opplysninger og personvern i forsikringssektoren (Insurance Information and Privacy Protection Act), utarbeidet av National Association of Insurance Commissioners (NAIC). Loven omfatter bestemmelser om informasjon til forsikringstakere, bruk og videreføring av opplysninger samt innsyn. I tillegg har nesten alle delstatene vedtatt NAICs modell om urimelig forsikringspraksis (Unfair Insurance Practices Act), som særlig gjelder urimelig handelspraksis i forsikringssektoren.

⁽¹²⁾ Med begrepet «private opplysninger om nettkunder» menes opplysninger om en kundes bruk av teletjenester med hensyn til «hyppighet, teknisk konfigurasjon, type, mottakere og mengde» samt fakturaopplysninger (47 USC § 222 f 1)). Begrepet omfatter derimot ikke opplysninger om abonnentlister (*id.*).

⁽¹³⁾ Begrepet «personlige, identifiserbare opplysninger» defineres ikke uttrykkelig i loven.

⁽¹⁴⁾ Denne myndigheten omfatter retten til å kreve erstatning for krenkelse av personvernet i henhold til avsnitt 222 i Communications Act eller, med hensyn til kabelnettabonnentene, i henhold til avsnitt 551 i Cable Act som endrer Communications Act (*se også* 47 USC § 551 f 3)) (sivilt søksmål ved en føderal førsteinstansdomstol utelukker ikke annen rettslig klageadgang «i tillegg til enhver annen rettslig klageadgang tilgjengelig for en kabelnettabonntent»).

et teleselskap (herunder kabelnettooperatører) har brutt personvernbestemmelsene i avsnitt 222 eller avsnitt 551, kan FCC treffe tre ulike tiltak. Etter å ha foretatt en høring og fastslått at det har skjedd en overtredelse, kan FCC først pålegge transportøren å betale skadeserstatning⁽¹⁵⁾ (47 USC § 209). FCC kan for det andre nedlegge påbud eller forbud mot transportørens ulovlige praksis eller unnlatelse. (47 USC § 205 a)). Til slutt kan FCC også pålegge en transportør som overtrer loven å «overholde og følge enhver bestemmelse eller praksis som er pålagt av FCC (*id.*).

Privatpersoner som mener at et teleselskap eller en kabelnettooperatør har brutt de aktuelle bestemmelsene i Communications Act eller Cable Act, kan klage til FCC eller reise sak ved en føderal førsteinstansdomstol (47 USC § 207). En klager som får medhold i en sak ved en føderal domstol mot et offentlig teleselskap pga. manglende vern av private opplysninger om kunder innenfor den allmenne rammen av avsnitt 222 i Communications Act, kan få erstatning for den faktiske skaden samt få dekket utgiftene til advokat (47 USC § 206). En klager som innleder rettslig forfølgning med påstand om krenkelse av personvernet i henhold til avsnitt 551 i Cable Act, som uttrykkelig gjelder for kabelnettooperatører, kan i tillegg til erstatningen for den faktiske skaden og advokatutgiftene, få straffeerstatning og dekket saksomkostninger innen rimelighetens grenser (47 USC § 551 f)).

FCC har fastsatt detaljerte regler for gjennomføring av avsnitt 222 (47 CFR § 64.2001-2009). Disse detaljerte reglene inneholder særlige beskyttelsestiltak for å verne private opplysninger om nettkunder mot ulovlig innsyn. Tiltakene pålegger teleselskapene

- å utvikle og gjennomføre programvaresystemer som viser en kundes status med hensyn til opplysning og godkjenning når kundens mappe kommer opp på skjermen for første gang,
- å føre et elektronisk «register» for å spore tilgang til en kundes mappe, og særlig for å fastslå når, av hvem og for hvilket formål en kundes mappe er åpnet,
- å lære opp personalet sitt i tillatt anvendelse av private opplysninger om nettkunder og innføre passende disiplinære framgangsmåter,
- å innføre en kontroll- og overvåkingsprosess for å sikre at reglene overholdes i forbindelse med ekstern markedsføring,
- å avgi en årlig rapport til FCC om hvordan disse reglene blir overholdt.

Luftfartsselskaper

Amerikanske og utenlandske luftfartsselskaper som er underlagt Federal Aviation Act av 1958 er også unntatt fra avsnitt 5 i FTC Act (15 USC § 45 a 2)). Dette gjelder alle som driver transport av gods eller passasjerer med luftfartøy mellom statene eller til utlandet, eller som transporterer post med luftfartøy (49 USC § 40102). Luftfartsselskaper er underlagt transportdepartementet. Transportministeren har følgelig myndighet til å treffe tiltak for å hindre «urimelig, villedende, utilbørlig eller konkurransebegrensende praksis i lufttransportsektoren» (49 USC § 40101 a 9)). Dersom det tjener offentlighetens interesser, kan transportministeren undersøke om et amerikansk eller utenlandsk luftfartsselskap eller en billettagent har fulgt en urimelig eller villedende praksis (49 USC § 41712). Etter en høring kan transportministeren gi ordre om å innstille den ulovlige praksisen (*id.*). Så vidt vi kjenner til har transportministeren ennå ikke utøvd denne myndigheten til å beskytte personopplysninger om luftfartsselskapers kunder⁽¹⁶⁾.

Det finnes to personvernbestemmelser med hensyn til personopplysninger som får anvendelse på luftfartsselskaper i særskilte tilfeller. På den ene siden sikrer Federal Aviation Act personvernet for søkere til pilotstillinger (49 USC § 44936 f)). Loven tillater luftfartsselskaper å innhente opplysninger om en søkers tidligere arbeidsforhold, men gir også søkeren rett til å bli underrettet om at det er blitt anmodet om slike opplysninger, til å gi sitt samtykke til denne anmodningen, til å rette opp feil og til å begrense viderefremmingen av disse opplysningene til de personer som skal avgjøre ansettelsen. På den andre siden krever transportdepartementets regler at opplysninger om passasjerlister som samles inn av offentlige myndigheter til bruk ved flykastastrøfer «blir behandlet fortrolig og sendes bare til De forente staters utenriksdepartement, National Transportation Board (på anmodning fra NTSB) og De forente staters transportdepartement» (14 CFR del 243, § 243.9 c)) (som tilføyd i 63 FR 8258).

⁽¹⁵⁾ En klage kan ikke avvises under henvisning til at klageren ikke har lidd noen direkte skade (47 USC § 208 a)).

⁽¹⁶⁾ Det virker som det gjøres en innsats innen denne næringen for å ta opp personvernproblemer. Representanter fra næringen har drøftet de foreslåtte «trygg havn»-prinsippene og deres eventuelle anvendelse på luftfartsselskaper. Drøftingen har omfattet et forslag om å vedta et personvernprogram for hele næringen der de selskapene som deltar, uttrykkelig underkaster seg transportdepartementets myndighet.

Emballeringsbedrifter og kjøttvareprodusenter

Packers and Stockyards Act av 1921 (7 USC § 181 *et seq.*) forbyr «enhver emballeringsbedrift med virksomhet i forbindelse med husdyr, kjøtt, næringsmidler av kjøtt og animalske produkter i ubearbeidet form, og enhver forhandler av levende fjørfe, å medvirke til eller anvende praksis eller atferd som er urimelig, som innebærer ubegrunnet forskjellsbehandling eller som er villedende» (7 USC § 192 a); se også 7 USC § 213 a)) (som forbyr «enhver praksis eller atferd som er urimelig, som innebærer ubegrunnet forskjellsbehandling eller som er villedende» i forbindelse med husdyr). Landbruksministeren har det overordnede ansvar for gjennomføringen av disse bestemmelsene, mens FTC har myndighet med hensyn til detaljhandel og transaksjoner innen fjørfeindustrien (7 USC § 227 b) 2)).

Det er usikkert om landbruksministeren vil fortolke det som «villedende» praksis i henhold til Packers and Stockyards Act at en emballeringsbedrift eller en kjøttvareprodusent ikke sikrer personvern i samsvar med sin erklærte politikk. Unntaket i avsnitt 5 får anvendelse på personer, interessentskap og aksjeselskaper bare «i den grad de er underlagt Packers and Stockyards Act». Dersom personvern ikke omfattes av Packers and Stockyards Act, er det derfor meget sannsynlig at unntaket i avsnitt 5 ikke får anvendelse, og emballeringsbedrifter og kjøttvareprodusenter vil i så fall være underlagt FTCs myndighet.

Delstatenes myndighet med hensyn til urimelig og «villedende praksis»

I henhold til analyser utarbeidet av FTC har «alle de 50 amerikanske delstatene samt District of Columbia, Guam, Puerto Rico og de amerikanske Jomfruøyene, vedtatt en lovgivning som er mer eller mindre lik Federal Trade Commission Act for å bekjempe urimelig og villedende praksis». («FTC faktaark», trykt på nytt i «Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation». 59 Tul. L. Rev. 427 (1984)). I alle tilfeller har et offentlige organ med ansvar for gjennomføringen av lovgivningen, myndighet til å «foreta undersøkelser ved bruk av innstevning eller pålegg om sivil etterforskning, oppnå forsikring fra berørte foretak om at de frivillig vil overholde loven, nedlegge forbud eller påbud samt oppnå at en domstol nedlegger påbud eller forbud med sikte på å hindre bruk av urimelig, uredelig eller villedende handelspraksis (*id.*). I 46 av de nevnte jurisdiksjoner tillater loven private søksmål for oppnå erstatning tilsvarende den faktiske skaden, to eller tre ganger dette beløp eller straffeerstatning, samt i visse tilfeller dekning av saksomkostninger og advokatutgifter (*id.*).

Floridas Deceptive and Unfair Trade Practices Act gir for eksempel statsadvokaten myndighet til å etterforske og reise sivil søksmål i tilfeller av «urimelige konkurransemetoder og urimelig, uredelig eller villedende handelspraksis», herunder uriktig og villedende reklame, villedende tilbud om franchise eller forretningsmuligheter, svikaktig telefonsalg og pyramidesalgsordninger. Se også NY General Business Law § 349 (som forbyr urimelig atferd og villedende praksis i forretningsverdenen).

En undersøkelse som ble gjort i år av National Association of Attorneys General (NAAG) bekrefter disse forholdene. Samtlige av de 43 statene som svarte har en «mini-FTC» eller garanterer lignende vern. 39 delstater opplyste også i forbindelse med denne undersøkelsen at de har myndighet til å behandle klager fra personer som ikke har bosted i vedkommende delstat. Med hensyn til personvern for forbrukere, opplyste 37 av de 41 delstatene som svarte, at de ville behandle klager over at foretak under deres jurisdiksjon ikke overholder personvernbestemmelsene slik de har erklært.

