KOMMISSIONENS BESLUT

av den 26 juli 2000

enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (*Safe Harbor Privacy Principles*) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat

[delgivet med nr K(2000) 2441]

(Text av betydelse för EES)

(2000/520/EG)

EUROPEISKA GEMENSKAPERNAS KOMMISSION HAR FATTAT DETTA BESLUT

med beaktande av Fördraget om upprättandet av Europeiska gemenskapen,

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter [1], särskilt artikel 25.6 i detta, och

av följande skäl:

(1) Enligt direktiv 95/46/EG skall medlemsstaterna föreskriva att överföring av personuppgifter till tredje land endast får ske om ifrågavarande tredje land säkerställer en adekvat skyddsnivå och om medlemsstatens lagar genom vilka andra bestämmelser i direktivet genomförs, efterlevs före överföringen.

(2) Kommissionen kan konstatera att ett tredje land har en adekvat skyddsnivå. I sådana fall får personuppgifter överföras från medlemsstaterna utan att det behövs några ytterligare garantier.

(3) Enligt direktiv 95/46/EG skall bedömningen av skyddsnivån ske på grundval av alla de förhållanden som har samband med en överföring eller en grupp överföringar av uppgifter och vissa omständigheter skall särskilt beaktas. Arbetsgruppen för skydd av enskilda med avseende på behandling av personuppgifter som inrättats genom det direktivet [2] har utfärdat riktlinjer för hur sådana beddömningar skall göras [3].

(4) Mot bakgrund av de olika sätten att se på frågan om uppgiftsskydd i olika tredje länder bör bedömningen av om skyddsnivån är adekvat ske, och beslut som grundar sig på artikel 25.6 i direktiv 95/46/EG verkställas, utan godtycklig eller obefogad diskriminering i förhållande till tredje land eller mellan tredje länder där liknande förhållanden råder och så att det inte utgör ett dolt handelshinder. Härvid bör hänsyn tas till gemenskapens nuvarande internationella åtaganden.

(5) Den adekvata skyddsnivån för överföring av uppgifter från gemenskapen till Förenta staterna i enlighet med detta beslut bör anses ha uppnåtts om organisationer följer *Safe Harbor Privacy*-principerna för skydd av personuppgifter som överförs från en medlemsstat till Förenta staterna (nedan kallade principerna) och de vägledande frågorna och svaren (nedan kallade FoS) som utfärdats av Förenta staternas regering den 21 juli 2000. Organisationerna bör dessutom offentliggöra sin politik för skydd av personuppgifter och vara underställda antingen Federal Trade Commission (FTC) enligt avsnitt 5 i Federal Trade Commission Act, som förbjuder illojala eller bedrägliga handlingar eller metoder i handeln och i verksamhet som påverkar handeln, eller någon annan tillsynsmyndighet som på ett effektivt sätt ser till att principerna, tillämpade i överensstämmelse med FoS, efterlevs.

(6) Områden och/eller databehandling som inte lyder under någon av de myndigheter i Förenta staterna som anges i bilaga VII till detta beslut bör inte omfattas av beslutet.

(7) För att se till att detta beslut tillämpas korrekt är det nödvändigt att de organisationer som ansluter sig till

[1] EGT L 281, 23.11.1995, s. 31.

[2] Arbetsgruppen har Internetadressen: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

[3] Arbetsdokument 12: Överföring av personuppgifter till tredje land: Tillämpning av artiklarna 25 och 26 i EU:s direktiv om dataskydd, som antogs av arbetsgruppen den 24 juli 1998.

principerna och FoS kan erkännas av berörda parter, t.ex. de registrerade, exportörer av uppgifter och dataskyddsmyndigheter. I detta syfte bör Förenta staternas handelsministerium, eller det organ som ministeriet bestämmer, förbinda sig att föra och göra tillgänglig för allmänheten en förteckning över de organisationer som förpliktat sig att följa principerna i överensstämmelse med FoS och som lyder under åtminstone en av de myndigheter som nämns i bilaga VII till detta beslut.

(8) För att värna om öppenhet och för att bevara förmågan hos de behöriga myndigheterna i medlemsstaterna att garantera skydd av enskilda med avseende på behandlingen av deras personuppgifter är det nödvändigt att i detta beslut specificera vilka omständigheter som i undantagsfall bör medföra att vissa dataflöden avbryts, trots att skyddsnivån befunnits vara adekvat.

(9) Systemet med *safe harbor* sådant det utformats enligt principerna och FoS kan behöva ses över i ljuset av erfarenheter från utveckling på integritetsskyddets område under förhållanden då tekniken ständigt gör det lättare att överföra och behandla personuppgifter och i ljuset av rapporter om genomförande av berörda tillsynsmyndigheter.

(10) Arbetsgruppen för skydd av enskilda med avseende på behandling av personuppgifter som inrättats genom artikel 29 i direktiv 95/46/EG har avgivit yttranden om den skyddsnivå som erbjuds av *safe harbor*-principerna i Förenta staterna, och vid utarbetandet av föreliggande beslut har hänsyn tagits till dessa yttranden ([4]).

(11) De åtgärder som föreskrivs i detta beslut är förenliga med yttrandet från den kommitté som inrättats genom artikel 31 i direktiv 95/46/EG.

([4]) Arbetsdokument 15: Yttrande 1/99 om skyddsnivån i Förenta staterna med avseende på personuppgifter och de pågående diskussionerna mellan Europeiska kommissionen och Förenta staterna.
Arbetsdokument 19: Yttrande 2/99 om de internationella *safe harbor*-principer som utfärdades av Förenta staternas handelsministerium den 19 april 1999.
Arbetsdokument 21: Yttrande 4/99 om de frågor och svar (FoS) som skall utfärdas av amerikanska handelsministeriet.
Arbetsdokument 23: Arbetsdokument om det nuvarande läget i de pågående diskussionerna mellan Europeiska kommissionen och Förenta staternas regering om de "Internationella *safe harbor*-principerna".
Arbetsdokument 27: Yttrande 7/99 om nivån på det dataskydd som erbjuds av *safe harbor*-principerna sådana de offentliggjorts med frågor och svar (FoS) och andra tillhörande handlingar den 15 och 16 november 1999 av det amerikanska handelsministeriet.
Arbetsdokument 31: Yttrande 3/2000 om dialogen mellan Europeiska unionen och Förenta staterna beträffande *safe harbor*.
Arbetsdokument 32: Yttrande 4/2000 om den dataskyddsnivå som garanteras genom *safe harbor*-principerna.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

1. Med avseende på artikel 25.2 i direktiv 95/46/EG skall i fråga om all verksamhet som omfattas av det direktivet, *safe harbor*-principerna om integritetsskydd (nedan kallade principerna), se bilaga I till detta beslut, tillämpade i enlighet med den vägledning som ges i de frågor och svar (nedan kallade FoS) som utfärdats av Förenta staternas handelsministerium den 21 juli 2000, se bilaga II till detta beslut, anses utgöra en adekvat skyddsnivå för personuppgifter som överförs från gemenskapen till organisationer som är etablerade i Förenta staterna med beaktande av följande dokument som utfärdats av Förenta staternas handelsministerium:

a) En översikt över genomförandet av *safe harbor*, bilaga III.

b) Ett memorandum om ersättning vid kränkning av enskildas integritet och uttryckliga behörigheter i Förenta staternas lagstiftning, bilaga IV.

c) En skrivelse från Federal Trade Commission, bilaga V.

d) En skrivelse från Förenta staternas transportministerium, bilaga VI.

2. I samband med varje överföring av uppgifter skall följande villkor vara uppfyllda:

a) Den organisation som tar emot uppgifterna har otvetydigt och offentligt förpliktat sig att följa principerna såsom de tillämpas i enlighet med FoS, och

b) denna organisation omfattas av de lagstadgade befogenheter som tillkommer någon av de myndigheter i Förenta staterna som anges i bilaga VII till detta beslut och som är bemyndigade att handlägga klagomål och ge upprättelse vid användning av illojala och bedrägliga metoder och att utverka skadestånd åt enskilda, oberoende av deras bosättningsland eller nationalitet, om principerna inte följs i överensstämmelse med FoS.

3. De villkor som anges i punkt 2 skall anses vara uppfyllda för varje organisation som genom självcertifiering förbinder sig att följa principerna i överensstämmelse med FoS från den dag då organisationen underrättar Förenta staternas handelsministerium, eller det organ som ministeriet bestämmer, om offentliggörandet av den förpliktelse som avses i punkt 2 a och om namnet på den myndighet som avses i punkt 2 b.

Artikel 2

Detta beslut gäller endast frågan om den skyddsnivå är adekvat som enligt principerna och FoS erbjuds i Förenta staterna, i förhållande till de krav som ställs i artikel 25.1 i direktiv 95/46/EG, och det påverkar inte tillämpningen av andra bestämmelser i det direktivet som gäller behandling av personuppgifter inom medlemsstaterna, särskilt artikel 4 i direktivet.

Artikel 3

1. Utan att det påverkar de befogenheter behöriga myndigheter i medlemsstaterna har att vidta åtgärder för att säkra efterlevnaden av nationella bestämmelser som antagits enligt andra bestämmelser i direktiv 95/46/EG än artikel 25, får dessa myndigheter utöva sin befogenhet att tillfälligt förbjuda överföringen av uppgifter till en organisation som genom självcertifiering förbundit sig att följa principerna i överensstämmelse med FoS, i syfte att skydda enskilda med avseende på behandling av deras personuppgifter i de fall då

a) den myndighet i Förenta staterna som avses i bilaga VII till detta beslut eller en sådan oberoende instans för handläggning av klagomål som avses under a i avsnittet om kontroll av efterlevnaden i bilaga I till detta beslut, har funnit att organisationen agerar i strid med principerna tillämpade i överensstämmelse med FoS, eller

b) det är i hög grad sannolikt att principerna överträds, det finns välgrundad anledning att tro att den berörda instansen för handläggning av klagomål inte vidtar och inte i rätt tid kommer att vidta de åtgärder som behövs för att lösa problemet, en fortsatt överföring av uppgifterna skulle innebära en överhängande risk för allvarlig skada för registrerade, och de behöriga myndigheterna i medlemsstaten har gjort vad som under rådande omständigheter rimligvis kan krävas för att anmärka mot organisationen och ge den tillfälle att gå i svaromål.

Förbudet skall hävas så snart det säkerställts att organisationen följer principerna i överensstämmelse med FoS och de behöriga myndigheterna i Europeiska unionen har underrättats härom.

2. Medlemsstaterna skall utan dröjsmål underrätta kommissionen om åtgärder som vidtagits med stöd av punkt 1.

3. Medlemsstaterna och kommissionen skall även underrätta varandra om varje fall där en myndighet, som är ansvarig för att principerna tillämpade i överensstämmelse med FoS följs i Förenta staterna, inte kunnat säkerställa detta.

4. Om den information som inhämtats i enlighet med punkterna 1, 2 och 3 visar att någon av de myndigheter som har ansvar för att principerna tillämpade i överensstämmelse med FoS följs i Förenta staterna inte fullgör denna uppgift på ett effektivt sätt, skall kommissionen underrätta Förenta staternas handelsministerium om detta och vid behov lägga fram förslag till bestämmelser i enlighet med det förfarande som föreskrivs i artikel 31 i direktivet i syfte att helt eller tills vidare upphäva detta beslut eller begränsa dess tillämpningsområde.

Artikel 4

1. Detta beslut kan vid vilken tidpunkt som helst ändras på grundval av erfarenheter i samband med beslutets genomförande och/eller om det i Förenta staternas lagstiftning ställs krav på minst samma skyddsnivå, som den som uppnås genom principerna och FoS.