VEDLEGG IV

Skadeserstatning ved krenkelse av personvernet, lovbestemte tillatelser samt fusjoner og overtakelser i amerikansk lovgivning

Dette dokument er utarbeidet på anmodning fra Europakommisjonen for å redegjøre for amerikansk lovgivning med hensyn til a) erstatningskrav for krenkelse av personvernet, b) «uttrykkelige tillatelser» i amerikansk lovgivning til bruk av personopplysninger på en måte som ikke er i samsvar med «trygg havn»-prinsippene og c) virkningene av fusjoner og overtakelser på de forpliktelser som inngås innenfor rammene av «trygg havn»-ordningen.

A. Erstatning for krenkelse av personvernet

Overtredelser av «trygg havn»-prinsippene kan, avhengig av omstendighetene, føre til en rekke private erstatningskrav. Særlig kan «trygg havn»-organisasjoner holdes ansvarlige for avgivelse av uriktige opplysninger dersom de ikke overholder det personvernprogram som de selv har offentliggjort. Amerikansk sedvanerett gir også mulighet for private erstatningssøksmål for krenkelse av personvernet. En rekke bestemmelser i den føderale lovgivning og i de enkelte staters lovgivning om personvern, gir også privatpersoner mulighet til å kreve erstatning for krenkelse av personvernet.

Retten til å kreve erstatning for krenkelse av personvernet er fast forankret i amerikansk sedvanerett.

I rettsvitenskapen gjøres det fra flere sider gjeldende at bruk av personlige opplysninger som ikke er i samsvar med «trygg havn»-prinsippene, kan medføre ansvar. For eksempel kan både den behandlingsansvarlige som overfører opplysningene, og de berørte personer saksøke «trygg havn»-organisasjoner for avgivelse av uriktige opplysninger dersom de misligholder sine «trygg havn»-forpliktelser. Følgende står i den amerikanske lovsamlingen Second Restatement of the Law om erstatninger⁽¹⁾:

Enhver person som svikaktig avgir uriktige opplysninger om fakta, meninger, hensikter eller lover, med det formål å få en annen person til å handle eller avstå fra å handle på grunnlag av disse (uriktige eller manglende) opplysningene, er erstatningspliktig overfor den andre personen for det økonomiske tap som denne måtte ha lidt som følge av de uriktige opplysningene.

Restatement, § 525. En uriktig opplysning anses som «svikaktig» dersom opphavsmannen vet eller tror at opplysningene er uriktige. Jf. § 526. Som hovedregel er den person som svikaktig avgir uriktige opplysninger, potensielt erstatningspliktig overfor enhver som han tenker seg eller forventer skal stole på de uriktige opplysningene, for ethvert økonomisk tap som disse personer måtte lide som følge av dette. Jf. § 531. En person som svikaktig avgir uriktige opplysninger til en annen, kan dessuten bli erstatningspliktig overfor tredjemann dersom skadevolderen tenkte seg eller forventet at de uriktige opplysningene ville bli gjentatt overfor tredjemann, som handler i god tro. Jf. § 533.

I forbindelse med «trygg havn»-ordningen er de relevante opplysningene den enkelte organisasjons offentlige erklæring om at den vil slutte seg til «trygg havn»-prinsippene. Når denne forpliktelsen er inngått, vil en bevisst misligholdelse av prinsippene kunne danne grunnlag for et søksmål for avgivelse av uriktige opplysninger fra personer som hadde tillit til dette. Fordi en forpliktelse til å slutte seg til prinsippene er offentlig, vil de personer som er gjenstand for opplysningen, og den registeransvarlige i EU som overfører personopplysninger til den amerikanske organisasjonen, alle ha grunn til å saksøke den amerikanske organisasjonen for avgivelse av uriktige opplysninger⁽²⁾. Den amerikanske organisasjonen forblir dessuten erstatningspliktig overfor disse personene for vedvarende avgivelse av uriktige opplysninger så lenge de til skade for seg selv handler på grunnlag av disse uriktige opplysningene. Jf. Restatement, § 535.

⁽¹⁾ Second Restatement of the Law – Torts: American Law Institute (1997).

⁽²⁾ Dette kan for eksempel være tilfelle når registrerte personer i tillit til den amerikanske organisasjonens «trygg havn»-forpliktelser har gitt den behandlingsansvarlige tillatelse til å overføre deres personopplysninger til USA.

Personer som stoler på uriktige opplysninger som er avgitt svikaktig, har rett til erstatning. Restatement lyder slik:

Enhver person som mottar uriktige opplysninger som er avgitt svikaktig, kan anlegge sak for bedrageri mot opphavsmannen og kreve erstatning for ethvert økonomisk tap som beviselig har oppstått som følge av disse uriktige opplysningene.

Restatement § 549. Den erstatning som kan tilkjennes, omfatter rene utlegg, men også tapt fortjeneste i forbindelse med forretningstransaksjoner. Jf. for eksempel *Boling v. Tennessee State Bank*, 890 S.W.2d 32 (1994). (Banken var i denne saken erstatningspliktig overfor låntakerne for USD 14 825 som kompensasjon for å ha gitt videre låntakeres personopplysninger og forretningsplaner til bankens styreleder, som hadde motstridende interesser).

Avgivelse av uriktige opplysninger kan betraktes som svikaktig bare dersom opphavsmannen faktisk hadde kjennskap til, eller i det minste trodde, at opplysningene var uriktige, men uaktsom avgivelse av uriktige opplysninger kan også medføre ansvar. Enhver som avgir uriktige erklæringer i forbindelse med sin forretningsvirksomhet, sitt yrke eller sin ansettelse eller innenfor rammene av enhver økonomisk transaksjon, kan i henhold til Restatement gjøres ansvarlig «dersom vedkommende innhenter eller videreformidler opplysningene uten passende aktpågivenhet eller sakkunnskap». Restatement § 522(1). I motsetning til erstatningsansvaret ved svikaktig avgivelse av uriktige opplysninger, begrenser erstatningsansvaret ved uaktsom avgivelse av uriktige opplysninger seg til rene utlegg. Jf. Restatement, § 552B(1).

Høyesterett i Connecticut avgjorde for eksempel i en sak nylig at et elektrisitetsverk som hadde unnlatt å opplyse om at det videreformidlet opplysninger om forbrukernes betaling til nasjonale kredittinstitusjoner, kunne saksøkes for avgivelse av uriktige opplysninger, jf. *Brouillard v. United Illuminating Co.*, 1999 Conn. Super. LEXIS 1754. I denne saken ble saksøkeren nektet kreditt fordi saksøkte hadde opplyst at saksøkers betaling var forsinket fordi den ble mottatt 30 dager etter fakturadato. Saksøker hevdet at han ikke var blitt underrettet om denne praksisen da han tegnet et privat strømabonnement i det saksøkte selskap. Retten fant særlig at «en klage over uaktsom avgivelse av uriktige opplysninger kan være basert på at saksøkte har unnlatt av å uttale seg selv om vedkommende er forpliktet til det». Saken viser også at det for søksmålsgrunnlaget for uaktsom avgivelse av uriktige opplysninger ikke stilles krav om forsett eller svikaktig hensikt. En amerikansk organisasjon som uaktsomt unnlater på en fyllestgjørende måte å opplyse om hvordan det akter å bruke personopplysninger som mottas innenfor rammene av «trygg havn»-ordningen, kan holdes ansvarlig for avgivelse av uriktige opplysninger.

Dersom en overtredelse av «trygg havn»-prinsippene medfører misbruk av personopplysninger, kan det også danne grunnlag for et erstatningskrav fra den registrerte i henhold til sedvanerett for krenkelse av privatlivets fred. Krenkelse av privatlivets fred har lenge vært godkjent som søksmålsgrunnlag i amerikansk lovgivning. I en sak fra 1905⁽³⁾ fastslo høyesterett i Georgia at retten til privatlivets fred var rotfestet i både naturrett og sedvanerett da den avsa kjennelse til fordel for en borger da et livsforsikringselskap hadde brukt et fotografi av borgeren for reklameformål uten vedkommendes tillatelse eller viten. Retten, som allerede den gangen brukte begreper som i dag har fått innpass i amerikansk rettspraksis med hensyn til personvern, fant at fotografiet hadde blitt brukt «i ond hensikt», «urettmessig» og «latterliggjorde saksøker overfor omverdenen»⁽⁴⁾. Grunnlaget for *Pavesich*-dommen har med mindre variasjoner bestått fram til i dag og er fundamentet for amerikansk lovgivning på området. Domstolene i enkeltstater har konsekvent tatt til følge søksmål der grunnlaget var krenkelse av personvernet, og minst 48 stater anerkjenner i dag denne form for søksmålsgrunnlag⁽⁵⁾. Dessuten har minst 12 stater bestemmelser i grunnloven som beskytter borgerne mot inngrep i privatlivets fred⁽⁶⁾, som i visse tilfeller kan omfatte beskyttelse mot inngrep fra ikke-statlige organer. Jf. for eksempel *Hill v. NCAA*, 865 P.2d 633 (Ca. 1994); jf. også S. Ginder, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 S.D.L. Rev. 1153 (1997): («Visse delstatsgrunnlover inneholder bestemmelser om personvern som går lenger enn bestemmelsene i den amerikanske grunnloven. Alaska,

⁽³⁾ *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68 (Ga. 1905).

⁽⁴⁾ Jf. 69.

⁽⁵⁾ Et elektronisk søk i Westlaw-databasen viste at det siden 1995 har blitt anlagt 2 703 sivile søksmål ved delstatsdomstolene med hensyn til privatlivets fred. Vi har tidligere gitt Kommisjonen opplysninger om dette søket.

⁽⁶⁾ Jf. for eksempel grunnloven i Alaska, artikkel 1, avsnitt 22; Arizona, artikkel 2, avsnitt 8; California, artikkel 1, avsnitt 1; Florida, artikkel 1, avsnitt 23; Hawaii, artikkel 1, avsnitt 5; Illinois, artikkel 1, avsnitt 6; Louisiana, artikkel 1, avsnitt 5; Montana, artikkel 2, avsnitt 10; New York, artikkel 1, avsnitt 12; Pennsylvania, artikkel 1, avsnitt 1; South Carolina, artikkel 1, avsnitt 10; og Washington, artikkel 1, avsnitt 7.

Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina og Washington har et mer omfattende personvern.»)