Kommissionen skall under alla omständigheter utvärdera tillämpningen av detta beslut på grundval av tillgänglig information tre år efter det att beslutet delgivits medlemsstaterna och skall underrätta den kommitté som inrättats gemom artikel 31 i direktiv 95/46/EG om alla iakttagelser av betydelse, däribland omständigheter som kan påverka den gjorda bedömningen att bestämmelserna i artikel 1 i detta beslut ger ett adekvat skydd i den mening som avses i artikel 25 i direktiv 95/46/EG samt varje omständighet som tyder på att detta beslut tillämpas på ett sätt som innebär diskriminering.

2. Kommissionen skall om så behövs föreslå åtgärder i enlighet med det förfarande som föreskrivs i artikel 31 i direktivet.

Artikel 5

Medlemsstaterna skall vidta alla åtgärder som är nödvändiga för att följa detta beslut senast nittio dagar efter det att beslutet har delgivits medlemsstaterna.

Artikel 6

Detta beslut riktar sig till medlemsstaterna.

Utfärdat i Bryssel den 26 juli 2000.

På kommissionens vägnar

Frederik BOLKESTEIN

Ledamot av kommissionen

BILAGA I

PRINCIPER OM *SAFE HARBOR* OCH INTEGRITETSSKYDD

fastlagda av Amerikas förenta staters handelsministerium den 21 juli 2000

Europeiska unionens omfattande lagstiftning om uppgiftsskydd, direktivet om skydd av personuppgifter (nedan kallat direktivet), trädde i kraft den 25 oktober 1998. Enligt direktivet får överföring av personuppgifter endast göras till tredje land som säkerställer ett adekvat skydd av den personliga integriteten. Även om målet för Förenta staterna (nedan kallat USA) och Europeiska unionen (nedan kallad EU) är detsamma, nämligen att stärka integritetsskyddet för sina medborgare, har USA anammat ett annat tillvägagångssätt i fråga om integritetsskydd än EU. USA använder sig av ett sektoriellt tillvägagångssätt som bygger på en blandning av lagstiftning, reglering och självreglering. Mot bakgrund av dessa skillnader känner många organisationer i USA osäkerhet inför effekterna av EU-kravet på en adekvat standard vid överföring av personuppgifter från EU till USA.

För att minska osäkerheten och för att ge en mer förutsägbar struktur åt sådan dataöverföring fastlägger handelsministeriet (Department of Commerce) detta dokument och frågorna och svaren (principerna) i enlighet med sitt lagstadgade bemyndigande att stödja, främja och utveckla utrikeshandeln. Principerna har utarbetats i samråd med näringslivet och allmänheten föra att underlätta handel och affärsverksamhet mellan USA och EU. De är endast avsedda att tillämpas på de organisationer i USA som tar emot personuppgifter från EU och syftet är att dessa organisationer skall uppfylla villkoren för *safe harbor* samt den presumtion om ”adekvat skyddsnivå” som därmed skapas. Eftersom principerna endast är utformade för att tjäna detta specifika ändamål skulle det vara olämpligt om de godkändes för andra ändamål. Principerna får inte tillämpas i stället för nationella bestämmelser som genomför direktivet och som gäller vid behandling av personuppgifter i medlemsstaterna.

Det är helt och hållet frivilligt för en organisation att besluta om den vill ansluta sig till *safe harbor*-systemet, och organisationerna kan gå tillväga på olika sätt för att tillerkännas *safe harbor*-status. Organisationer som beslutar sig för att följa principerna måste rätta sig efter dem för att få och behålla sin *safe harbor*-status och offentligt deklarera att de följer dem. Om till exempel en organisation ansluter sig till ett integritetsskyddsprogram som utarbetats inom den privata sektorn och som följer principerna, är denna organisation berättigad till att omfattas av *safe harbor*-systemet. En organisation kan också ansluta sig genom att utarbeta en egen policy för integritetsskydd under förutsättning att denna överensstämmer med principerna. Om en organisation ansluter sig till ett integritetsskyddsprogram som utarbetats inom den privata sektorn eller utarbetar sin egen policy för integritetsskydd skall den på samma sätt kunna ställas till svars enligt paragraf 5 i Federal Trade Commission Act, som förbjuder illojal eller bedräglig praxis, eller liknande lagstiftning som förbjuder sådana handlingar om organisationen inte följer bestämmelserna. (Se bilagan för förteckningen över tillsynsmyndigheter i USA som erkänts av EU.) Dessutom kan organisationer som är underställda i USA gällande lagar, förordningar, förvaltningslagar eller andra lagsamlingar (eller bestämmelser) som effektivt skyddar den personliga integriteten med avseende på personuppgifter även åtnjuta de förmåner som *safe harbor* för med sig. Förmåner i samband med *safe harbor* garanteras i alla dessa fall från och med det datum då en organisation som vill ansluta sig till *safe harbor* lämnar in en självcertifiering till handelsministeriet (eller dess företrädare) om att principerna kommer att efterlevas i enlighet med vägledningen i den FoS som handlar om självcertifiering.

Efterlevnaden av principerna kan begränsas a) till vad som är nödvändigt för att uppfylla krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden eller b) av lagar, myndighetsföreskrifter eller rättspraxis som skapar motstridiga skyldigheter eller ger explicita befogenheter, förutsatt att organisationen då den utövar dessa befogenheter kan visa att avvikelsen från principerna begränsar sig till vad som är nödvändigt för att de övergripande legitima intressen som är beroende av dessa befogenheter skall kunna tillgodoses, eller c) om följden av direktivet eller medlemsstaternas lagstiftning är att man tillåter undantag och avvikelser förutsatt att sådana undantag eller avvikelser tillämpas i jämförbara sammanhang. I överenstämmelse med målen om ökat integritetsskydd bör organisationerna sträva efter att genomföra dessa principer öppet och fullt ut, samt även ange i sina planer för integritetsskydd på vilka områden undantag från principerna av skäl angivna i b ovan kommer att göras regelbundet. Av samma skäl förväntas organisationerna, såvida det finns en valmöjlighet enligt principerna och/eller amerikansk lag, välja en högre skyddsnivå om det är möjligt.

Organisationerna kan av praktiska eller andra skäl vilja tillämpa principerna på hela sin verksamhet av uppgiftsbehandling, men de är endast skyldiga att tillämpa dem på uppgifter som överförts efter det att de anslutit sig till *safe harbor*. För att en organisation skall vara berättigad till att omfattas av *safe harbor* krävs inte att den tillämpar principerna på uppgifter i register som sköts manuellt. Organisationer som vill ansluta sig till *safe harbor* i fråga om att från EU ta emot överföringar av uppgifter i register som sköts manuellt kan tillämpa principerna på alla sådana dataöverföringar efter det att de anslutit sig till *safe harbor*. En organisation som vill att förmånerna i samband med *safe harbor* även skall omfatta personaluppgifter som överförs från EU för att användas i samband med ett anställningsförhållande måste ange detta när den lämnar in sin självcertifiering till handelsministeriet (eller dess företrädare) och uppfylla kraven enligt FoS om självcertifiering. Organisationerna kan även lämna de garantier som anses vara nödvändiga enligt artikel 26 i direkti-

vet om de innefattar principerna i skriftliga överenskommelser med den part som överför uppgifterna från EU i fråga om de centrala integritetsskyddsbestämmelserna, när övriga bestämmelser för sådana standardavtal är godkända av kommissionen och medlemsstaterna.

Frågor som rör tolkning och efterlevnad av *safe harbor*-principerna (inbegripet frågor och svar) och den policy för integritetsskydd som tillämpas av organisationer anslutna till *safe harbor* omfattas av amerikansk lag utom i de fall då en organisation har förbundit sig att samarbeta med dataskyddsmyndigheter i EU. Där inte annat sägs skall bestämmelser enligt *safe harbor*-principerna och därtill knutna frågor och svar gälla på de områden de avser.

Personuppgifter är sådana uppgifter om en identifierad eller identifierbar fysisk person som faller inom tillämpningen av direktivet och som mottagits av en organisation i USA från Europeiska unionen och är registrerade i någon form.

MEDDELANDE

En organisation måste meddela den enskilde anledningen till att den samlar in och använder uppgifter om honom eller henne, hur den enskilde kontaktar organisationen om han eller hon har frågor eller klagomål, vilken slags tredje man som får ta del av uppgifterna samt vilka valmöjligheter och tillvägagångssätt som organisationen ger den enskilde att begränsa uppgifternas användning och utlämnande. Detta meddelande, som skall vara lättbegripligt och lättläst, skall lämnas vid det tillfälle då den enskilde för första gången ombeds lämna personuppgifter till en viss organisation eller så snart därefter det är praktiskt möjligt, men i alla händelser innan organisationen använder sådana uppgifter för ett annat ändamål än det för vilket de ursprungligen insamlades eller behandlades av den organisation som överför uppgifterna eller lämnar ut dem till tredje part för första gången [1].

VALMÖJLIGHET

En organisation skall ge den enskilde möjlighet att välja (opt out) om hans eller hennes personuppgifter skall a) lämnas till tredje part [1] eller b) användas till ett ändamål som inte stämmer överens med det syfte/de syften för vilka de ursprungligen insamlades eller den enskilde i efterhand har gett sitt tillstånd till. Enskilda måste på ett tydligt och lättillgängligt sätt ges möjlighet att till en rimlig kostnad utöva denna valmöjlighet.

För känsliga uppgifter (dvs. personuppgifter som rör medicinska förhållanden och hälsa, ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller uppgifter rörande sexualliv) skall den enskilde ges möjlighet att genom att bekräfta eller göra ett uttryckligt val (opt in) ange om uppgifterna får lämnas ut till en tredje part eller användas för ett annat ändamål än det för vilket de ursprungligen samlades in eller den enskilde i efterhand har gett sitt tillstånd till genom att välja (opt in). Om en tredje part anser att uppgifter är känsliga och behandlar dem därefter skall en organisation som mottagit dessa alltid behandla dem som känsliga.

VIDARE ÖVERFÖRING

För att få lämna uppgifter till en tredje part, måste organisationer tillämpa principerna om meddelande och valmöjlighet. Om en organisation vill överföra uppgifter till en tredje part som enligt beskrivningen i fotnoten agerar som förmedlare kan organisationen göra detta, om den först förvissar sig om att tredje part ansluter sig till principerna eller omfattas av direktivet eller på annat sätt garanterar en adekvat skyddsnivå eller om den ingår ett skriftligt avtal med denna tredje part om att denne skall tillhandahålla minst samma integritetsskyddsnivå som krävs i principerna. Om organisationen uppfyller dessa krav skall den inte ställas till svars (om organisationen inte själv godtar annat) för fall då en tredje part som organisationen överför uppgifter till behandlar uppgifterna på något sätt som strider mot gällande begränsningar eller villkor, såvida inte organisationen kände till eller borde känt till att tredje part behandlar uppgifterna på ett sätt som strider mot kraven och organisationen inte vidtagit rimliga åtgärder för att förhindra eller stoppa sådan behandling.

[1] Att tillämpa principen om meddelande eller valmöjlighet är inte nödvändigt när uppgifter lämnas ut till en tredje part som agerar på organisationens vägnar och därvid utför uppgifter åt organisationen enligt dennas instruktioner. Principen om vidare överföring gäller dock för sådana utlämnanden.

SÄKERHET

Organisationer som skapar, lagrar, använder eller sprider personuppgifter skall vidta rimliga försiktighetsåtgärder för att se till att de inte går förlorade, missbrukas eller utan tillstånd tas fram, utlämnas, förvanskas eller förstörs.