Second Restatement of Torts gir en pålitelig oversikt over lovbestemmelsene på dette området. Det forklares i Restatement med utgangspunkt i alminnelig rettspraksis, at «retten til personvern» omfatter fire ulike gunner for erstatningssøksmål. Jf. Restatement, § 652A. Det kan for det første anlegges sak på grunn av «krenkelse av privatlivets fred» mot enhver som med forsett på fysisk eller annen måte krenker en person som ønsker å leve tilbaketrukket eller ensomt eller krenker en annen persons privatliv eller private anliggender⁽⁷⁾. Det kan for det andre anlegges sak på grunn av «urettmessig tilegnelse» mot enhver som til eget bruk eller for egen vinning bruker en annen persons navn eller bilde⁽⁸⁾. Den tredje søksmålsgrunn er «offentliggjøring av private opplysninger» når det offentliggjorte materialet er av en slik art at det kan virke krenkende for enhver bonus pater familias og ikke er av interesse for offentligheten⁽⁹⁾. Den fjerde og siste søksmålsgrunn er «ærekrenkelse» når en person forsettelig eller uaktsomt offentlig omtaler en annen person på en måte som vil virke krenkende for enhver bonus pater familias⁽¹⁰⁾.

«Krenkelse av privatlivets fred» vil innenfor rammen av «trygg havn»-prinsippene omfatte ulovlig innsamling av personopplysninger, mens en ulovlig bruk av personopplysninger for kommersielle formål kan danne grunnlag for et erstatningskrav på grunn av urettmessig tilegnelse». Videreformidling av uriktige personopplysninger vil på tilsvarende måte kunne danne grunnlag for et erstatningskrav på grunn av «ærekrenkelse» dersom opplysningene kan betegnes som krenkende for enhver bonus pater familias. Til slutt vil krenkelser av privatlivets fred som skyldes offentliggjøring eller videreformidling av følsomme personopplysninger, kunne danne grunnlag for et søksmål for «offentliggjøring av private opplysninger.» (Jf. eksempler nedenfor).

Med hensyn til erstatningsansvar gir en krenkelse av privatlivets fred den skadelidende retten til å kreve erstatning for

- a) enhver skade på vedkommendes privatliv som følge av krenkelsen,
- b) enhver psykisk overlast som det kan bevises at vedkommende har lidt, dersom dette under normale omstendigheter kan tilskrives en slik krenkelse, og
- c) enhver særskilt skade som begrunnes med den aktuelle krenkelsen.

Restatement, § 652H. Fordi erstatningsrettslige bestemmelser får alminnelig anvendelse, og fordi det finnes en lang rekke søksmålsgrunner som dekker de ulike sider ved personvernet, har de personer som får sitt privatliv krenket som følge av en overtredelse av «trygg havn»-prinsippene, som regel rett til økonomisk erstatning.

Domstolene i enkeltstatene behandler en stor mengde lignende saker om krenkelse av privatlivets fred. I saken *Ex Parte AmSouth Bancorporation et al.*, 717 So. 2d 357 ble det for eksempel framsatt et kollektivt søksmål der det ble hevdet at saksøkte hadde «misbrukt den tillit som kundene hadde til banken, ved å gi videre fortrolige opplysninger om bankens innskytere og deres konti» for å gi en tilknyttet bank muligheten til å selge andeler i investeringsselskaper og andre investeringsobjekter. Det tilkjennes ofte erstatning i slike saker. I saken *Vassiliades v. Garfinckel's, Brooks Bros.*, 492 A.2d 580 (D.C.App. 1985) omstøtte en appelldomstol en dom fra en lavere domstol og fastslo at bruken av bilder av saksøker før og etter en plastisk operasjon med henblikk på markedsføring i et stormagasin, var en krenkelse av privatlivets fred fordi det var en offentliggjøring av private opplysninger. I saken *Candebat v. Flanagan*, 487 So.2d 207 (Miss. 1986) brukte det saksøkte forsikringsselskapet en ulykke der saksøkers kone var blitt alvorlig skadd, i en reklamekampanje. Saksøker anla sak for krenkelse av privatlivets fred. Domstolen fastslo at saksøker skulle tilkjennes erstatning for psykisk overlast og tilegnelse av identitet. Selv personer som ikke er berømte, kan anlegge sak for urettmessig tilegnelse, jf. for eksempel *Staruski v. Continental Telephone Co.*, 154 Vt. 568 (1990) (saksøkte brukte en av sine ansattes navn og bilde for kommersielle formål i en avisreklame). I saken *Pulla v. Amoco Oil Co.*, 882 F.Supp. 836 (S.D Iowa 1995) krenket en arbeidsgiver en av sine ansattes privatliv ved å få en annen av sine ansatte til å undersøke saksøkers kredittkortopplysninger for å kontrollere vedkommendes sykefravær. Domstolen stadfestet en jury's tilkjennelse av USD 2 i skadeserstatning for faktisk tap, og en straffeerstatning på USD 500 000. En annen arbeidsgiver ble pålagt å betale erstatning fordi det i foretakets avis var blitt offentliggjort en artikkel om en ansatt som var blitt oppsagt fordi vedkommende var mistenkt for å ha forfalsket ansettelsespapirene sine, jf. *Zinda v. Louisiana-Pacific Corp.*, 140 Wis.2d 277 (Wis.App. 1987). Artikkelen krenket saksøkers

⁽⁷⁾ Jf. kapittel 28, avsnitt 652B.

⁽⁸⁾ Jf. kapittel 28, avsnitt 652C.

⁽⁹⁾ Jf. kapittel 28, avsnitt 652D.

⁽¹⁰⁾ Jf. kapittel 28, avsnitt 652E.

privatliv fordi den inneholdt private opplysninger, og fordi avisen sirkulerte i lokalsamfunnet. Til slutt ble en skole kjent skyldig i krenkelse av privatlivets fred fordi den HIV-testet elevene etter å ha fortalt dem at blodprøvene bare var for røde hunder. Jf. Doe v. High-Tech Institute, Inc., 972 P.2d 1060 (Colo.App. 1998). (For andre saker se Restatement, § 652H, vedlegg.)

USA kritiseres ofte for at konflikter altfor ofte løses ved domstolene, men dette betyr også at enkeltpersoner har mulighet til å anlegge sak, og gjør det, når de mener at deres rettigheter har blitt krenket. Det amerikanske rettssystemet gjør det på mange måter enkelt å anlegge sak, enten som enkeltperson eller kollektivt. Advokatstanden, som er forholdsmessig større enn i de fleste andre land, gjør det enkelt å søke profesjonell bistand. Saksøkernes advokater, som representerer enkeltpersoner i forbindelse med private søksmål, får vanligvis et salær som fastsettes på grunnlag av sakens utfall, noe som gjør det mulig selv for fattige eller ubemidlede personer å søke erstatning. Dette leder fram til et viktig punkt, nemlig at det i USA vanligvis er slik at hver part bærer sine egne kostnader til advokatsalærer og annet. Dette står i kontrast til forholdene i Europa, der den gjeldende regel er at den tapende part betaler den andre partens omkostninger. Uten å diskutere de to systemers fordeler og ulemper, er det mindre fare for at det amerikanske systemet forhindrer personer som ikke vil være i stand til å betale den andre partens kostnader, fra å anlegge sak.

Enkeltpersoner kan anlegge sak selv om erstatningskravene deres er forholdsvis beskjedne. De fleste, om ikke alle, jurisdiksjoner i USA har domstoler som behandler små erstatningssaker med mulighet til enklere og mindre kostbare prosedyrer for bileggelse av tvister under den lovbestemte grense⁽¹⁾. Muligheten for å få tilkjent en straffeerstatning virker også som en økonomisk oppmuntring for personer som kanskje har lidt bare en beskjeden direkte skade, til å anlegge sak på grunn av ulovlig atferd. Til slutt kan personer som alle har lidt samme form for skade, forene sine ressurser og krav i et kollektivt søksmål.

Den pågående saken mot Amazon.com for krenkelse av personvernet er et godt eksempel på enkeltpersoners mulighet til å anlegge sak for å få oppreisning. Amazon.com, som er en stor direktekoplet detaljist, er gjenstand for et kollektivt søksmål der saksøkerne hevder at de ikke ble underrettet om eller hadde gitt sitt samtykke til at deres personopplysninger ble innsamlet da de brukte dataprogrammet «Alexa», som tilhører Amazon. Saksøkerne har i denne saken hevdet at det har funnet sted en overtredelse av Computer Fraud and Abuse Act, fordi saksøkte på ulovlig vis har skaffet seg tilgang til deres lagrede meldinger, og av Electronic Communications Privacy Act på grunn av ulovlig avlytting av deres elektroniske og telegrafiske meldinger. De hevder dessuten at det i henhold til sedvaneretten har funnet sted en krenkelse av personvernet. Dette bygger på en klage som i desember ble inngitt av en ekspert på Internett-sikkerhet. I denne saken ble det framsatt et erstatningskrav på USD 1 000 for hver saksøker i det kollektive søksmålet i tillegg til advokatsalærer og tilbakebetaling av den fortjeneste som kan tilskrives lovovertrедelsen. Erstatningen kan beløpe seg til flere milliarder dollar, ettersom det kan dreie seg om flere millioner personer. Federal Trade Commission undersøker også denne saken.

Den føderale og delstatlige lovgivning om personvern gir ofte mulighet for private søksmål for økonomisk erstatning.

I tillegg til å medføre erstatningsansvar i henhold til erstatningsretten, kan en overtredelse av «trygg havn»-prinsippene være et brudd på én eller flere av de mange hundre bestemmelsene i den føderale lovgivning eller delstatslovgivningene. Mange av disse lovbestemmelsene som gjelder både offentlig og privat behandling av personopplysninger, gir enkeltpersoner mulighet til å søke om erstatning dersom deres rettigheter krenkes. For eksempel:

Electronic Communications Privacy Act av 1986: Denne loven forbyr ikke-tillatt avlytting av mobiltelefonsamtaler og overføringer mellom datamaskiner. Overtredelser kan medføre erstatningsansvar på minst USD 100 for hver dag overtredelsen finner sted. Loven beskytter også mot ikke-tillatt adgang eller videreformidling av lagrede elektroniske kommunikasjoner. Overtredere er erstatningsansvarlige for den skade de har forvoldt, eller kan få inndratt den gevinst som kan tilskrives overtredelsen.

Telecommunications Act av 1996: Private opplysninger om nettkunder (customer proprietary network information), CPNI, kan i henhold til avsnitt 702 ikke brukes for andre formål enn å yte teletjenester. Abonnenter kan enten klage til Federal Communications Commission eller anlegge sak ved en føderal førsteinstansdomstol (federal district court) for å få tilkjent erstatning og dekket advokatsalærer.

Consumer Credit Reporting Reform Act av 1996: Loven av 1996 har i forhold til Fair Credit Reporting Act av 1970 (FCRA) ført til en rekke forbedringer med hensyn til opplysningsplikt og rett til innsyn for personer som er gjenstand for kredittrapportering. Med denne nye loven av 1996 ble det også innført nye

⁽¹⁾ Vi har tidligere gitt Kommissjonen opplysninger om søksmål av begrenset verdi.

begrensninger for videresalg av forbrukerkredittrapporter. Forbrukere kan i tilfeller av overtredelse få tilkjent erstatning og dekket advokatsalærer.