DATAINTEGRITET

I enlighet med principerna måste personuppgifterna vara relevanta för det ändamål för vilket de skall användas. En organisation får inte behandla personuppgifter på ett sätt som är oförenligt med det ändamål för vilket de samlades in om inte den enskilde i efterhand har gett sitt tillstånd. I den omfattning som krävs för dessa ändamål skall en organisation vidta nödvändiga åtgärder för att se till att uppgifterna är tillförlitliga för det avsedda ändamålet samt riktiga, fullständiga och aktuella.

TILLGÅNG

Enskilda skall ha tillgång till de personuppgifter om dem själva som en organisation innehar och skall ha möjlighet att rätta, ändra eller utplåna dessa uppgifter då de är felaktiga, utom då arbetet eller kostnaden för denna tillgång inte står i proportion till risken för den enskildes personliga integritet i ärendet i fråga eller då en annan persons legitima rättigheter skulle kränkas.

GENOMFÖRANDE OCH UPPFÖLJNING

Ett effektivt skydd av den personliga integriteten måste innefatta mekanismer för att se till att principerna följs, att de enskilda som uppgifterna rör och som drabbats av att principerna inte följts kan vidta rättsliga åtgärder samt att det blir påföljder för den organisation som inte följer principerna. Dessa mekanismer skall minst omfatta följande: a) Enkelt tillgängliga och billiga oberoende rättsmedel genom vilka varje enskilds klagomål och tvister kan handläggas och lösas genom hänvisning till principerna samt skadestånd tilldelas då tillämpliga lagar eller initiativ inom den privata sektorn så föreskriver. b) Uppföljningsförfaranden för att kontrollera att företagens intyg och försäkringar i fråga om deras förfaranden för integritetsskydd är sanna och att förfaranden för integritetsskydd har genomförts såsom angivits. c) Skyldighet att åtgärda problem som uppstår till följd av att principerna inte har efterlevts i de organisationer som har tillkännagivit att de följer dem samt påföljder för dessa organisationer. Påföljderna skall vara tillräckligt stränga för att garantera att organisationerna följer principerna.

Bilaga

Förteckning över tillsynsmyndigheter i Förenta staterna vilka erkänts av Europeiska unionen

Europeiska unionen erkänner följande statliga myndigheter i Förenta staterna såsom behöriga att handlägga klagomål och ge upprättelse i samband med illojala eller bedrägliga behandlingar och att utverka skadestånd för enskilda om *safe harbor*-principerna, tillämpade i överensstämmelse med FoS, inte följs:

— Federal Trade Commission (den federala konkurrensmyndigheten) på grundval av dess behörighet enligt avsnitt 5 i Federal Trade Commission Act

— Department of Transportation (transportministeriet) på grundval av dess behörighet enligt kapitel 49 i United States Code Section 41712.

BILAGA II

FRÅGOR OCH SVAR (FoS)

FoS 1 – Känsliga uppgifter

F: *Måste en organisation alltid erbjuda en uttrycklig valmöjlighet (ställningstagande för) när det rör sig om känsliga uppgifter?*

S: Nej, en sådan valmöjlighet krävs inte när behandlingen 1) är av avgörande betydelse för den registrerade eller annan person, 2) är nödvändig för fastställande av rättsliga yrkanden eller rättsligt försvar, 3) är nödvändig för medicinsk behandling eller diagnos, 4) företas inom ramen för laglig verksamhet som utövas av en stiftelse, förening eller annat organ vars verksamhet inte bedrivs i vinstsyfte och vars ändamål är politiskt, filosofiskt, religiöst eller fackligt, på villkor att databehandlingen endast hänför sig till organisationens medlemmar eller till personer som har regelbunden kontakt med den inom ramen för dess ändamål och att uppgifterna inte lämnas ut till tredje part utan de registrerades samtycke, 5) är nödvändig för att en organisation skall kunna fullgöra sina förpliktelser på arbetslagstiftningens område, eller 6) gäller uppgifter som uttryckligen offentliggörs av den enskilde.

FoS 2 – Journalistiska undantag

F: *Gäller* safe harbor*-principerna, mot bakgrund av att tryckfriheten är inskriven i Förenta staternas konstitution och att direktivet gör undantag för journalistiskt material, även sådana personuppgifter som insamlas, lagras eller sprids för journalistiska ändamål?*

S: När den tryckfrihet som är fastlagd i det första tillägget till Förenta staternas konstitution råkar i konflikt med rätten till skydd för den personliga integriteten, skall första tillägget styra hur avvägningen mellan dessa intressen skall göras när det gäller medborgare eller företag i Förenta staterna. Personuppgifter som samlas in för publicering, radio- och TV-sändningar eller andra former av offentliggörande av journalistisk stoff, vare sig det används eller inte, samt uppgifter som återfinns i tidigare offentliggjort stoff som sprids från mediers arkiv omfattas inte av kraven enligt *safe harbor*-principerna.

FoS 3 – Sekundärt ansvar

F: *Är Internetleverantörer, teleföretag eller andra organisationer ansvariga enligt* safe harbor*-principerna när de på en annan organisations vägnar endast överför, dirigerar, växlar eller cachar uppgifter som strider mot bestämmelserna enligt dessa principer?*

S: Nej, i likhet med direktivet skapar *safe harbor*-principerna inte något sekundärt ansvar. När en organisation endast kanaliserar uppgifter som överförts av tredje man och inte bestämmer ändamålet eller sättet för behandlingen av personuppgifterna, är den inte ansvarig.

FoS 4 – Investeringsbanker och revisorer

F: *Den verksamhet som bedrivs av revisorer och investeringsbanker kan medföra att personuppgifter behandlas utan den enskildes samtycke eller vetskap. Under vilka omständigheter är detta tillåtet enligt principerna om meddelande, valmöjlighet och tillgång?*

S: Investeringsbanker och revisorer får utan den enskildes vetskap behandla uppgifter endast i den omfattning och under den tid som det är nödvändigt för att lagstadgade krav skall kunna uppfyllas eller det allmänna intresset tillgodoses, och under andra förhållanden där en tillämpning av dessa principer skulle skada organisationens rättmätiga intressen. Sådana rättmätiga intressen är övervakningen av att ett företag uppfyller sina lagstadgade förpliktelser och sin redovisningsskyldighet, liksom behovet av sekretess i samband med eventuella förvärv, fusioner, samriskföretag eller andra liknande arrangemang som genomförs av investeringsbanker eller revisorer.

FoS 5 [1] **– Dataskyddsmyndigheternas roll**

F: *På vilket sätt skall förteag som förpliktar sig att samarbeta med dataskyddsmyndigheterna i EU göra dessa åtaganden och hur skall de fullgöras?*

S: Enligt *safe harbor*-principerna skall organisationer i USA som tar emot personuppgifter från EU förbinda sig att på lämpligt sätt sörja för att *safe harbor*-principerna efterlevs. De skall – enligt principen om genomförande och uppföljning (enforcement) – a) tillhandahålla möjlighet för de personer som uppgifterna berör att få sin sak prövad, b) tillhandahålla uppföljningsrutiner för att kontrollera att de försäkringar de gjort om sina integritetsskyddsrutiner är sanningsenliga och c) förplikta sig att lösa problem som beror på att principerna inte följs och ta konsekvenserna i form av påföljder i förekommande fall. En organisation kan uppfylla förpliktelserna enligt a och c i principen om genomförande och uppföljning om den iakttar kraven enligt föreliggande FoS om samarbete med dataskyddsmyndigheterna.

En organisation kan förplikta sig att samarbeta med dataskyddsmyndigheterna genom att i sin skrivelse om självcertifiering till Förenta staternas handelsministerium (se FoS 6 om självcertifiering) förklara att den

1. väljer att uppfylla de krav som anges i punkt a och c i *safe harbor*-principen om genomförande och uppföljning genom att förbinda sig att samarbeta med dataskyddsmyndigheterna,

2. kommer att samarbeta med dataskyddsmyndigheterna vid handläggning av klagomål som inges inom ramen för *safe harbor,* och

3. kommer att rätta sig efter dataskyddsmyndigheternas rekommendationer om dessa finner att organisationen måste vidta särskilda åtgärder för att den skall anses följa *safe harbor*-principerna; detta omfattar korrigerande åtgärder och gottgörelse till enskilda som drabbats av att principerna inte följs, och att den skriftligen till dataskyddsmyndigheterna kommer att bekräfta att sådana åtgärder har vidtagits.

Dataskyddsmyndigheternas samarbete sker i form av information och rekommendationer på följande sätt:

— Dataskyddsmyndigheternas rekommendationer avges via en informell särskild arbetsgrupp, bestående av dataskyddsmyndigheter inrättad på europeisk nivå. Denna arbetsgrupp skall bl.a. hjälpa till med att se till att ett enhetligt och konsekvent tillvägagångssätt tillämpas.

— Arbetsgruppen skall avge rekommendationer till berörda amerikanska organisationer om olösta klagomål från enskilda rörande hanteringen av personuppgifter som har överförts från EU inom ramen för *safe harbor*. Dessa rekommendationer skall vara utformade på ett sätt som säkerställer att *safe harbor*-principerna tillämpas korrekt och skall innehålla uppgifter om den gottgörelse till den enskilde som dataskyddsmyndigheterna anser är lämplig.

— Arbetsgruppen skall avge sådana rekommendationer i ärenden som hänskjutits till den av berörda organisationer och/eller som svar på klagomål som inkommer direkt från enskilda och rör organisationer som har förbundit sig att samarbeta med dataskyddsmyndigheterna i samband med *safe harbor*. Gruppen skall uppmuntra och vid behov hjälpa enskilda att först och främst använda de interna förfarande för handläggning av klagomål som organisationen erbjuder.

— Rekommendationer kommer först att avges efter det att båda parter i en tvist har givits en rimlig möjlighet att inkomma med synpunkter och förete eventuella bevis. Arbetsgruppen skall avge sina rekommendationer så snabbt som möjligt inom ramen för korrekt handläggning av ärendet. Normalt gäller att gruppen skall ha som målsättning att avge sina rekommendationer inom 60 dagar efter det att den mottagit ett klagomål eller ett ärende hänskjutits för handläggning, och om möjligt ännu snabbare.

— Arbetsgruppen kommer att offentliggöra hur den handlagt klagomål som inkommit, om den anser att detta är lämpligt.

— Arbetsgruppens rekommendationer innebär inga åligganden vare sig för arbetsgruppen själv eller för enskilda dataskyddsmyndigheter.

---

[1] Huruvida denna FoS kommer att ingå i paketet är beroende av överenskommelsen med dataskyddsmyndigheterna. Föreliggande text har diskuterats av myndigheterna inom ramen för artikel 29-gruppen och majoriteten anser att texten kan godkännas. De är emellertid bara beredda att ta ställning slutgiltigt mot bakgrund av det övergripande yttrandet, som arbetsgruppen skall avge om slutpaketet.

Organisationer som väljer detta alternativ för tvistlösning måste i enlighet med ovanstående förbinda sig att följa dataskyddsmyndigheternas rekommendationer. Om en organisation inte följer dessa rekommendationer inom 25 dagar efter det att rekommendationerna avgivits och inte har någon tillfredsställande förklaring till förseningen, skall arbetsgruppen underrätta organisationen om sin avsikt att hänskjuta ärendet till antingen den amerikanska federala konkurrensmyndigheten (Fedral Trade Commission) eller annan/annat federal myndighet/offentligt organ i Förenta staterna som har lagstadgad behörighet att vidta tvingande åtgärder mot bedrägliga metoder och missvisande information eller som kan fastställa att en allvarlig överträdelse har skett av samarbetsavtalet, som därmed skall anses ogiltigt. I det senare fallet skall den särskilda arbetsgruppen underrätta handelsministeriet (eller dess utsedda företrädare) så att förteckningen över de organisationer som omfattas av *safe harbor* kan ändras på motsvarande sätt. Underlåtenhet att fullgöra förpliktelsen att samarbeta med dataskyddsmyndigheterna kan liksom underlåtenhet att följa *safe harbor*-principerna leda till att åtal väcks för bedrägligt beteende enligt avdelning 5 i den amerikanska lagen om osann utsaga (False Statements Act) eller liknande regelverk.

Organisationer som väljer detta alternativ påförs en årsavgift som är avsedd att täcka kostnaderna för den särskilda arbetsgruppens verksamhet. Dessutom kan organisationerna påföras de eventuella översättningskostnader som uppstår under arbetsgruppens behandling av klagomål eller ärenden som hänskjutits till den. Årsavgiften skall uppgå till högst 500 US-dollar och vara lägre för mindre företag.

Alternativet att samarbeta med dataskyddsmyndigheterna kommer att stå öppet för organisationer som ansluter sig till *safe harbor* under en treårsperiod. Dataskyddsmyndigheterna kan ompröva detta innan denna tidsperiod löper ut, om det skulle visa sig att antalet amerikanska organisationer som väljer detta alternativ blir alltför omfattande.

FoS 6 – Självcertifiering

F: *Hur sker en organisations självcertifiering efter det att den har anslutit sig till* safe harbor-*principerna?*

S: En organisation omfattas av de fördelar som *safe harbor* medför från den dag då organisationen till handelsministeriet (eller dess utsedda företrädare) anmäler att den har anslutit sig till principerna genom självcertifiering i enlighet med de riktlinjer som anges nedan.

Organisationer som vill ansluta sig till *safe harbor* genom självcertifiering kan till handelsministeriet (eller dess utsedda företrädare) sända en skrivelse, som skall vara undertecknad av en person i ansvarig ställning på den organisations vägnar som ansluter sig till *safe harbor*. Denna skrivelse skall innehålla åtminstone följande uppgifter:

1. Organisationens namn, postadress, e-postadress, telefon- och faxnummer.

2. En beskrivning av den del av organisationens verksamhet som rör personuppgifter som tas emot från EU.

3. En beskrivning av organisationens integritetsskyddspolicy för sådana personuppgifter, vilket skall omfatta a) uppgift om hur allmänheten kan ta del av den, b) det datum den trädde i kraft, c) en kontaktpunkt för handläggningen av klagomål, ansökningar om åtkomst och andra frågor som kan uppstå inom ramen för *safe harbor*, d) den tillsynsmyndighet som är behörig att behandla klagomål som rör organisationen och gäller eventuell förekomst av illojala eller bedrägliga metoder och brott mot gällande lagstiftning om integritetsskydd (och som förtecknas i bilagan till principerna), e) namn på eventuella program för integritetsskydd som organisationen deltar i, f) kontrollmetod (t.ex. intern eller genom tredje man) [2] och g) förfarande vid oberoende instans som kan handlägga olösta klagomål.

Om organisationen vill att de fördelar som *safe harbor* innebär skall omfatta personaluppgifter som överförs från EU för att användas inom ramen för anställningsförhållandet, kan detta tillåtas om det finns en tillsynsmyndighet som är behörig att behandla klagomål som för organisationen och gäller sådana personaluppgifter som förtecknas i bilagan till principerna. Dessutom skall organisationen i sin självcertifiering ange att den vill att sådana personaluppgifter skall omfattas, att den förbinder sig att samarbeta med myndigheterna i EU i enlighet med FoS 9 och 5, beroende på vilken som är tillämplig, samt att den kommer att följa dessa myndigheters rekommendationer.

Handelsministeriet (eller dess utsedda företrädare) skall hålla en förteckning över alla organisationer som insänder sådana skrivelser, varigenom fördelarna med *safe harbor* garanteras. Förteckningen skall uppdateras i överensstämmelse med de skrivelser om självcertifiering som inkommer varje år och de anmälningar som erhålls i enlighet med FoS 11. Sådana skrivelser om självcertifiering skall insändas minst en gång om året. I annat fall stryks organisatio-

[2] Se FoS 7 om kontroll.

nen från förteckningen och de fördelar som *safe harbor* innebär kan inte längre åberopas. Såväl förteckningen som de skrivelser om självcertifiering som organisationer sänder in skall vara offentliga. Alla organisationer som väljer självcertifiering skall även i den ifrågavarande offentliga redogörelsen för den egna integritetsskyddspolicyn som är tillämplig förklara att de följer *safe harbor*-principerna.

Åtagandet att följa *safe harbor*-principerna gäller utan tidsbegränsning för de uppgifter som organisationen mottagit under den tid som organisationen åtnjuter fördelarna med *safe harbor*. Åtagandet innebår att organisationen kommer att fortsätta att tillämpa principerna på dessa uppgifter under hela den tid som organisationen lagrar, behandlar eller lämnar ut uppgifterna, även om organisationen av någon anledning lämnar *safe harbor*.

En organisation som till följd av fusion eller uppköp kommer att upphöra som separat juridisk person skall anmäla detta i förväg till handelsministeriet (eller dess utsedda företrädare). I denna anmälan skall det även anges om den förvärvande enheten eller den enhet som uppstår genom fusionen 1) kommer att fortsätta att vara bunden av *safe harbor*-principerna enligt den lagstiftning som styr uppköpet eller fusionen, eller 2) väljer självcertifiering för anslutning till *safe harbor*-principerna eller inför andra garantier, t.ex. ett skriftligt avtal som säkrar anslutningen till *safe harbor*-principerna. Om varken alternativ 1 eller 2 är tillämpligt skall samtliga uppgifter som erhållits inom ramen för *safe harbor* omedelbart raderas.

En organisation behöver inte tillämpa *safe harbor*-principerna på alla personuppgifter, men den måste tillämpa *safe harbor*-principerna på alla personuppgifter som den tar emot från EU efter det att den anslutit sig till *safe harbor*.

Vid missvisande information till allmänheten om en organisations anslutning till *safe harbor* kan den federala konkurrensmyndigheten (Federal Trade Commission) eller annan federal instans väcka åtal. Missvisande information till handelsministeriet (eller dess utsedda företrädare), kan leda till åtal i enlighet med den amerikanska lagen om osann utsaga (False Statements Act, 18USC § 1001).

FoS 7 – Kontroll

F: *Vilka uppföljningsförfaranden tillämpar orgnisationer för att kontrollera att de försäkringar de gjort om sina integritetsskyddsrutiner inom ramen för safe harbor är sanningsenliga och att dessa integritetsskyddsrutiner tillämpas enligt vad som framförts och i överensstämmelse med* safe harbor*-principerna*

S: För att kraven på kontroll enligt genomförfarandeprincipen skall uppfyllas kan en organisation kontrollera sådana försäkringar antingen genom egenkontroll eller externa granskningar.

Om man väljer en sådan egenkontroll måste förfarandet visa att organisationens offentliggjorda integritetsskyddspolicy avseende personuppgifter som erhålls från EU är korrekt, heltäckande och offentliggjord på ett tydligt sätt, att den tillämpas fullt ut och att den är tillgänglig för insyn. Organisationen måste också visa att dess integritetsskyddspolicy stämmer överens med *safe harbor*-principerna; att konsumenten känner till de mekanismer som finns för att behandla klagomål från konsumenter; att det finns förfaranden för utbildning av personal av tillämpning av denna policy och att man vidtar disciplinära åtgärder om policyn inte följs; samt att organisationen har interna förfaranden att genomföra återkommande objektiva granskningar för att kontrollera att ovanstående efterlevs. En rapport om egenkontrollen skall undertecknas av en person i ansvarig ställning eller en annan behörig representant vid företaget minst en gång om året och göras tillgänglig på konsumentens begäran eller inom ramen för en undersökning eller ett klagomål över att bestämmelserna inte efterlevts.

Organisationerna skall dokumentera sina integritetsskyddsrutiner inom ramen för *safe harbor* och på begäran göra dessa dokumentationer tillgängliga (i samband med en undersökning eller klagomål över att bestämmelserna inte följs) för det oberoende organ som svarar för handläggning av klagomål eller till den myndighet som har ansvar för frågor om illojala metoder och bedrägligt beteende.

Om organisationerna väljer en extern granskning, skall en sådan granskning visa att organisationens integritetsskyddspolicy avseende personuppgifter som erhålls från EU överensstämmer med *safe harbor*-principerna och att den tillämpas. Metoderna för granskning kan utan begränsning omfatta revision, slumpmässiga kontroller, användandet av ”lockbeten”, eller i tillämpliga fall användandet av tekniska verktyg. En rapport om att en extern granskning har genomförts skall undertecknas av granskaren eller av en person i ansvarig ställning eller en annan behörig

representant vid företaget. Detta skall ske minst en gång om året och rapporten skall göras tillgänglig på begäran av konsumenterna eller inom ramen för ett överklagande.

FoS 8 – Tillgång

Principen om tillgång:

Enskilda skall ha tillgång till de personuppgifter om dem själva som en organisation innehar och skall ha möjlighet att rätta, ändra eller utplåna dessa uppgifter då de är felaktiga, utom då arbetet eller kostnaden för denna tillgång inte står i proportion till risken för den enskildes personliga integritet i ärendet i fråga eller då en annan persons legitima rättigheter skulle kränkas.

F1: *Är rätten till tillgång oinskränkt?*

S: Nej, enligt *safe harbor*-principerna är rätten till tillgång grundläggande för integritetsskyddet. I synnerhet medger den enskilda att kontrollera om de uppgifter som finns om dem är korrekta. En organisations skyldighet att göra uppgifter den har om en enskild person tillgängliga är dock underordnad principen om proportionalitet eller rimlighet och måste modifieras i vissa fall. Faktum är att i motiveringen till OECD:s riktlinjer för integritetsskydd från 1980 framgår tydligt att denna skyldighet inte är oinskränkt. Det krävs ingen utomordentligt grundlig sökning till exempel till följd av en stämning. Inte heller finns det något krav på att tillgängligheten gäller alla olika former i vilka uppgifterna kan finnas hos organisationen.

Erfarenheten visar snarare att då man tillmötesgår enskildas förfrågan om tillgång bör organisationerna först låta sig ledas av bakgrunden till förfrågningen. Till exempel om en förfrågan om tillgång är vagt formulerad eller väldigt omfattande kan en organisation inleda en dialog med den enskilde för att ta reda på varför förfrågan gjorts och för att lättare kunna hitta lämpliga uppgifter. Organisationen kan ta reda på vilken del eller vilka delar av organisationen den enskilde hade kontakt med och/eller vilka slags uppgifter (eller vilket användningsområde) som ligger till grund för förfrågan. Enskilda behöver dock inte motivera sin förfrågan om att få ta del av uppgifter om sig själva.

Kostnader och arbetsinsats är viktiga faktorer som man bör ta hänsyn till, men de avgör inte huruvida det är rimligt att bevilja tillgång till uppgifter. Om uppgifterna till exempel används för att fatta beslut som är av stor betydelse för den enskilde (t.ex. i samband med avslag eller beviljande av viktiga förmåner, som försäkring, lån eller arbete), måste organisationen i överensstämmelse med övriga bestämmelser i dessa FoS lämna ut uppgifter även om detta är svårt eller innebär höga kostnader.

Om det inte rör sig om känsliga uppgifter eller om dessa inte används för att fatta beslut som är av stor betydelse för den enskilde (t.ex. uppgifter om affärsverksamhet som inte är känsliga och som används för att avgöra om man skall skicka en katalog till den enskilde), men är lättillgängliga och det inte innebär några stora kostnader att få fram dessa, måste organisationen göra dessa uppgifter som finns hos organisationen tillgängliga. Dessa uppgifter kan innehålla fakta som man fått av den enskilde och som samlats in i samband med en affär, eller som härrör från andra personer och som gäller den enskilde.