Delstatslovgivningene beskytter også personvernet i en rekke ulike situasjoner. Blant de områdene der delstatene har grepet inn er bankopplysninger, kabelfjernsynsabonnementer, kredittopplysninger, personalopplysninger, offentlige registre, genetiske opplysninger og pasientjournaler, forsikringsopplysninger, karakterutskrift, elektroniske meldinger og leie av video⁽¹²⁾.

B. Uttrykkelige lovfestede tillatelser

«Trygg havn»-prinsippene inneholder et unntak når lover, forskrifter eller rettspraksis skaper «motstridende forpliktelser eller uttrykkelige tillatelser, forutsatt at organisasjonen ved anvendelse av slike tillatelser kan vise at den overtrer prinsippene bare i det omfang som er nødvendig for å ivareta de overordnede, rettmessige interesser som slike tillatelser skal fremme». Amerikanske organisasjoner skal, uavhengig av sin deltaking i «trygg havn»-ordningen, helt klart følge loven når det i amerikansk lovgivning forekommer motstridende forpliktelser. Mens «trygg havn»-prinsippene har som mål å binde sammen det amerikanske og det europeiske personvernssystemet, skal vi med hensyn til uttrykkelige tillatelser ta hensyn til våre folkevalgte lovgiveres særretter. Det begrensede unntaket fra en streng overholdelse av «trygg havn»-prinsippene er et forsøk på å tilgodese begge parter rettmessige interesser.

Unntaket er begrenset til tilfeller der det foreligger en uttrykkelig tillatelse. Den relevante loven, forskriften eller domstolsavgjørelsen skal derfor først og fremst uttrykkelig tillate «trygg havn»-organisasjonenes atferd⁽¹³⁾. Unntaket kan med andre ord ikke gjøres gjeldende dersom det ikke står noe i loven. Videre kan unntaket gjelde bare dersom den uttrykkelige tillatelsen er i konflikt med «trygg havn»-prinsippene. Selv i disse tilfellene er unntaket begrenset til «det omfang som er nødvendig for å ivareta de overordnede, rettmessige interesser som slike tillatelser skal fremme». Unntaket vil for eksempel ikke få anvendelse dersom loven tillater et foretak å gi personopplysninger bare til offentlige myndigheter. Dersom loven på den annen side gir et foretak særskilt tillatelse til å gi personopplysninger videre til statlige organer uten den enkeltes samtykke, dreier det seg om en «uttrykkelige tillatelse» til å handle på en måte som er i strid med «trygg havn»-prinsippene. Alternativt vil særlige unntak fra uttrykkelige krav om meldeplikt og samtykke være omfattet av unntaket (ettersom det ville være det samme som en særskilt tillatelse til å viderefordre opplysningene uten meldeplikt og samtykke). En lovbestemmelse som gir leger tillatelse til å gi pasientjournaler videre til helsemyndighetene uten pasientenes forhåndssamtykke, vil for eksempel medføre et unntak fra prinsippene om meldeplikt og valgfrihet. Denne tillatelsen gir ikke leger mulighet til å viderefordre de samme pasientjournalene til helseorganisasjoner eller kommersielle farmasøytiske forskningslaboratorier, noe som ville ha ligget utenfor lovens formål og dermed utenfor unntaket virkeområde⁽¹⁴⁾. Det rettslige grunnlaget kan være en enkeltstående tillatelse til å gjøre visse ting med personopplysninger, men som eksemplene nedenfor viser, vil det sannsynligvis være et unntak fra en vidtrekkende lov som forbyr innsamling, bruk eller viderefordling av personopplysninger.

Telecommunications Act av 1996

I de fleste tilfeller er den tillatte bruken i samsvar med kravene i direktivet og prinsippene, eller ville ha vært tillatt i henhold til et av de andre unntakene. Avsnitt 702 i Telecommunications Act (konsolidert i 47 USC § 222) pålegger for eksempel teleoperatører å behandle fortrolig alle personopplysninger som de mottar i forbindelse med sin tjenestevirksomhet. Denne bestemmelsen gir teleoperatører tillatelse til

1. å bruke kundeopplysninger for å yte tjenester, herunder utgivelse av telefonkataloger,
2. å gi kundeopplysninger til tredjemann på skriftlig anmodning fra kunden, og
3. å gi kundeopplysninger i sammenfattet form.

⁽¹²⁾ Et søk som nylig ble foretatt i Westlaw-databasen, gav 994 registrerte saker på delstatsplan som omhandlet erstatningskrav på grunn av krenkelse av personvernet.

⁽¹³⁾ Det presiseres at det ikke kreves at rettsmyndighetene henviser særskilt til «trygg havn»-prinsippene.

⁽¹⁴⁾ På samme vis kan legen i dette eksemplet ikke under henvisning til det rettslige grunnlag, tilsidesette enkeltpersoners rett i henhold til VS 12 til å velge bort direkte markedsføring. Virkeområdet for ethvert unntak for «uttrykkelige tillatelser» er nødvendigvis begrenset til tillatelsens virkeområde i henhold til loven.

Jf. 47 USC § 222(c)(1)-(3). Loven inneholder også et unntak som gir teleoperatører mulighet til å bruke kundeopplysninger for

- 1) å iverksette, yte, fakturere og kreve betaling for sine tjenester,
- 2) å beskytte mot svikaktig, lyssky eller ulovlig atferd, og
- 3) å foreta telefonsalg, gi opplysninger eller yte administrative tjenester under oppringninger som kunden har tatt initiativ til⁽¹⁵⁾.

Jf. også § 222(d)(1)-(3). Til slutt pålegges teleoperatører å forsyne utgivere av telefonkataloger med abonnentlister som bare kan inneholde navn, adresser, telefonnumre og bransje dersom det er en forretningskunde. Jf. § 222(e).

Unntaket for «uttrykkelige tillatelse» kan få anvendelse når teleoperatører bruker CPNI for å forebygge bedrageri eller andre ulovlige handlinger. Selv i slike tilfeller kan det hevdes at det dreier seg om tiltak i «offentlighetens interesse» og dermed i samsvar med prinsippene.

Forslag til regler fra helsedepartementet

Helsedepartementet har foreslått regler for personvern med hensyn til personlige, identifiserbare opplysninger om helse. Jf. 64 Fed. Reg. 59,918 (3. november 1999) (kommende konsolidering: 45 C.F.R. nr. 160-164). Med disse reglene innføres kravene med hensyn til personvern i Health Insurance Portability and Accountability Act av 1996, Pub. L. 104-191. I korthet går de foreslåtte reglene ut på å forby alle enheter som omfattes (dvs. sykekasser, datasentraler for helseopplysninger og tjenesteytere innenfor helsetjenesten som overfører helseopplysninger i elektronisk format), å bruke eller videreformidle beskyttede helseopplysninger uten særskilt tillatelse. Jf. forslag til avsnitt 45 i Code of Federal Regulations, § 164.506. I henhold til de foreslåtte reglene kan beskyttede helseopplysninger videreformidles bare for to formål: 1) for å gi enkeltpersoner mulighet til å kontrollere og kopiere helseopplysninger om seg selv, jf. § 164.514, og 2) for å håndheve reglene, jf. § 164.522.

De foreslåtte reglene vil tillate bruk eller videreformidling av beskyttede helseopplysninger uten særskilt tillatelse fra den registrerte i et begrenset antall tilfeller. Disse tilfellene omfatter f.eks. tilsyn med helsesystemet, håndheving av loven og nødstilfeller. Jf. § 164.510. De foreslåtte regler inneholder en detaljert beskrivelse av begrensningene for slik bruk og videreformidling. Videre vil tillatt bruk og videreformidling av beskyttede opplysninger være begrenset til det nødvendige minste antall av opplysninger. Jf. § 164.506.

Den bruken som de foreslåtte reglene uttrykkelig tillater, er i alminnelighet i samsvar med «trygg havn»-prinsippene, eller tillatt i henhold til et annet unntak. For eksempel er håndheving av loven og rettsforvaltning tillatt, og også medisinsk forskning. Andre bruksområder, herunder tilsyn med helsesystemet, det offentlige helsevesen og myndighetenes helsedatabaser, tjener offentlighetens interesse. Videreformidling med henblikk på behandling av betalinger og premier i forbindelse med helsetjenester, er nødvendig innenfor helsesektoren. Bruk i nødssituasjoner når det er nødvendig å drøfte behandlingen med de nærmeste pårørende fordi pasientens samtykke «ikke kan innhentes på en praktisk eller rimelig måte», for å fastslå avdødes identitet eller dødsårsaken eller for å beskytte den registrertes eller andres vitale interesser. Bruk i forbindelse med administrasjon av vernepliktige eller andre særskilte grupper av personer gjør det lettere å utføre militærets oppgaver eller er nødvendig i andre krevende situasjoner. Slik bruk vil under alle omstendigheter sjelden få anvendelse på forbrukere i alminnelighet.

Det eneste som gjenstår, er bruken av personopplysninger innenfor helsesektoren til framstilling av pasientlister. Selv om slik bruk ikke kan regnes for å være av «vital» interesse, er slike pasientlister nyttige for både pasienter, venner og bekjente. Virkeområdet for dette unntaket er dermed av naturlige grunner begrenset. Det er derfor en svært begrenset fare for krenkelse av pasientenes personvern når et unntak i henhold til en lovfestet «uttrykkelig tillatelse» brukes for dette formålet.

⁽¹⁵⁾ Dette unntaket har et meget begrenset virkeområde. Teleoperatører kan i henhold til bestemmelsen bruke CPNI bare ved en oppringning foretatt av kunden selv. FCC har dessuten opplyst at teleoperatører ikke kan bruke CPNI til å markedsføre tjenester utover det som kunden selv har bedt om. Denne bestemmelsen er ikke et egentlig «unntak», ettersom kunden skal tillate bruk av disse opplysningene for dette formål.

Fair Credit Reporting Act

Europakommisjonen har uttrykt bekymring over at et unntak i henhold til «uttrykkelig tillatelse» vil medføre at det beskyttelsesnivå som oppnås ved hjelp av Fair Credit Reporting Act (FCRA) betraktes som tilstrekkelig. Det vil imidlertid ikke være tilfelle. Uten at et tilstrekkelig beskyttelsesnivå er besluttet særskilt for FCRA, vil de amerikanske organisasjoner som ellers ville ta utgangspunkt i en slik beslutning, måtte love å slutte seg til «trygg havn»-prinsippene på alle måter. Det betyr at de amerikanske organisasjonene bare behøver å overholde FCRA når beskyttelsesnivået som oppnås ved hjelp av FCRA, overstiger prinsippenes. I motsatt fall skal organisasjonene bringe sin praksis for behandling av personopplysninger i samsvar med prinsippene når beskyttelsesnivået med FCRA ikke er på høyde med prinsippenes. Unntaket vil ikke påvirke denne grunnleggende regelen. Unntaket får anvendelse bare når den gjeldende lovgivning uttrykkelig tillater en atferd som normalt ville være i strid med «trygg havn»-prinsippene. Unntaket vil ikke gjelde på områder der FCRA-kravene ikke lever opp til «trygg havn»-prinsippene⁽¹⁶⁾.