I överensstämmelse med själva principen bakom tillgång bör organisationerna alltid visa sin goda vilja när det gäller att ge tillgång till uppgifter. Om t.ex. vissa uppgifter behöver skyddas och lätt kan skiljas från övriga uppgifter som det begärs tillgång till skall organisationen bearbeta de skyddade uppgifterna och göra de icke-konfidentiella uppgifterna tillgängliga. Om en organisation beslutar att i vissa fall vägra ge tillgång till uppgifter, skall organisationen lämna en förklaring till den enskilde som ansökt om att få tillgång till uppgifterna om varför man kommit fram till detta beslut och ange en kontaktpunkt för ytterliga frågor.

F2: *Vad är konfidentiella uppgifter om affärsverksamhet och får organisationer neka tillgång i syfte att skydda dessa uppgifter?*

S: Konfidentiella uppgifter om affärsverksamhet (som detta uttryck används i Federal Rules of Civil Procedure on discovery) är uppgifter som en organisation har vidtagit åtgärder för att skydda från insyn och där insynen skulle vara till fördel för en konkurrent på marknaden. Det särskilda datorprogram som en organisation använder, t.ex. modelleringsprogram, eller delar av ett sådant program kan vara konfidentiella uppgifter om affärsverksamhet. I fall då vissa konfidentiella uppgifter om affärsverksamhet lätt kan skiljas från övriga uppgifter som det begärs till-

gång till skall organisationen bearbeta de konfidentiella uppgifterna om affärsverksamhet och göra de icke-konfidentiella uppgifterna tillgängliga. Organisationer kan neka eller begränsa tillgång om det skulle innebära att man genom att göra uppgifterna tillgängliga avslöjar organisationens egna konfidentiella uppgifter om affärsverksamhet, såsom dessa definieras ovan, t.ex. slutsatser eller klassificeringar av marknadsföring som utarbetas av organisationen, eller en annan organisations konfidentiella uppgifter om affärsverksamhet där dessa uppgifter omfattas av ett avtalsreglerat sekretesskrav, under sådana omständigheter där sekretess normalt skulle krävas eller utlovas.

F3: *Kan en organisation, när den ger tillgång till uppgifter, lämna personuppgifterna till den enskilde från organisationens databaser eller gäller tillgången själva databaserna?*

S: Tillgången kan ges genom att en organisation lämnar ut uppgifterna till den enskilde och det är inte nödvändigt att den enskilde får tillgång till organisationens databas.

F4: *Måste en organisation omstrukturera sina databaser för att göra dessa tillgängliga?*

S: Tillgång behöver bara medges i den mån en organisation lagrar uppgifterna. Tillgångsprincipen innebär inte att organisationerna är skyldiga att hålla kvar, upprätthålla, omorganisera eller omstrukturera register med personuppgifter.

F5: *Dessa svar klargör att tillgång kan nekas i vissa fall. Vilka andra omständigheter skall föreligga för att organisationerna inte skall behöva ge enskilda tillgång till personuppgifter som organisationerna har?*

S: Sådana omständigheter är begränsade och alla skäl för att neka tillgång måste tydligt anges. En organisation kan vägra tillgång till uppgifter om utlämnandet troligtvis kan försvåra skyddet av viktiga offentliga intressen, som nationell säkerhet, försvar eller allmän säkerhet. Dessutom kan tillgång nekas i fall då personuppgifterna uteslutande behandlas för att användas i forskning eller statistik. Andra skäl att neka eller begränsa tillgången till uppgifter kan vara att det annars kan:

a) Försvåra brottsbekämpning, inklusive förebyggande, utredning eller upptäckt av brottsliga handlingar eller rätten till en rättvis rättegång.

b) Försvåra i civilmål, inklusive förebyggande eller utredningar vid rättsliga tvister eller rätten till en rättvis rättegång.

c) Innebära utlämnande av personuppgifter som innehåller hänvisningar till andra enskilda personer i fall där dessa hänvisningar inte kan redigeras bort.

d) Innebära brott mot rättsliga eller yrkesmässiga privilegier eller skyldigheter.

e) Medföra brott mot nödvändig sekretess i samband med framtida eller pågående förhandlingar, t.ex. rörande förvärv av börsnoterade företag.

f) Försvåra säkerhetskontroller som gäller anställda eller klagomålsförfaranden.

g) Skada den konfidentialitet som kan vara nödvändig under begränsade perioder i samband med turordning när det gäller personplanering och omstrukturering av bolag, eller

h) skada den konfidentialitet som kan vara nödvändig i samband med övervakning, inspektion eller reglerande funktioner som tillhör en sund ekonomisk eller finansiell förvaltning, eller

i) under andra omständigheter, innebära att kostnaderna för att ge denna tillgång skulle bli oproportionerliga eller att andra personers legitima rättigheter eller intressen skulle kränkas.

Det åligger den organisation som åberopar rätten att göra undantag att bevisa att denna är tillämplig (såsom normalt är fallet). Enligt vad som framhållits ovan skall en motivering till att organisationer nekar eller begränsar tillgången till uppgifter samt information om en kontaktpunkt för ytterligare undersökningar lämnas till den enskilde.

F6: *Kan en organisation ta ut en avgift för att täcka kostnaderna i samband med att den ger tillgång till uppgifter?*

S: Ja, enligt OECD:s riktlinjer kan organisationer ta ut en avgift, förutsatt att denna inte är orimligt hög. Följaktligen kan organisationer ta ut en rimlig avgift för att göra uppgifter tillgängliga. Att ta ut en avgift kan vara meningsfullt om man vill förhindra ständigt återkommande okynnesförfrågningar.

Organisationen som bedriver verksamhet med att sälja offentliga uppgifter kan ta ut en avgift från organisationer i samband med en förfrågan om tillgång. Enskilda personer kan också få tillgång till uppgifter om sig själva från den organisation som ursprungligen samlade in dessa.

Tillgång får inte förvägras av kostnadsskäl om den enskilde erbjuder sig att stå för kostnaderna.

F7: *Är en organisation skyldig att ge tillgång till personuppgifter som härrör ur offentliga register?*

S: Offentliga register hålls av myndigheter och enheter på olika nivåer och är tillgängliga för allmänheten. Det är inte nödvändigt att tillämpa principen om tillgång eller vidare överföring på sådana uppgifter så länge dessa inte kombineras med andra personuppgifter, med undantag av de fall då ett ringa antal icke-officiella registeruppgifter används för indexering eller organisering av offentliga registeruppgifter. Om det finns villkor för användning av ett register vilka fastställts av behöriga myndigheter skall dessa dock alltid gälla. Om offentliga registeruppgifter kombineras med andra icke-offentliga registeruppgifter (andra än de som särskilt framhållits ovan), måste en organisation emellertid ge tillgång till alla sådana uppgifter om dessa inte omfattas av andra legitima undantag.

F8: *Måste tillgångsprincipen tillämpas om det rör sig om offentligt tillgängliga personuppgifter?*

S: På samma sätt som med uppgifter från offentliga register (se fråga 7) är det inte nödvändigt att ge tillgång till uppgifter som redan finns tillgängliga för den stora allmänheten så länge dessa inte kombinerats med icke-offentliga uppgifter.

F9: *Hur kan en organisation skydda sig mot återkommande och besvärande krav på tillgång?*

S: En organisation behöver inte tillmötesgå sådana krav på tillgång. Av dessa skäl kan organisationerna ta ut en rimlig avgift och fastställa rimliga begränsningar vad gäller antalet förfrågningar från en viss person vilka behöver besvaras under en viss period. När dessa begränsningar fastställs skall man ta hänsyn till hur ofta uppgifterna uppdateras, i vilket syfte de används och vilka slags uppgifter det rör sig om.

F10: *Hur kan en organisation skydda sig själv mot bedrägliga förfrågningar om tillgång till uppgifter?*

S: En organisation är inte skyldig att ge tillgång till uppgifter om den inte erhåller tillräcklig information för att bekräfta identiteten på den person som ansöker om att få tillgång till uppgifterna.

F11: *Finns det en period inom vilken svaret på förfrågan om tillgång måste lämnas?*

S: Ja, organisationerna skall svara utan onödigt dröjsmål och inom en rimlig tidsperiod. Detta krav kan bemötas på olika sätt, vilket fastställs i OECD:s riktlinjer för integritetsskydd från 1980. Till exempel kan en registeransvarig som tillhandahåller upgifter om berörda personer vid regelbundna tillfällen undantas från skyldigheten att omedelbart lämna svar på den enskildas förfrågan.

FoS 9 – Personaluppgifter

F1: *Omfattas personuppgifter som insamlas inom ramen för ett anställningsförhållande av* safe harbor *då de överförs från EU till USA?*

S: Ja, om ett företag i EU överför personuppgifter som insamlats om de anställda (tidigare eller nuvarande) inom ramen för ett anställningsförhållande till ett moderbolag, en filial eller en oberoende tjänsteleverantör i USA anslu-

ten till *safe harbor*, har överföringen de fördelar som *safe harbor* innebär. I sådana fall omfattas insamlandet av uppgiferna liksom behandlingen av dessa innan de överförs av lagstiftningen i det EU-land där de samlades in, och om dessa lagar föreskriver villkor eller begränsningar för överföringen måsta sådana bestämmelser följas.

Safe harbor-principerna är relevanta endast om enskilt identifierbara register överförs eller görs tillgängliga. Statistikrapportering som bygger på sammanförda sysselsättningsuppgifter och/eller användandet av uppgifter som avidentifierats eller på annat sätt gjorts omöjliga att identifiera innebär inte något problem för integritetsskyddet.

F2: *Hur tillämpas principerna för meddelande och valmöjlighet på sådana uppgifter?*

S: En organisation i USA som har fått uppgifter om anställda från EU inom ramen för *safe harbor* får utlämna dessa uppgifter till en tredje part och/eller använda dem för andra ändamål endast i enlighet med principerna om meddelande och valmöjlighet. När en organisation t.ex. har för avsikt att använda personuppgifter som samlats in i samband med ett anställningsförhållande för marknadskommunikation, måste organisationerna i USA ge de berörda enskilda en valmöjlighet innan den använder uppgifterna, såvida dessa inte redan tidigare har gett sitt samtycke till att uppgifterna används för dessa ändamål. Att en person utnyttjar denna valmöjlighet får inte användas för att begränsa karriärmöjligheter eller för att bestraffa den anställde på något sätt.

Det bör påpekas att vissa allmänt tillämpliga villkor för överföring från en del medlemsstater kan utesluta annan användning av sådana uppgifter även efter det att uppgifterna har överförts till ett land utanför EU och att sådana villkor är bindande.

Att en person utnyttjar denna valmöjlighet får inte användas för att begränsa karriärmöjligheter eller för att bestraffa den anställde på något sätt.

Dessutom skall arbetsgivare göra rimliga ansträngningar för att tillmötesgå den anställdes önskemål om integritetsskydd. Detta kan t.ex. inbegripa att man begränsar tillgången till uppgifterna, avidentifierar dem eller inför koder eller pseudonymer om det i förvaltningssyfte inte är nödvändigt att uppge de riktiga namnen. Om och när det är nödvändigt att undvika inblandning i organisationens personalpolitik, dvs. befordringar, tillsättande av tjänster eller liknande, behöver en organisation inte lämna någon valmöjlighet eller meddelande.