Det er med andre ord ikke meningen at unntaket skal oppfattes som at alt som ikke kreves, er «uttrykkelig tillatt». Dessuten får unntaket anvendelse bare når det som uttrykkelig tillates i henhold til amerikansk lovgivning, er i strid med kravene i «trygg havn»-prinsippene. Den relevante lovgivning å oppfylle begge disse kriteriene for at det skal være tillatt å tilsidesette prinsippene.

Avsnitt 604 i FCRA inneholder for eksempel en uttrykkelig tillatelse for forbrukeropplysningsbyråer til å videreformidle forbrukeropplysninger i ulike særskilt angitte tilfeller. Jf. § 604 i FCRA. Dersom avsnitt 604 dermed gir kredittopplysningsbyråene tillatelse til å handle i strid med «trygg havn»-prinsippene, vil disse byråene påberope seg dette unntaket (med mindre et annet unntak får anvendelse, naturligvis). Kredittopplysningsbyråene skal rette seg etter domstolenes avgjørelser og innstevninger fra storjury (grand jury subpoenas), og offentlige bevillingsmyndigheters, sosialmyndigheters og barnebidragsmyndigheters bruk av kredittopplysninger skal være i offentlighetens interesse. Jf. § 604(a)(1), (3)(D), og (4). Kredittopplysningsbyrået trenger dermed i disse tilfellene ikke å påberope seg unntaket i henhold til «uttrykkelige tillatelser». Et forbrukeropplysningsbyrå overholder «trygg havn»-prinsippene når det handler i samsvar med forbrukerens skriftlige instruks. Jf. § 604(a)(2). På samme måte kan forbrukeropplysninger videreformidles for ansettelsesformål bare dersom forbrukeren har gitt skriftlig tillatelse til dette (jf. § 604(a)(3)(B) og (b)(2)(A)(ii)), og i forbindelse med kreditt- eller forsikringstransaksjonene som ikke foretas på forbrukerens initiativ, bare dersom forbrukeren ikke har valgt bort slike muligheter (jf. § 604(c)(1)(B)). FCRA forbyr kredittopplysningsbyråer å formidle helseopplysninger for ansettelsesformål uten forbrukerens tillatelse. Jf. § 604(g). Slike anvendelser samsvarer med prinsippene om meldeplikt og valgfrihet. Andre formål som tillates i henhold til § 604 omfatter transaksjoner som involverer forbrukeren, og som derfor ville være tillatt i henhold til prinsippene. Jf. § 604(a)(3)(A) og (F).

Den siste bruken som «tillates» i henhold til avsnitt 604, gjelder de sekundære kredittmarkedene. Jf. § 604(a)(3)(E). Det er ingen konflikt i seg selv mellom bruken av forbrukeropplysninger og «trygg havn»-prinsippene. Det er riktig at det i FCRA ikke er noe krav om at kredittopplysningsbyråer for eksempel skal underrette forbrukerne og innhente deres samtykke når de utsteder rapporter for dette formål. Vi vil likevel på nytt understreke at et manglende krav ikke er ensbetydende med en «uttrykkelig tillatelse» til å handle på en annen måte enn påkrevd. På samme måte kan kredittopplysningsbyråer i henhold til avsnitt 608 formidle visse personopplysninger til offentlige organer. Denne «tillatelsen» gir ikke et kredittopplysningsbyrå lov til å tilsidesette sin forpliktelse til å overholde «trygg havn»-prinsippene. Dette står dermed i kontrast til våre andre eksempler, der unntak fra prinsippene om meldeplikt og valgfrihet medfører en uttrykkelig tillatelse til å bruke personopplysninger uten å overholde disse to prinsippene.

Konklusjon

Selv denne begrensede gjennomgåelsen av de gjeldende regler, viser et tydelig mønster:

- En «uttrykkelig tillatelse» i loven gir i alminnelighet mulighet til bruk eller videreformidling av personopplysninger uten den registrertes forhåndssamtykke; unntaket vil dermed være begrenset til prinsippene om meldeplikt og valgfrihet.

⁽¹⁶⁾ Våre drøftelser på dette området skal ikke betraktes som en innrømmelse av at FCRA ikke gir en «tilstrekkelig» beskyttelse. Enhver vurdering av FCRA skal ta høyde for den beskyttelse som oppnås ved hjelp av loven i sin helhet, og ikke fokusere bare på unntakene slik tilfellet er her.

- De lovbestemte unntakene er i de fleste tilfeller nøye beskrevet slik at de får anvendelse i særskilte situasjoner og for særskilte formål. For øvrig forbyr loven ikke-tillatt bruk eller videreformidling av personopplysninger som ikke faller innenfor disse rammene.
- I de fleste tilfeller tjener den tillate bruk eller videreformidling offentlighetens interesse, noe som avspeiler lovens formål.
- Den tillate bruk eller videreformidling er i nesten alle tilfeller enten i fullt samsvar med «trygg havn»-prinsippene eller omfattet av de andre tillatte unntakene.

Konklusjonen er at unntak i henhold til en lovfestet «uttrykkelig tillatelse» har begrenset rekkevidde.

C. Fusjoner og overtakelser

Artikkel 29-arbeidsgruppen har uttrykt bekymring for de situasjoner der en «trygg havn»-organisasjon overtas eller fusjonerer med et foretak som ikke har forpliktet seg til å overholde «trygg havn»-prinsippene. Arbeidsgruppen synes å forutsette at foretaket som blir igjen, ikke er bundet til å bruke «trygg havn»-prinsippene på personopplysninger fra organisasjonen som overtas, men det er ikke nødvendigvis tilfellet i henhold til amerikansk lovgivning. Hovedregelen i USA med hensyn til fusjoner og overtakelser er at foretak som overtar aksjene i et annet foretak, som regel tar over denne organisasjonens forpliktelser og ansvar. Jf. 15 Fletcher *Cyclopedia of the Law of Private Corporations*, § 7117 (1990); jf. også *Model Bus. Corp. Act*, § 11.06(3) (1979) («det gjenværende foretak overtar alle forpliktelser fra hvert foretak som er del i fusjonen»). Med andre ord blir det gjenværende foretak etter en fusjon med, eller en overtakelse av, et «trygg havn»-foretak, bundet av sistnevntes «trygg havn»-forpliktelser.

Selv om en fusjon eller overtakelse skjer ved kjøp av aktiva, kan forpliktelsene til det oppkjøpte foretaket dessuten i visse tilfeller likevel være bindende for oppkjøperen. Jf. 15 Fletcher, § 7122. Selv når forpliktelsene ikke følger med i fusjonen, er det imidlertid verd å merke seg at de heller ikke ville følge med i en fusjon der opplysningene ble overført fra Europa i henhold til en avtale, som er det eneste holdbare alternativet til «trygg havn»-prinsippene for overføring av opplysninger til USA. I tillegg kreves det i «trygg havn»-dokumentenes nåværende utgave at alle «trygg havn»-organisasjoner underretter det amerikanske handelsdepartement om enhver overtakelse og gir mulighet til fortsatt å overføre opplysninger til den overtakende organisasjon bare dersom den slutter seg til «trygg havn»-ordningen, jf. VS nr. 6. USA har nemlig endret «trygg havn»-bestemmelsene slik at de amerikanske organisasjonene i denne situasjon pålegges å slette de opplysninger som de har mottatt innenfor rammene av «trygg havn»-ordningen, dersom deres «trygg havn»-deltaking ikke opprettholdes eller det ikke treffes andre passende sikkerhetstiltak.

VEDLEGG V

14. juli 2000

John Mogg
Generaldirektør, DG XV
Europakommisjonen
Kontor C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Brussel

Herr John Mogg,

Jeg forstår at en rekke spørsmål har oppstått som følge av mitt brev av 29. mars 2000. Derfor henvender jeg meg igjen for å redegjøre for vår myndighet på de berørte områder, og dette brevet, som utfyller og sammenfatter noen av de tidligere brevene, vil i framtiden med fordel kunne fungere som referansedokument.

De har i forbindelse med Deres besøk på vårt kontor og i Deres brev stilt en rekke spørsmål omkring den amerikanske Federal Trade Commissions (FTC) myndighet innenfor personvern ved direktekoblede tjenester. Jeg synes derfor at det vil være nyttig å gi et sammendrag av mine tidligere svar samt gi ytterligere opplysninger om FTCs myndighet med hensyn til de spørsmål om personvern for forbrukere som De tok opp i Deres seneste brev. De spør nærmere bestemt 1) om FTC har myndighet når overføring av ansettelsesopplysninger skjer i strid med de amerikanske «trygg havn»-prinsippene, 2) om FTC har myndighet i forbindelse med ideelle merkingsordninger for personvern, 3) om FTC Act får samme anvendelse på frakoblede og direktekoblede tjenester, samt 4) hva som skjer i tilfelle overlapping mellom FTCs og andre lovhåndhevende organers myndighet.

Anvendelse av FTC Act på personvern

FTCs rettslige myndighet på dette området er fastsatt i avsnitt 5 i FTC Act, som forbyr «urimelig eller villedende atferd eller praksis» i forbindelse med handel⁽¹⁾. Villedende praksis defineres som en framstilling, utelatelse eller praksis som antas å kunne villede en bonus pater familias på en avgjørende måte. En praksis er urimelig dersom den medfører eller antas å medføre en betydelig skade for forbrukerne som ikke på rimelig vis kan unngås, og som ikke oppveies av andre fordeler for forbrukerne eller konkurransen⁽²⁾.

Visse former for innsamling av opplysninger kan antas å være i strid med FTC Act. Dersom det for eksempel feilaktig hevdes at et nettsted er i samsvar med erklærte personvernbestemmelser eller et sett av retningslinjer for selvregulering, er det i avsnitt 5 i FTC Act rettslig grunnlag for å gjøre innsigelse mot slik avgivelse av uriktige opplysninger med påstand om at den er villedende. Vi har faktisk lyktes med å håndheve loven på en måte som har gjort det mulig å fastslå dette prinsippet⁽³⁾. FTC har dessuten besluttet i henhold til avsnitt 5 å gjøre innsigelse mot enhver urimelig personvernpraksis dersom den involverer barn eller bruk av svært følsomme opplysninger, herunder finansielle⁽⁴⁾ og medisinske opplysninger. FTC har håndhevet og vil fortsette å håndheve loven gjennom aktiv overvåking og undersøkelser samt på grunnlag av de saker som blir henvist fra selvreguleringsorganer og andre, herunder EU-medlemsstater.