F3: *Hur tillämpas principen om tillgång på personaluppgifter?*

S: FoS om tillgänglighet ger en vägledning om vilka orsaker som kan berättiga att en organisation avvisar eller efter en begäran endast ger begränsad tillgång till personaluppgifter. Givetvis måste arbetsgivare i EU handla i enlighet med lokala bestämmelser och se till att anställda inom EU får tillgång till sådana uppgifter som är en lagstadgad rättighet i deras hemländer, oavsett var dessa uppgifter bearbetas eller lagras. Enligt *safe harbor* skall en organisation som behandlar sådana uppgifter i USA samarbeta för att ge tillgång till uppgifterna antingen direkt eller genom arbetsgivaren i EU.

F4: *Hur kommer genomförandet av integritetsskydd för anställda enligt* safe harbor*-principerna att behandlas?*

S: I den mån uppgifterna endast används i samband med ett anställningsförhållande ligger ansvaret för uppgifterna gentemot den anställde hos företaget i EU. Därmed bör i fall då anställda i EU klagar på att deras rättigheter när det gäller uppgiftsskydd har kränkts och de inte är nöjda med resultatet av förfaranden för intern granskning, klagomål eller överklagande (eller något annat förfarande som avtalats med en fackförening) vända sig direkt till den nationella myndigheten för uppgiftsskydd eller myndigheten med ansvar för arbetsförhållanden inom det område där den berörda personen är anställd. Detta omfattar även fall då den påstådda felhanteringen av uppgifterna har ägt rum i USA och det är den organisation i USA som mottagit uppgifterna från arbetsgivaren och inte arbetsgivaren själv som påstås ha gjort sig skyldig till en felhantering, varvid den snarare innebär ett brott mot *safe harbor* principerna än ett brott mot den nationella lagstiftning genom vilken direktivet genomförs. Detta är det mest effektiva tillvägagångssättet för att hantera ofta förekommande överlappning av rättigheter och skyldigheter som införts genom lokal arbetsrätt, arbetsmarknadsavtal och lagar om uppgiftsskydd.

En organisation i USA som är ansluten till *safe harbor* och som använder personaluppgifter om EU-medborgare som överförts från EU i samband med anställningsförhållandet och därvid önskar att överföringen skall omfattas av *safe harbor*-avtalet måste därför samarbeta vid undersökningar som utförs av behöriga myndigheter i EU och följa dessa myndigheters anvisningar i de enskilda fallen. De dataskyddsmyndigheter som gått med på att sam-

arbeta på detta sätt skall underrätta Europeiska kommissionen och USA:s handelsministerium om detta. Om en organisation i USA som är ansluten till *safe harbor* önskar överföra personaluppgifter från en medlemsstat vars dataskyddsmyndighet inte gått med på att samarbeta på detta sätt, gäller bestämmelserna enligt FoS 5 ([3]).

FoS 10 – Artikel 17 – avtal

F: *Krävs det ett avtal, oavsett om den som behandlar uppgifterna är ansluten till* safe harbor *eller inte, när uppgifter överförs från EU till USA endast för behandling?*

S: Ja, registeransvariga i Europa måste alltid ingå ett avtal för överföring av uppgifter för behandling, oavsett om behandlingen görs inom eller utanför EU. Syftet med avtalet är att skydda den registeransvariges intressen, dvs. den person eller det organ som bestämmer i vilket syfte uppgifterna skall användas och hur de skall behandlas och som har fullt ansvar för uppgifterna gentemot berörda personer. I avtalet anges alltså detaljer om behandlingen som skall utföras och de åtgärder som är nödvändiga för att garantera att uppgifterna är skyddade.

En amerikansk organisation som är ansluten till *safe harbor* och mottar personuppgifter från EU endast för att behandla dessa behöver inte tillämpa principerna på dessa uppgifter, eftersom den registeransvarige i EU har ansvaret för dem inför den enskilde, i enlighet med relevanta EU-bestämmelser (som kan vara mycket strängare än motsvarande *safe harbor*-principer).

Eftersom ett adekvat skydd garanteras av alla som är anslutna till *safe harbor*, kan avtal endast för behandling av uppgifter slutas med organisationer som är anslutna till *safe harbor* utan att tillstånd behöver begäras i förväg (eller också beviljas sådant *safe harbor* utan att tillstånd behöver begäras i förväg (eller också beviljas sådant tillstånd automatisk av medlemsstaterna), till skillnad från avtal med mottagare som inte är anslutna till *safe harbor* eller inte på annat sätt garanterar ett adekvat skydd.

FoS 11 – Tvistlösning, genomförande och uppföljning

F: *Hur skall kraven på tvistlösning enligt principen om genomförande och uppföljning uppfyllas och hur skall en organisations upprepade underlåtenhet att följa principen hanteras?*

S: Principen om genomförande och uppföljning anger de krav som skall ställas på metoder för genomförande och uppföljning av *safe harbor*-principerna. Hur kraven som uppställs i principens punkt b skall uppfyllas framgår av FoS om kontroll (FoS 7). Denna FoS 11 behandlar punkterna a och c som både kräver oberoende instanser för behandling av klagomål. Dessa metoder kan ha olika former men de måste uppfylla kraven enligt principen om genomförande och uppföljning. En organisation kan uppfylla kraven på något av följande sätt: 1) Den kan följa ett program för integritetsskydd som utarbetats inom den privata sektorn och i vilket *safe harbor*-principerna inlemmats. I programmet skall det ingå effektiva metoder för kontroll av efterlevnaden av det slag som beskrivs i principen om genomförande och uppföljning. 2) Den kan förbinda sig att rätta sig efter beslut från lagstadgade tillsynsmyndigheter eller andra offentliga tillsynsorgan som handlägger individuella klagomål och tillhandahåller tvistlösning. 3) Den kan förbinda sig att samarbeta med dataskyddsmyndigheter inom Europeisk gemenskapen eller deras bemyndigade ombud. Denna förteckning är inte ämnad att vara uttömmande utan snarare belysande. Den privata sektorn kan utarbeta andra metoder för genomförande och uppföljning förutsatt att de uppfyller kraven enligt principen och FoS. Observera att villkoren som uppställs i principen om genomförande och uppföljning gäller utöver de krav som uppställs i punkt 3 i inledningen till principerna om att tvistlösningsmodeller skall tillhandahålla lösningar som kan verkställas enligt avsnitt 5 i lagen om en federal konkurrensmyndighet (Federal Trade Commission Act) eller liknande regelverk.

Rättsmedel.

Konsumenterna skall uppmuntras att först inge klagomål till den berörda organisationen innan de vänder sig till oberoende instanser för behandling av klagomål. Att en sådan instans kan anses vara oberoende kan visas på ett antal olika sätt, t.ex. genom öppenhet i fråga om dess sammansättning och finansiering eller genom styrkt erfarenhet. Enligt principen om genomförande och uppföljning skall de rättsmedel som enskilda utnyttja vara lättillgäng-

([3]) Tillvägagångssättet enligt FoS 5 är begränsat till tre år. Artikel 29-arbetsgruppen uppmanas att diskutera olika sätt att säkerställa att en bestående lösning kan uppnås för anställningsuppgifter.

liga och kunna utnyttjas till en rimlig kostnad. Organ för tvistlösning skall undersöka varje klagomål från enskilda som inte är klart ogrundat eller oseriöst. Detta är inget hinder för att den organisation som tillhandahåller rättsmedlet uppställer kriterier för vilka som kan tas upp till behandling; sådana kriterier skall dock vara klara och rimliga (t.ex. undanta klagomål som faller utanför programmets räckvidd eller som bör tas upp i ett annat sammanhang) och får inte leda till att uppdraget, nämligen att reda ut berättigade klagomål, försvåras. Organisationen som tillhandahåller rättsmedlet bör dessutom på ett lättillgängligt och uttömmande sätt informera de enskilda om förfarandet för tvistlösning när dessa lämnar in ett klagomål. Sådan information bör, i enlighet med *safe harbor*-principerna, innehålla en upplysning om vilka regler till skydd för privatlivet som tillämpas av organisationen som tillhandahåller rättsmedlet ([4]). De bör även samarbeta vid framtagandet av t.ex. standardformulär för besvär så att handläggningen av ärendena underlättas.

Gottgörelse och påföljder.

Gottgörelse som ett organ för tvistlösning beslutat om skall leda till att de negativa effekter som blivit följden av att reglerna inte efterlevts i görligaste mån rättas till av den ansvariga organisationen och att all behandling av personuppgifter i framtiden sker i överensstämmelse med principerna samt, i tillämpliga fall, att all behandling av personuppgifter om den person som inlämnat klagomålet kommer att upphöra. Påföljderna måste vara tillräckligt kännbara för att borga för att organisationen kommer att följa principerna i framtiden. Ett flertal olika sanktionsmöjligheter av varierande svårighetsgrad kommer att göra det möjligt för organet för tvistlösning att välja en rimlig påföljd beroende på hur allvarligt fallet är. Det kan röra sig om offentliggörande av information om att organisationen inte följt principerna och om kravet att radera berörda uppgifter ([5]). Andra tänkbara påföljder är upphävande av organisationens status som ”ansluten till principerna”, skadestånd för personer som drabbats av att reglerna inte efterlevts eller förbudsförelägganden. Privata organ för tvistlösning eller självreglering skall anmäla fall där en *safe harbor*-organisation underlåter att rätta sig efter deras beslut till domstol eller i förekommande fall de statliga myndigheter som är behöriga att fatta beslut i ärendet samt att även informera Förenta Staternas handelsministerium eller dess utsedda företrädare.

Åtgärder från den federala konkurrensmyndighetens sida.

Den federala konkurrensmyndigheten (FTC) har förbundit sig att göra en förhandsprövning av klagomål som mottagits av organ för självreglering på integritetskyddets område, t.ex. BBBOnline och TRUSTe, och från medlemsstater i EU vilka hävdar att *safe harbor*-principerna inte följs, i syfte att avgöra huruvida det föreligger en överträdelse av avdelning 5 i Federal Trade Commission Act, som förbjuder illojala eller bedrägliga handlingar och metoder i handeln. Om den federala konkurrensmyndigheten har skäl att anta att det har skett en överträdelse av avdelning 5, kan myndigheten utverka ett förvaltningsbeslut som förbjuder de handlingar som klagomålet avser eller inge ett klagomål till den federala underrätten, som kan resultera i ett federalt domstolsbeslut. Konkurrensmyndigheten kan utverka böter för överträdelse av ett förvaltningsbeslut eller inleda civilrättsliga eller straffrättsliga förhandlingar om överträdelse av ett federalt domstolsbeslut. Konkurrensmyndigheten underrättar Förenta staternas handelsministerium om varje sådan åtgärd. Handelsministeriet anmodar andra statliga myndigheter att meddela ministeriet det slutliga avgörandet i varje sådant hänskjutet ärende liksom andra beslut och domar som gäller efterlevnad av *safe harbor*-principerna.

Upprepad överträdelse av principerna.

Om en organisation upprepade gånger överträder principerna, förlorar den sin rätt att omfattas av de fördelar *safe harbor* medför. Upprepad överträdelse av principerna föreligger när en organisation som genom självcertifiering till handelsministeriet (eller dess utsedda företrädare) anslutit sig till *safe harbor*-principerna vägrar att efterleva ett slutligt avgörande från ett privat eller statligt organ för tivstlösning eller där ett sådant organ finner att en organisation så ofta gör sig skyldig till överträdelser att det inte längre är rimligt att tro på organisationens försäkran att den följer principerna om *safe harbor*. I sådana fall måste organisationen snarast meddela handelsministeriet (eller dess utsedda företrädare) dessa fakta. Underlåtenhet att göra detta kan leda till enligt den amerikanska lagen om osann utsaga (False Statements Act).