⁽¹⁾ 15 USC § 45. Fair Credit Reporting Act får også anvendelse på innsamling og salg av Internett-opplysninger som omfattes av lovdefinisjonene av «forbrukeropplysning» og «forbrukeropplysningsbyrå».

⁽²⁾ 15 USC § 45(n).

⁽³⁾ Jf. GeoCities, saksnr. C-3849. (Endelig beslutning av 12. februar 1999, tilgjengelig på www.ftc.gov/os/1999/9902/9823015d%26o.htm); Liberty Financial Cos., saksnr. C-3891 (Endelig beslutning av 12. august 1999, tilgjengelig på www.ftc.gov/opa/1999/9905/younginvestor.htm). Jf. også Children's Online Privacy Protection Act Rule (COPPA), 16 C.F.R. del 312, tilgjengelig på www.ftc.gov/opa/1999/9910/childfinal.htm. Det kreves i henhold til COPPA-regelen, som trådte i kraft forrige måned, at operatører av nettsteder som henvender seg til barn under 13 år, eller som bevisst samler inn personopplysninger fra barn under 13 år, følger de prinsipper for god informasjonspraksis (fair information practice standards) som er fastsatt i regelen.

⁽⁴⁾ Jf. FTC v. Touch Tone, Inc., sivilt søksmål nr. 99-WM-783 (D.Co), registrert 21. april 1999, tilgjengelig på www.ftc.gov/opa/1999/9904/touchtone.htm. Uttalelse (Staff Opinion Letter) av 17. juli 1997 utstedt som svar på en anmodning om rettsmøte fra Center for Media Education, tilgjengelig på www.ftc.gov/os/1997/9707/cenmed.htm.

FTC støtter selvregulering

FTC vil gi prioritet til saker som gjelder manglende overholdelse av retningslinjene for selvregulering som henvises fra organisasjoner som for eksempel BBBOnline og TRUSTe (.). Denne framgangsmåten vil være i samsvar med vårt mangeårige samarbeid med National Advertising Review Board (NARB), under Better Business Bureau, som henviser klager som gjelder reklame til FTC. National Advertising Division (NAD) under NARB avgjør klager som gjelder landsdekkende reklame ved en form for voldgift. Dersom en part nekter å rette seg etter en avgjørelse truffet av NAD, henvises saken til FTC. FTCs saksbehandlere gir saken fortrinnsrett og undersøker den aktuelle reklamen for å fastslå om den er i strid med FTC Act. FTC lykkes ofte med å stanse den omstridte praksisen, eller med å overbevise parten om å gjenoppta NARB-proseduren.

FTC gir på samme måte prioritet til saker om manglende overholdelse av «trygg havn»-prinsippene som henvises fra EU-medlemsstatene. Som tilfellet er med saker som henvises fra amerikanske selvreguleringsorganer, vil FTCs saksbehandlere ta hensyn til enhver opplysning som kan bidra til å fastslå om den aktuelle praksis er i strid med avsnitt 5 i FTC Act. Denne forpliktelsen framgår også av «trygg havn»-prinsippene under VS nr. 11 om håndheving.

GeoCities: FTCs første sak om personvern ved direktekoblede tjenester.

FTCs første sak om personvern på Internett, GeoCities, ble innledet på grunnlag av FTCs myndighet i henhold til avsnitt 5⁽⁵⁾. FTCs påstand i denne saken at GeoCities gav uriktige opplysninger til både barn og voksne om hvordan deres personopplysninger ville bli brukt. Ifølge FTCs klage opplyste GeoCities at visse personopplysninger som ble samlet inn gjennom nettstedet var beregnet bare til intern bruk eller til å gi forbrukerne særskilte reklametilbud, varer eller tjenester som de hadde bedt om, samt at visse tilleggsopplysninger som forbrukeren stod fritt til å oppgi, ikke ville bli videreformidlet til tredjemann uten forbrukerens tillatelse. Opplysningene ble imidlertid gitt videre til tredjemann, som brukte dem til målrettede henvendelser som forbrukeren ikke hadde gitt sin tillatelse til. Et av klagepunktene var også at GeoCities' praksis med hensyn til innsamling av opplysninger fra barn, var villedende. I henhold til FTCs klage opplyste GeoCities at de på sin nettside hadde et område for barn, og at de opplysninger som ble innsamlet her, ble forvaltet av GeoCities. I virkeligheten ble disse områdene på nettstedet drevet av tredjemann som samlet inn og oppbevarte opplysningene.

Avgjørelsen i denne saken forbyr GeoCities å gi uriktige opplysninger om formålet for innsamlingen eller bruken av personopplysninger fra eller om forbrukere, herunder barn. Foretaket pålegges å legge ut på nettstedet en klar og tydelig personvernmelding, slik at forbrukerne får vite om hvilke opplysninger som samles inn, for hvilke formål de samles inn, hvem de vil bli videreformidlet til og hvordan forbrukerne kan få innsyn i og eventuelt fjerne disse opplysningene. For å sikre foreldrekontroll, pålegges GeoCities også å innhente samtykke fra foreldrene før de samler inn opplysninger fra barn under 13 år. GeoCities pålegges å underrette sine abonnenter og gi dem muligheten til å få sine personopplysninger slettet fra GeoCities' og enhver tredjemanns database. I avgjørelsen angis særskilt at GeoCities skal underrette foreldre til barn under 13 år og slette deres personopplysninger, med mindre en av foreldrene uttrykkelig gir sitt samtykke til at opplysningene oppbevares og brukes. Til slutt pålegges GeoCities å kontakte enhver tredjemann som foretaket tidligere har videreformidlet opplysninger til, for å anmode om at også disse opplysningene blir slettet⁽⁶⁾.

ReverseAuction.com

I januar 2000 godkjente FTC en klage mot, og inngikk deretter forlik med, ReverseAuction.com, et auksjonsnettsted som i henhold til klagen innhentet personopplysninger om forbrukerne fra et konkurrerende nettsted (eBay.com) for deretter å sende villedende og uønsket e-post for å markedsføre seg selv overfor de aktuelle forbrukerne⁽⁷⁾. Vi hevdet i vår klage at ReverseAuction overtrådte avsnitt 5 i FTC Act ved å innhente personopplysninger som omfattet eBay-brukernes e-postadresser og brukeridentifikasjon («user ID»), og ved å sende villedende e-postmeldinger.

⁽⁵⁾ GeoCities, saksnr. C-3849, (endelig beslutning av 12. februar 1999, tilgjengelig på www.ftc.gov/os/1999/9902/9823015d%26o.htm).

⁽⁶⁾ FTC avgjorde senere en annen sak som gjaldt elektronisk innsamling av personopplysninger fra barn. Liberty Financial Companies Inc. drev nettstedet Young Investor, som henvendte seg til barn og tenåringer og fokuserte på penge- og investerings spørsmål. FTC hevdet at nettstedet feilaktig opplyste at personopplysningene som ble samlet inn fra barn i forbindelse med en undersøkelse, ville bli oppbevart anonymt, og at deltakerne ville motta et elektronisk nyhetsbrev og gaver. Personopplysningene om barna og om familiens økonomiske forhold ble i virkeligheten ikke oppbevart anonymt, og det ble verken sendt nyhetsbrev eller gaver. Liberty Financial forbyr med dette forliket å avgi slike uriktige opplysninger i framtiden, og pålegges å legge ut en personvernmelding på sine nettsider for barn, samt å innhente samtykke fra foreldrene, som kan etterprøves, før det samles inn personopplysninger fra barn. Liberty Financial Cos., saksnr. C-3891 (Endelig beslutning av 12. august 1999) (tilgjengelig på www.ftc.gov/opa/1999/9905/younginvestor.htm).

⁽⁷⁾ Jf. ReverseAuction.com, Inc., sivil søksmål nr. 000032 (D.D.C.) (registrert 6. januar 2000) (pressemelding og prosesskrifter: www.ftc.gov/opa/2000/01/reverse4.htm).

Som beskrevet i klagen lot ReverseAuction seg registrere som eBay-bruker før foretaket innhentet opplysninger, og det forpliktet seg til å overholde eBays brukeravtale og personvernprogram. Brukeravtalen og programmet sikrer forbrukernes personvern ved å forby eBay-brukerne å samle inn og bruke personopplysninger for ikke-tillatte formål, herunder å sende uønsket kommersiell e-post. I vår klage ble det for det første hevdet at ReverseAuction feilaktig utgav seg for å ville følge eBays brukeravtale og personvernprogram, noe som utgjør en villedende praksis i henhold til avsnitt 5 i FTC Act. For det andre hevdet vi at ReverseAuctions bruk av opplysningene for å sende uønsket kommersiell e-post i strid med brukeravtalen og personvernprogrammet, utgjorde en urimelig handelspraksis i henhold til avsnitt 5 i FTC Act.

Det ble dessuten hevdet i klagen at e-posten til brukerne inneholdt en villedende setning om at deres bruker-ID til eBay «snart ville utgå». Til slutt ble det hevdet at e-posten feilaktig opplyste om at eBay direkte eller indirekte forsynte ReverseAuction med eBay-brukernes personopplysninger eller på annet vis deltok i spredningen av uønsket e-post.

Avgjørelsen som ble oppnådd i denne saken, hindrer ReverseAuction i å begå disse overtredelsene i framtiden. ReverseAuction pålegges også å sende en melding til brukerne som lot seg registrere eller akter å la seg registrere hos ReverseAuction som følge av ReverseAuctions e-post. I meldingen underrettes disse forbrukerne om at deres bruker-ID til eBay ikke var i ferd med å utløpe, og at eBay ikke kjente til eller hadde tillatt ReverseAuctions spredning av uønsket e-post. Meldingen gir også disse forbrukerne muligheten til å annullere sin registrering hos ReverseAuction og til å få sine personopplysninger slettet fra ReverseAuctions database. Dessuten pålegges ReverseAuction med denne avgjørelsen å slette samt avstå fra å bruke eller videreformidle personopplysninger om eBay-abonnenter som mottok e-post fra ReverseAuction, men ikke lot seg registrere hos ReverseAuction. I samsvar med tidligere avgjørelser i personvernsaker som FTC har reist, ble ReverseAuction til slutt pålagt å offentliggjøre sitt eget personvernprogram på sitt nettsted, og avgjørelsen inneholder omfattende bestemmelser som gir FTC mulighet til å overvåke om avgjørelsen blir overholdt.