Handelsministeriet (eller dess utsedda företrädare) skall i den offentliga förteckning som den för över organisationer som genom självcertifiering anslutit sig till *safe harbor*-principerna anteckna varje anmälan om upprepade överträdelser oavsett om den mottagits från organisationen själv, från ett organ för självreglering eller från en statlig myndighet, dock först sedan de gett den berörda organisationen en möjlighet att inom trettio (30) dagar gå i svaromål. Av den förteckning som handelsministeriet (eller dess utsedda företrädare) upprättar kommer följaktligen att framgå vilka organisationer som omfattas och vilka som inte omfattas av *safe harbor*-principerna.

([4]) Organen för tvistlösning behöver inte själva följa principerna för verkställighet. De kan också göra avsteg från principerna i fall med motstridiga intressen eller där det föreligger uttalade anvisningar för utförandet av organets specifika uppgifter.

([5]) Organen för tivstlösning kan själva välja de påföljder de anser rimliga. De berörda uppgifternas känslighet är ett kriterium som bör beaktas vid bedömningen av om uppgifterna behöver raderas. Ett annat kriterium är om en organisation har samlat in, använt eller publicerat information på ett sätt som uppenbart strider mot principerna.

En organisation som ansöker om att få delta i ett privat organ för självreglering med målsättningen att kvalificera sig för *safe harbor* måste till detta organ överlämna all information om tidigare deltagande i *safe harbor*.

FoS 12 – Valmöjlighet – Tidsfrister när man undanber sig direktmarknadsföring

F: *Innebär principen om valmöjlighet att en enskild får välja endast i början av ett förhållande eller när som helst?*

S: Allmänt sett är syftet med principen om valmöjlighet att se till att personuppgifter används och vidarebefordras på ett sätt som överensstämmer med den enskildes förväntningar och val. Därför skall en enskild när som helst kunna välja att undanbe sig att personuppgifter används för direktmarknadsföring, med förbehåll för rimliga tidsgränser för organisationen så att den t.ex. får tid på sig att verkställa den enskildes val. En organisation får också begära de uppgifter som krävs för att bekräfta identiteten hos den som undanber sig direktmarknadsföring. I USA kan de enskilda utöva denna möjlighet med hjälp av ett centralt system som det amerikanska direktreklamförbundets tjänst (Direct Marketing Association) Mail Preference Service. Organisationer som deltar i denna tjänst bör göra de konsumenter som inte vill ta emot direktreklam uppmärksamma på att tjänsten finns. Under alla omständigheter skall den enskilde ges möjlighet att på ett lättillgängligt och billigt sätt utöva denna möjlighet.

På samma sätt får en organisation använda personuppgifter i samband med viss direktmarknadsföring, om det är orimligt svårt att erbjuda den enskilde möjlighet att undanbe sig direktmarknadsföring innan uppgifterna används. För detta krävs att organisationen samtidigt och utan dröjsmål (eller när som helst, på begäran) ger den enskilde möjlighet att (utan kostnad för den enskilde) undanbe sig ytterligare direktmarknadsföring, och att organisationen rättar sig efter den enskildes önskemål.

FoS 13 – Reseuppgifter

F: *När får uppgifter om flygbokningar och andra uppgifter i anslutning till resor, t.ex. om* frequent flyer*-program, hotellbokningar och särskilda behov, t.ex. måltidskrav av religiösa skäl eller behov på grund av funktionshinder, överföras till organisationer belägna utanför EU?*

S: Sådana uppgifter får överföras under flera olika omständigheter. Enligt artikel 26 i direktivet får personuppgifter överföras ”till ett tredje land som inte har en adekvat skyddsnivå i den mening som avses i artikel 25.2” förutsatt att 1) det är nödvändigt för att tillhandahålla tjänster som konsumenten begär eller fullgöra ett avtal, t.ex. ett *frequent flyer*-avtal eller att 2) konsumenten otvetydigt samtyckt till överföringen. Organisationer i USA som omfattas av *safe harbor*-principerna ger adekvat skydd för personuppgifter, och får därför ta emot upgifter från EU utan att uppfylla dessa villkor eller andra villkor i artikel 26 i direktivet. Eftersom *safe harbor*-principerna har särskilda regler för känsliga uppgifter, får sådana uppgifter (som exempelvis samlats in för att betjäna funktionshindrade passagerare) ingå i överföringar till organisationer som deltar i *safe harbor*-samarbetet. Under alla omständigheter måste dock den organisation som överför uppgifterna följa lagen i den EU-medlemsstat den verkar i, vilket bl.a. kan innebära särskilda villkor för behandling av känsliga uppgifter.

FoS 14 – Farmaceutiska och medicinska produkter

F1: *Om personuppgifter insamlas inom EU och överförs till Förenta staterna för läkemedelsforskning och/eller för andra ändamål, tillämpas i så fall medlemsstaternas lagar eller* safe harbor*-principerna?*

S: Medlemsstaternas lagstiftning tillämpas vid insamling av personuppgifter och vid all den bearbetning, som äger rum före överförandet till USA. *Safe harbor*-principerna tillämpas på uppgifterna först sedan de överförts till USA. Uppgifter som används för läkemedelsforskning eller för andra ändamål skall när så befinns lämpligt avidentifieras.

F2: *Personuppgifter som framkommit vid specificerade medicinska och farmaceutiska forskningar och undersökningar spelar ofta en framträdande roll vid kommande vetenskaplig forskning. När personuppgifter som insamlats för forskning och studium, överförs till en* safe harbor*-organisation i Förenta staterna, får då denna organisation använda dessa uppgifter för ny vetenskaplig forskningsverkamhet?*

S: Ja, om principerna för meddelande och valmöjlighet vederbörligen följts vid den första användningen. I ett meddelande skall upplysningar ges om varje kommande specificerad användning av dessa uppgifter såsom periodisk uppföljning, undersökningar inom närliggande områden eller marknadsföring. Det underförstås, att all framtida användning av dessa uppgifter inte kan specificeras, emedan ny användning av forskningsrön kan uppstå ur förnyad förståelse av ursprungliga rön, nya upptäckter och framsteg inom medicinen samt utvecklingen inom folkhälsa och hälsovårdslagstiftning. Där så befinns lämpligt, skall följaktligen meddelandet innehålla en förklaring av huruvida personuppgifter får användas vid sådan framtida medicinsk och farmakologisk forskningsverksamhet som inte kan förutses. Om användningen inte är förenlig med de(t) allmänna forskningssyfte(n) vartill uppgifterna ursprungligen insamlats, eller vartill den enskilde sedermera samtyckt, måste nytt samtycke inhämtas.

F3: *Vad händer med uppgifter om en individ, om en deltagare frivilligt eller på det sponsrande företagets begäran beslutar att dra sig ur det kliniska försöket?*

S: Deltagare får när som helst besluta sig för eller uppmanas att dra sig ur ett kliniskt försök. Alla uppgifter som insamlats före utträdet får emellertid fortsätta att bearbetas tillsammans med de övriga uppgifter som insamlats för användning i det kliniska försöket, om detta klargjordes för deltagaren i meddelandet då han/hon samtyckte till att delta.

F4: *Läkemedels- och sjukvårdsutrustningsföretag har tillstånd att lämna personuppgifter från kliniska försök som genomförts i EU till tillsynsmyndigheter i USA för kontroll- och övervakningsändamål. Tillåts liknande överföringar till andra intresserade än tillsynsmyndigheter såsom produktionsanläggningar och övriga forskare?*

S: Ja, om det är förenligt med principerna för meddelande och valmöjlighet.

F5: *För att säkerställa objektivitet kan vid många kliniska försök varken deltagare eller forskningsledare få tillgång till uppgifter om vilken behandling som varje deltagare erhåller. Om så skulle ske skulle undersökningens giltighet och dess resultat kunna äventyras. Kommer deltagarna i sådana kliniska försök (s.k. blindtest) att få tillgång till uppgifter?*

S: Nej, sådan tillgång behöver inte beredas deltagaren, om denna inskränkning förklarats när deltagaren började delta i försöket, och om avslöjande av sådana uppgifter skulle äventyra forskningsförsökets integritet. Samtycke till att delta i försöket medför under dessa betingelser rimligen ett avstående från rätten till tillgång. När försöket avslutats, och resultaten analyserats, kommer deltagarna att få tillgång till uppgifterna om sig själva, om de fordrar det. De skall i första hand begära dem av den läkare eller annan sjukvårdsproducent som inom ramen för det kliniska försöket behandlat dem eller i andra hand av det sponsrande företaget.

F6: *Bör läkemedels- eller sjukvårdsutrustningsföretag i sin strävan efter produktsäkerhet och effektivitetskontroll inklusive rapporter om negativa effekter och spårande av patienter/försökspersoner, som använder vissa mediciner eller viss medicinsk utrustning (t.ex. pacemaker), tillämpa* safe harbor-*principerna, när det gäller meddelande, valmöjlighet, vidare överföring och tillgång?*

S: Nej, i den utsträckning dessa principer tillämpas, så att de sammanfaller med efterlevnaden av tillsynslagstiftningens krav. Detta gäller både rapporter från t.ex. sjukvårdsproducenter till läkemedels- och sjukvårdsutrustningsföretag och rapporter från läkemedels- och sjukvårdsutrustningsföretag till regeringsorgan som Food and Drug Administration.

F7: *Forskningsrön kodas alltid inledningsvis av ansvarig forskningsledare för att enskilda försökspersoners identitet inte skall avslöjas. De läkemedelsföretag, som sponsrar sådan forskning, får ej tillgång till kodnyckeln. Den enda kodnyckeln finns endast hos forskaren, för att han/hon under vissa omständigheter skall kunna identifiera försökspersonen (t.ex. om medicinsk uppföljning erfordras). Utgör en överföring från EU till USA av uppgifter, som kodats på detta sätt, en sådan överöring av personuppgifter som omfattas av* safe harbor-*principerna?*

S: Nej, den utgör inte en sådan överföring av personuppgifter som omfattas av dessa principer.

FoS 15 – Offentliga register och allmänt tillgängliga uppgifter

F: *Är det nödvändigt att tillämpa principerna om meddelande, valfrihet och vidare överföring på offentliga register och allmänt tillgängliga uppgifter?*

S: Det är inte nödvändigt att tillämpa principerna om meddelande, valfrihet och vidare överföring på allmänt tillgängliga uppgifter, förutsatt att de inte kombineras med icke offentliga uppgifter och att alla villkor för att ta del av uppgifterna som fastställts av behörig myndighet följs.

Det är i allmänhet inte heller nödvändigt att tillämpa principerna om meddelande, valfrihet och vidare överföring på allmänt tillgängliga uppgifter, om inte den som överför uppgifterna från EU anger att uppgifterna omges av restriktioner så att det krävs att principerna för det aktuella ändamålet tillämpas av organisationen. Organisationer har inget ansvar för hur sådana uppgifter används av dem som erhåller uppgifterna från offentligt material.

Om en organisation befinns ha uppsåtligt offentliggjort personuppgifter i strid med principerna så att den eller andra kunnat utnyttja dessa undantag, skall den inte längre anses uppfylla kraven för att omfattas av *safe harbor*-förmånerna.