ReverseAuction-saken viser at FTC bestreber seg på å benytte håndheving for å støtte næringens selvregulering innenfor personvern ved direktekoblede tjenester. Det ble i denne saken gjort direkte innsigelse mot en praksis som undergraver en brukeravtale og et personvernprogram som sikrer forbrukernes personvern, og som kunne forringe forbrukernes tillit til direktekoblede foretaks personverntiltak. Fordi denne saken omfattet et foretaks urettmessige tilegnelse av forbrukeropplysninger som var beskyttet av et annet foretaks personvernprogram, kan den være særlig relevant med hensyn til beskyttelse av personopplysninger som overføres mellom foretak i ulike land.

Til tross for FTCs rettshåndhevende tiltak i tilfellene GeoCities, Liberty Financial Cos. og ReverseAuction, har FTC mer begrenset myndighet på visse områder innenfor personvern ved direktekoblede tjenester. Som tidligere nevnt, får FTC Act anvendelse bare på innsamling og bruk av personopplysninger uten samtykke, men bare dersom den aktuelle praksisen er enten villedende eller urimelig. FTC Act vil dermed ikke få anvendelse på et nettsted som samler inn personopplysninger fra forbrukere, dersom det ikke har blitt gitt uriktige opplysninger om formålet for den aktuelle innsamlingen, eller dersom opplysningene ikke har blitt brukt eller videreformidlet på en måte som kan medføre betydelig skade for forbrukerne. FTC har i øyeblikket heller ikke fullmakt til å kreve at organisasjoner som samler inn opplysninger via Internett, i alminnelighet slutter seg til et personvernprogram, eller at en organisasjon slutter seg til et særskilt program⁽⁸⁾. Som nevnt ovenfor, kan et foretaks manglende overholdelse av et personvernprogram som det har erklært at det vil overholde, likevel betraktes som en villedende praksis.

⁽⁸⁾ FTC har av den grunn tilkjennegitt overfor den amerikanske kongressen at det sannsynligvis ville bli nødvendig å vedta ytterligere lovgivning for å påby alle amerikanske kommersielle nettsteder som henvender seg direkte til forbrukerne, å følge god informasjonspraksis. «Consumer Privacy on the World Wide Web» framlagt for Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce United States House of Representatives, 21. juli 1998, (tilgjengelig på www.ftc.gov/os/9807/privac98.htm). FTC har utsatt sin anmodning om en slik lovgivning for at nettstedene gjennom selvregulering skal få muligheten til å demonstrere mer utstrakt bruk av god informasjonspraksis. I FTCs rapport til kongressen om personvern ved tilkoblede tjenester (Privacy Online: A Report to Congress) av juni 1998 (tilgjengelig på www.ftc.gov/reports/privacy3/toc.htm) anbefalte FTC at det i lovgivningen skulle være et krav om at kommersielle nettsteder skal innhente foreldrenes samtykke for det samles inn personopplysninger fra barn under 13 år. Jf. fotnote 3. Det ble i FTCs rapport (Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress) av juli 1999 (tilgjengelig på www.ftc.gov/os/1999/9907/index.htm#13) fastslått at det hadde skjedd tilstrekkelige framskritt innen selvregulering, og at FTC dermed den gang valgte ikke å anbefale ytterligere lovgivning på det tidspunktet. I mai 2000 framla FTC en ny rapport for kongressen «Privacy Online: Fair Information Practices in the Electronic Marketplace» (tilgjengelig på www.ftc.gov/os/2000/05/index.htm#22), som behandler FTCs seneste undersøkelse av kommersielle nettsteder og deres overholdelse av god informasjonspraksis. I rapporten anbefales det også (av et flertall i FTC) at kongressen vedtar en lovgivning som fastsetter et minimumsnivå for personvern i forbindelse med kommersielle nettsteder som henvender seg til forbrukere.

FTCs myndighet på dette området omfatter dessuten urimelig eller villedende atferd eller praksis dersom slik atferd eller praksis utøves «i forbindelse med handel». Innsamling av opplysninger som foretas av kommersielle enheter som markedsførere varer eller tjenester, herunder innsamling og bruk av opplysninger for kommersielle formål, vil sannsynligvis oppfylle kravet om «virksomhet i forbindelse med handel». På den annen side kan mange enkeltpersoner eller enheter foreta direktekoplet innsamling av informasjon uten noe kommersielt formål og på den måten havne utenfor FTCs myndighet. Et eksempel på denne begrensningen er «chat rooms» som drives av ikke-kommersielle enheter, for eksempel villedelige organisasjoner.

Til slutt finnes det et antall helt eller delvis lovbestemte unntak fra FTCs grunnleggende myndighet med hensyn til handelspraksis som begrenser FTCs evne til å gi et uttømmende svar på alle spørsmål knyttet til personvern på Internett. Det gjelder bl.a. unntak for mange forbrukerorienterte foretak med stort behov for forbrukeropplysninger, som banker, forsikringsselskaper og luftfartsselskaper. Som kjent vil disse enhetene være underlagt andre føderale eller statlige organer, som for eksempel de føderale bankmyndighetene eller De forente staters transportdepartement.

I de saker der FTC har myndighet, og i den grad ressursene tillater det, behandler FTC klager fra forbrukerne som mottas via e-post eller telefon til forbrukertjenesten (Consumer Response Center - CRC) og i den senere tid også på nettstedet sitt⁽⁹⁾. CRC tar imot klager fra alle forbrukere, herunder forbrukere som er bosatt i EU-medlemsstater. FTC Act gir FTC myndighet til å nedlegge forbud eller påbud i forbindelse med nye overtredelser av FTC Act, samt til å gi oppreisning til skadelidende forbrukere. Vi vil likevel undersøke om det for det aktuelle foretak tegner seg et mønster av ulovlig adferd, ettersom vi ikke behandler individuelle forbrukerklager. Tidligere har FTC gitt erstatning til borgere både i USA og i andre land⁽¹⁰⁾. FTC vil i aktuelle tilfeller fortsatt utøve sin myndighet for at borgere fra andre land som har lidt skade som følge av en villedende praksis som omfattes av FTCs myndighet, skal få erstatning.

Ansettelsesopplysninger

De bad i Deres seneste brev om en ytterligere redegjørelse for FTCs myndighet med hensyn til ansettelsesopplysninger. For det første spør de om FTC i henhold til avsnitt 5 kan gripe inn overfor et foretak som hevder at det overholder de amerikanske «trygg havn»-prinsippene, men som overfører eller bruker ansettelsesopplysninger på en måte som er i strid med disse prinsippene. Vi vil gjerne forsikre Dem om at vi, etter nøye å ha gjennomgått den lovgivning som regulerer FTCs virksomhet, tilknyttede dokumenter og rettspraksis, har konkludert at FTC har samme myndighet med hensyn til ansettelsesopplysninger som det i alminnelighet har i henhold til avsnitt 5 i FTC Act. Det viser at dersom en sak oppfyller våre gjeldende krav (urimelig eller villedende handelspraksis) for å innlede søksmål med hensyn til personvern, vil vi kunne gripe inn i forbindelse med ansettelsesopplysninger.

Vi ønsker også å avvise enhver påstand om at FTCs evne til å treffe håndhevingstiltak med hensyn til personvern skulle være begrenset til situasjoner der et foretak har villedet individuelle forbrukere. Som FTCs sak mot ReverseAuction tydelig viser, akter FTC å treffe håndhevingstiltak i saker som gjelder overføring av opplysninger mellom foretak når det hevdes at et av foretakene har opptrådt ulovlig overfor et annet foretak og dermed har skadet både forbrukerne og foretaket. Vi forventer at problemene omkring ansettelsesopplysninger oftest vil oppstå i slike situasjoner, ettersom ansettelsesopplysninger om EU-borgere overføres fra europeiske til amerikanske foretak som har forpliktet seg til å overholde «trygg havn»-prinsippene.

Vi vil gjerne gjøre oppmerksom på ett tilfelle der FTCs muligheter likevel vil være begrensede, nemlig i situasjoner der saken allerede behandles innenfor rammene av en tradisjonell arbeidsrettslig tvisteløsningsprosedyre, som oftest i forbindelse med en klage eller voldgift, eller en klage over urimelig

⁽⁹⁾ Se <http://www.ftc.gov/ftc/complaint.htm> for FTCs elektroniske klageskjema.

⁽¹⁰⁾ For eksempel i en sak av nyere dato som omhandlet en pyramidesalgssordning på Internett, der FTC oppnådde en erstatning til 15 622 forbrukere på til sammen USD 5,5 millioner. Forbrukerne var bosatt i USA og 70 andre land. Jf. www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftcrefund01.htm.

arbeidspraksis ved National Labor Relations Board. Det kan for eksempel være tilfelle dersom en arbeidsgiver i en tariffavtale har forpliktet seg med hensyn til bruk av personopplysninger, og en arbeidstaker eller en fagforening hevder at arbeidsgiveren har misligholdt avtalen. FTC vil sannsynligvis avvise en slik sak⁽¹³⁾.

Myndighet med hensyn til merkingsordninger

Det andre spørsmålet Deres var om FTC har myndighet med hensyn til amerikanske merkingsordninger («seal» programs) som forvalter tvisteløsningsordninger i USA, som har feiltolket sin rolle med hensyn til håndheving av «trygg havn»-prinsippene og behandling av individuelle klager, selv når disse enhetene teknisk sett var ideelle organisasjoner. For å fastslå om FTCs myndighet omfatter en enhet som gir seg ut for å være ideell, undersøker vi nøye om den aktuelle enheten derimot søker vinning på vegne av sine medlemmer. FTC har lyktes med å gjøre sin myndighet gjeldende overfor slike enheter, og så sent som 24. mai 1999 bekreftet amerikansk høyesterett i saken mellom California Dental Association og Federal Trade Commission enstemmig at FTC i en sak om monopol hadde myndighet over en frivillig ideell sammenslutning av lokale tannklinikker. Retten uttalte:

«FTC Act omfatter ikke bare enheter som «har til formål å drive forretningsvirksomhet for egen vinnings skyld» (15 USC §44), men også dem som søker å oppnå vinning «for sine medlemmer» (...) Det er usannsynlig at kongressen har hatt til hensikt i denne grad å begrense bruksområdet for «hjelporganisasjoner», med den mulighet dette gir for å omgå loven, når formålet med FTC Act nettopp er å gjøre loven gjeldende.»

For å fastslå om FTC har myndighet over en særskilt ideell enhet som driver en merkingsordning, kreves det altså en saklig gjennomgåelse av i hvilken grad den aktuelle enheten har skaffet økonomiske fordeler for sine medlemmer. Dersom en slik enhet har forvaltet merkingsordningen på en måte som har skaffet medlemmene økonomiske fordeler, vil FTC antakelig bruke sin myndighet. Dessuten vil FTC trolig ha myndighet over en svikaktig merkingsordning som uriktig framstiller seg som en ideell enhet.

Personvern ved frakoplede tjenester

For det tredje påpeker De at vi i vår tidligere korrespondanse har fokusert på personvern i forbindelse med direktekoplede tjenester. FTC har lagt stor vekt på personvern ved direktekoplede tjenester som en avgjørende faktor for utviklingen av elektronisk handel, men FTC Act er fra 1914 og får dermed også anvendelse på frakoplede tjenester. Vi kan dermed saksøke foretak som tilbyr frakoplede tjenester, og som driver urimelig eller villedende handelspraksis med hensyn til forbrukernes personvern⁽¹⁴⁾. I en sak som ble reist av FTC i fjor (FTC v. TouchTone Information Inc⁽¹⁵⁾), ble en «informasjonsformidler» anklaget for ulovlig å ha innhentet og solgt private økonomiske opplysninger. FTC hevdet at TouchTone skaffet seg forbrukernes opplysninger «under foregivende» (pretexting), et begrep som oppstod blant private etterforskere og betyr at man skaffer seg adgang til personopplysninger om andre under falskt påskudd, vanligvis per telefon. I saken som ble registrert 21. april 1999 ved en føderal domstol i Colorado, ble det nedlagt påstand om forbud og tilbakebetaling av alle urettmessige økonomiske gevinster.

Disse erfaringene med håndheving av loven og den voksende bekymring på grunn av sammenslåingen av frakoplede og direktekoplede databaser, det uklare skillet mellom direktekoplede og frakoplede handel, samt det faktum at en betydelig mengde personopplysninger samles inn og brukes frakoplet, viser klart at det kreves en særlig innsats med hensyn til personvern i forbindelse med frakoplede tjenester.

Overlappende myndighet

Til slutt spør De om samspillet mellom FTCs og andre rettshåndhevende organers myndighet, særlig i saker der myndigheten kan være overlappende. Vi har utviklet et nært samarbeid med en lang rekke andre rettshåndhevende organer, deriblant de føderale bankmyndighetene og delstatenes statsadvokater. Vi samordner ofte våre undersøkelser for å dra størst mulig nytte av våre ressurser i saker med overlappende

⁽¹³⁾ Bortsett fra de særskilte unntakene, (som framgår av lovbestemmelsene som fastsetter FTCs myndighet) er FTCs myndighet i henhold til FTC Act med hensyn til praksis «i forbindelse med handel» sammenfallende med kongressens forfatningsmessige myndighet i henhold til Commerce Clause, jf. United States v. American Building Maintenance Industries, 422 U.S. 271, 277 nr. 6 (1975). FTCs myndighet vil dermed omfatte foretaks og næringers ansettelsespraksis innenfor internasjonal handel.

⁽¹⁴⁾ Jf. «Online Auction Site Settles FTC Privacy Charges», FTC-pressemedling av 6. januar 2000, tilgjengelig på <http://www.ftc.gov/opa/2000/01/reverse4.htm>.

⁽¹⁵⁾ Avgjørelsen av om en praksis er en «urimelig arbeidspraksis» eller et brudd på en tariffavtale, er et teknisk spørsmål som vanligvis overlates til arbeidsdomstolene, som hører partene, herunder voldgiftsdommere og NLRB.

myndighet. Vi henviser dessuten ofte saker til de relevante organer på føderalt eller delstatlig plan for utredning.

Jeg håper at dette brevet vil være til hjelp, og står naturligvis til rådighet dersom De skulle ønske ytterligere opplysninger.

Med vennlig hilsen

Robert Pitofsky

VEDLEGG VI

John Mogg
Generaldirektør, GD XV
Europakommisjonen
Kontor C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Brussel

Herr generaldirektør

Dette brevet sendes til Dem på anmodning fra De forente staters handelsdepartement for å redegjøre for hvilken rolle De forente staters transportdepartement har med hensyn til forbrukernes personvern i forbindelse med de opplysninger de avgir til luftfartsselskaper.

Transportdepartementet går inn for selvregulering ettersom det er et mindre inngrep som gir den mest effektive beskyttelsen av de opplysninger som forbrukerne avgir til luftfartsselskapene, og det støtter derfor opprettelsen av en «trygg havn»-ordning som vil gi luftfartsselskapene mulighet til å oppfylle kravene i Den europeiske unions personverndirektiv med hensyn til overføringer utenfor EU. Departementet innser imidlertid at en selvreguleringsordning kan fungere bare dersom luftfartsselskapene som forplikter seg til å overholde «trygg havn»-ordningens personvernprinsipper, også faktisk følger dem. Derfor bør selvregulering kombineres med retts håndheving. Departementet vil derfor gjøre bruk av sin eksisterende lovfestede myndighet med hensyn til forbrukervern, for å sikre at luftfartsselskapene overholder sine offentlige erklæringer om personvern, og til å behandle saker om påstått manglende overholdelse som det får henvist fra selvreguleringsorganisasjoner og andre, herunder EU-medlemsstatene.

Departementet har gjennomføringsmyndighet på dette området i henhold til 49 USC 41712 som forbyr transportører å bruke «en urimelig eller villedende praksis eller urimelige konkurransemetoder» ved salg av lufttransportytelser som er eller kan være til skade for forbrukerne. Avsnitt 41712 er utformet etter avsnitt 5 i Federal Trade Commission Act (15 USC 45). Luftfartsselskaper er i henhold til 15 USC 45(a)(2) imidlertid ikke underlagt Federal Trade Commissions regulering etter avsnitt 5.

Mitt kontor behandler og forfølger saker under 49 U.S.C. 41712 (jf. for eksempel transportdepartementets beslutning 99-11-5 av 9. november 1999; 99-8-23 av 26. august 1999; 99-6-1 av 1. juni 1999; 98-6-24 av 22. juni 1998; 98-6-21 av 19. juni 1988; 98-5-31 av 22. mai 1998 og 97-12-23 av 18. desember 1997.) Vi innleder rettsforfølging i slike saker på grunnlag av våre egne undersøkelser eller som følge av formelle og uformelle klager fra enkeltpersoner, reisebyråer, luftfartsselskaper samt offentlige myndigheter i USA og i utlandet.

Jeg vil gjerne understreke at det ikke automatisk blir betraktet som en overtredelse av avsnitt 41712 dersom en transportør unnlater å beskytte passasjeropplysninger. Dersom en transportør formelt og offentlig har forpliktet seg til å overholde «trygg havn»-prinsippene og dermed beskytte de forbrukeropplysninger vedkommende kommer i besittelse av, kan departementet gjøre bruk av sin lovfestede myndighet i henhold til avsnitt 41712 for å sikre at prinsippene overholdes. Dersom en passasjer gir opplysninger til en transportør som har forpliktet seg til å overholde «trygg havn»-prinsippene, kan det derfor være til skade for forbrukeren og dermed være en overtredelse av avsnitt 41712 dersom denne forpliktelsen ikke overholdes. Mitt kontor akter å gi høyeste prioritet til behandlingen av enhver påstand om slike forhold og til rettsforfølgelse av enhver sak der det foreligger beviser for slike forhold. Vi vil også underrette handelsdepartementet om utfallet av eventuelle slike saker.

Overtredelser av avsnitt 41712 kan medføre at det utstedes forbud og iverksettes sivilrettslige sanksjoner dersom disse forbudene ikke følges. Selv om vi ikke har myndighet til å tilkjenne erstatning eller gi økonomisk godtgjøring til individuelle klagere, kan vi godkjenne forlik som inngås på bakgrunn av undersøkelser og saker som er reist av departementet, og som gir forbrukerne en viss kompensasjon enten i form av nedsettelse eller utligning av gebyrer eller lignende som ellers skulle betales. Vi har tidligere gjort det slik, og kan og vil, når det er berettiget, fortsette denne praksisen innenfor rammene av «trygg havn»-ordningen. Dersom et amerikansk luftfartsselskap gjentatte ganger overtrer avsnitt 41712, vil det

også oppstå tvil om selskapets evne til i det hele tatt å overholde loven, noe som i ekstreme tilfeller kan medføre at det blir ansett som uegnet til å drive virksomhet, og dermed mister sin tillatelse (jf. transportdepartementets beslutning 93-6-34 av 23. juni 1993 og 93-6-11 av 9. juni 1993. Selv om disse sakene ikke var omfattet av avsnitt 41712, ble den aktuelle transportøren fratatt sin tillatelse etter fullstendig å ha ignorert bestemmelsene i Federal Aviation Act, som er en bilateral avtale, og departementets regler og forskrifter).

Jeg håper at De kan dra nytte av disse opplysningene, og står naturligvis til rådighet dersom De har spørsmål eller ønsker ytterligere opplysninger.

Med vennlig hilsen

Samuel Podberesky

Assistant General Counsel for
Aviation Enforcement and Proceeding

VEDLEGG VII

Med henvisning til artikkel 1 nr. 2 bokstav b) er de amerikanske offentlige organer som har myndighet til å behandle klager og utstede forbud eller påbud i forbindelse med urimelig eller villedende praksis og oppnå oppreisning for enkeltpersoner, uavhengig av bostedsstat eller nasjonalitet i tilfelle av manglende overholdelse av prinsippene som gjennomføres i samsvar med VS:

- 1) Federal Trade Commission
- 2) De forente staters transportdepartement

Federal Trade Commission utøver sin myndighet i henhold til avsnitt 5 i Federal Trade Commission Act. Federal Trade Commission har i henhold til avsnitt 5 ikke myndighet med hensyn til banker, spare- og utlånsforetak og kredittforeninger, offentlige teleselskaper og offentlige mellomstatlige transportører, luftfartsselskaper samt emballeringsbedrifter og kjøttvareprodusenter. Selv om forsikringsbransjen ikke uttrykkelig er oppført på listen over unntak i avsnitt 5, overlates det i henhold til McCarran-Ferguson Act⁽¹⁾ til de enkelte stater å regulere forsikringsbransjen. FTC Act får anvendelse på forsikringsbransjen i den grad den ikke omfattes av enkeltstatenes lovgivning. FTC har fortsatt myndighet over forsikringsselskaper som følger urimelig eller villedende praksis i annen virksomhet enn forsikringsvirksomhet.

De forente staters transportdepartement utøver sin myndighet i henhold til avdeling 49 i United States Code avsnitt 41712. Det amerikanske transportdepartementet behandler saker på grunnlag av egne undersøkelser så vel som på grunnlag av formelle og uformelle klager fra borgere, reisebyråer, luftfartsselskaper samt amerikanske og utenlandske offentlige organer.

⁽¹⁾ U.S.C. § 1011 *et seq.*