BILAGA III

Översikt över tillämpningen av *safe harbor*-förslaget

Integritetsskyddet och befogenheter på federal nivå och delstatsnivå avseende ”illojala metoder och bedrägligt beteende”

I denna PM redovisas översiktligt vilka befogenheter Federal Trade Commission (FTC) har enligt paragraf (section) 5 i lagen om dess inrättande (Federal Trade Commission Act, 15 U.S.C. [Förenta staternas lag, United States Code] §§ 41–58, i den senaste lydelsen) att ingripa mot den som underlåter att skydda personuppgifter i överensstämmelse med sina egna framställningar och/eller åtaganden att göra detta. Dessutom redogörs för undantagen från dessa befogenheter och för vilka möjligheter andra federala myndigheter och delstatsmyndigheter har att ingripa i fall där FTC saknar befogenhet ([1])

FTC:s befogenheter när det gäller ”illojala eller bedrägliga metoder”

Enligt paragraf 5 i Federal Trade Commission Act är ”illojala eller bedrägliga handlingar eller metoder inom handeln eller med påverkan på denna” olagliga, se 15 U.S.C. § 45(a)(1). Genom paragraf 5 får FTC oinskränkt rätt att förhindra sådana handlingar och metoder, se 15 U.S.C. § 45(a)(2). Detta innebär att FTC efter att ha anordnat ett formellt förhör får fatta ett förvaltningsbeslut (*cease and desist order*) som förbjuder det felaktiga beteendet, se 15 U.S.C. § 45(b). FTC kan också, om detta gynnar allmänintresset, ansöka hos en amerikansk underrätt (U.S. district court) om ett tillfälligt rättsligt förbud (temporary restraining order) eller om ett interimistiskt eller permanent förbudsföreläggande (temporary injunction eller permanent injunction), se 15 U.S.C. § 53(b). I fall där det föreligger ett utbrett mönster av illojala eller bedrägliga handlingar eller metoder, eller där FTC redan har fattat förvaltningsbeslut om förbud, får FTC utfärda en förvaltningsföreskrift (administrative rule) om förbud mot handlingarna eller metoderna i fråga, se 15 U.S.C. § 57a.

Underlåtenhet att efterleva ett av FTC fattat förvaltningsbeslut beivras med vite (civil penalty) på upp till 11 000 US-dollar för varje dag som underlåtenheten fortgår ([2]), se 15 U.S.C. § 45(1). Den som medvetet överträder en av FTC utfärdad förvaltningsföreskrift kan åläggas att betala 11 000 US-dollar för varje sådan överträdelse, se 15 U.S.C. § 45(m). Verkställighetstalan kan väckas antingen av justitieministeriet eller, om detta avstår, av FTC, se 15 U.S.C. § 56.

Integritetskyddet och FTC:s befogenheter

I utövandet av sina befogenheter enligt paragraf 5 intar FTC den ståndpunkten att lämnande av missvisande information om varför uppgifter samlas in från konsumenterna eller om hur sådana uppgifter kommer att användas utgör ett bedrägligt beteende ([3]). År 1998 framställde FTC exempelvis klagomål mot företaget GeoCities för att utan de berördas förhandstillstånd ha lämnat ut information som företaget samlat in på sin webbplats till en utomstående som avsåg att använda information för marknadsföring, trots att GeoCities gjort en framställning om att så inte skulle kunne ske ([4]). FTC:s personal har också framhållit att insamling av personuppgifter från barn liksom försäljning och utlämnande av sådana uppgifter sannolikt utgör illojala metoder om föräldrarnas medgivande saknas ([5]).

([1]) Här tar vi inte upp vare sig alla de olika federala författningar som berör integritetsskydd i specifika sammanhang eller de delstatsförfattningar och den rättspraxis som kan äga tillämplighet. Bland de federala författningar som reglerar kommersiell insamling och användning av personuppgifter märks Lagen om kabelkommunikationer (Cable Communications Policy Act, 47 U.S.C. § 551), Lagen om integritetsskydd för bilförare (Driver's Privacy Protection Act, 18 U.S.C. § 2721), Lagen om elektronisk brevhemlighet (Electronic Communications Privacy Act, 18 U.S.C. § 2701 f.), Lagen om elektronisk överföring av pengar (Electronic Funds Transfer Act, 15 U.S.C. §§ 1693, 1693m), Lagen om rättvis kreditrapportering (Fair Credit Reporting Act, 15 U.S.C. § 1681 f), Lagen om integritetsskydd för finansiella uppgifter (Right to Financial Privacy Act, 12 U.S.C. § 3401 f), Lagen om konsumentskydd för telefonabonnenter (Telephone Consumer Protection Act, 47 U.S.C. § 227) och Lagen om integritetsskydd i samband med videouthyrning (Video Privacy Protection Act, 18 U.S.C. § 2710). Många av delstaterna har motsvarande lagstiftning på dessa områden. Se t.ex. Massachusetts allmänna lagar (Mass. Gen. Laws) kapitel 167B § 16 (om förbud för finansinstitut att lämna ut finansiella uppgifter om en kund till tredje part utan vare sig kundens medgivande eller ett beslut av domstol) och New Yorks allmänna hälsolag (N.Y. Pub. Health Law) § 17 (om begränsningar för användning och utlämnande av uppgifter om en persons medicinska eller mentala hälsa samt om rätt för patienterna att få tillgång till sådana uppgifter).

([2]) I ett sådant ärende kan den amerikanska underrätten dessutom meddela förbudsföreläggande och föreskriva andra lämpliga säkerhetsåtgärder för verkställigheten av FTC:s förvaltningsbeslut. 15 U.S.C. § 45(1).

([3]) ”Bedrägligt beteende” definieras som en framställning, ett utelämnande eller ett beteende som sannolikt väsentligen vilseleder en omdömesgill konsument.

([4]) Se www.ftc.gov/opa/1998/9808/geocitie.htm.

([5]) Se brev från personalen till Center for Media Education, www.ftc.gov/os/1997/9707/cenmed.htm. Dessutom ger Lagen om integritetsskydd för barn i samband med direkttjänster (Children's Online Privacy Protection Act of 1998) FTC specifik rättslig befogenhet att reglera sådan insamling av personuppgifter från barn som utförs av företag som driver webbplatser och direkttjänster (online services), se 15 U.S.C. §§ 6501–6506. I synnerhet krävs i den ovannämnda lagen att den som driver en direkttjänst och vill samla in, använda eller lämna ut barns personuppgifter måste informera föräldrarna om detta och få deras medgivande, som måste kunna verifieras *Idem* § 6502(b). Samma lag ger dessutom föräldrarna rätt att få tillgång till uppgifterna och att förbjuda vidare användning av dem *Idem*.

I ett brev till generaldirektör John Mogg vid Europeiska kommissionen nämnde FTC:s ordförande Pitofsky att det finns begränsningar för FTC:s befogenheter i fråga om integritetsskydd när det inte har lämnats någon missvisande information (eller någon information över huvud taget) om hur de insamlade uppgifterna kommer att användas. FTC-ordföranden Pitofskys brev till John Mogg (23 september 1998). Företag som vill utnyttja *safe harbor*-förslaget kommer emellertid att vara tvungna att garantera att de kommer att skydda de uppgifter de samlar in i enlighet med föreskrivna riktlinjer. Detta innebär att ett företag som garanterar att det kommer att skydda personuppgifter men sedan underlåter att göra detta har lämnat missvisande information och således gjort sig skyldigt till ett ”bedrägligt beteende” i den mening som avses i paragraf 5.

FTC:s jurisdiktion omfattar illojala eller bedrägliga handlingar eller metoder ”inom handeln eller med påverkan på denna”, vilket betyder att FTC saknar jurisdiktion när det gäller insamling och användning av personuppgifter i andra syften än affärsmässiga, såsom att samla in pengar till välgörande ändamål. Se brevet från Pitofsky, s. 3. Det räcker emellertid med att personuppgifter är inbegripna i någon affärsmässig transaktion för att FTC skall ha jurisdiktion. Således skulle exempelvis en arbetsgivares försäljning av sina anställdas personuppgifter till ett direktmarknadsföringföretag omfattas av paragraf 5.

Undantag enligt paragraf 5

I paragraf 5 anges att FTC:s befogenheter vad gäller illojala eller bedrägliga handlingar eller metoder inte gäller

— finansinstitut, inbegripet banker, hypotekskassor (savings and loans) och kooperativa lånekassor (credit unions),

— allmänna teleoperatörer och företag som ägnar sig åt allmänna transporter mellan delstater,

— lufttransportföretag och

— förpackningsföretag (packers) och operatörer av boskapsdepåer (stockyard operators).

Se 15 U.S.C § 45(a)(2). Här nedan diskuterar vi de enskilda undantagen och vilka tillsynsmyndigheterna är för vart och ett av dem.

Finansinstitut ([6])

Det första undantaget avser ”banker, sådana hypotekskassor som beskrivs i paragraf 18(f)(3) (15 U.S.C. § 57a(f)(3))” och ”sådana federala kooperativa lånekassor som beskrivs i paragraf 18(f)(4) (15 U.S.C. § 57a(f)(4)” ([7]). Dessa finansinstitut omfattas i stället av föreskrifter utfärdade av Federal Reserve Board, Office of Thrift Supervision ([8]) respektive National Credit Union Administration Board, se 15 U.S.C. § 57a(f). Dessa tillsynsorgan har ålagts att meddela de föreskrifter som krävs för att förhindra illojala metoder och bedrägligt beteende från de berörda finansinstitutens sida ([9]) och att inrätta en särskild avdelning med uppgiften att handlägga klagomål från konsumenter, se 15 U.S.C. § 57a(f)(1). Befogenheterna i fråga om verkställighet härrör från paragraf 8 i Lagen om federal garanti för bankinlåning (Federal Deposit Insurance Act. 12 U.S.C. § 1818) vad gäller banker och hypotekskassor och från paragraferna 120 och 206 i Lagen om federala kooperativa lånekassor (Federal Credit Union Act) vad gäller federala kooperativa lånekassor, se 15 U.S.C. §§ 57a(f)(2)–(4).

Försäkringsbranschen nämns inte uttryckligen i listan över undantag i paragraf 5, men lagen McCarran-Ferguson Act (15 U.S.C. § 1011 f.) överlåter generellt tillsynen över försäkringsverksamhet till de enskilda delsta-

([6]) Den 12 november 1999 undertecknade president Clinton lagen Gramm-Leach-Bliley Act (Pub. L. 106–102. kodifiering: 15 U.S.C. § 6801 ff), vilket innebar att den trädde i kraft. Genom denna lag begränsas finansinstitutens möjligheter att lämna ut personuppgifter om sina kunder. Instituten åläggs bland annat att informera alla sina kunder om sin integritetsskyddspolicy och om sin praxis i fråga om spridning av personuppgifter till närstående och icke-närstående bolag. Lagen ger FTC, de federala banktillsynsmyndigheterna och andra myndigheter rätt att meddela föreskrifter för att få till stånd det integritetsskydd som krävs i lagen. Dessa myndigheter har utarbetat förslag till föreskrifter med det syftet.

([7]) Detta undantag är så formulerat att det inte gäller värdepapperssektorn. Därför hat Securities and Exchange Commission och FTC konkurrerande jurisdiktion över mäklare, börshandlare och andra i värdepappersbranschen när det gäller illojala eller bedrägliga handlingar och metoder.

([8]) Undantaget i paragraf 5 hänvisade ursprungligen till Federal Home Loan Bank Board som avskaffade i augusti 1989 genom Lagen om reformering, återställande och genomförande för finansinstitut (Financial Institutions Reform, Recovery and Enforcement Act of 1989). Dess funktioner överfördes till Office of Thrift Supervision och till Resolution Trust Corporation, Federal Deposit Insurance Corporation och Housing Finance Board.

([9]) I paragraf 5 anges visserligen att vissa finansinstitut inte omfattas av FTC:s jurisdiktion, men där sägs också att när FTC meddelar en förvaltningsföreskrift avseende illojala eller bedrägliga handlingar och metoder bör tillsynsorganen för finansinstituten meddela motsvarande föreskrifter inom 60 dagar, se 15 U.S.C. § 57a(f)(1).

terna ([10]). Dessutom sägs i paragraf 2(b) i McCarran-Ferguson Act att ingen federal lag kan annullera, begränsa eller ha företräde framför delstaternas föreskrifter ”annat än om den federala lagen i fråga specifikt avser försäkringsverksamhet”, se 15 U.S.C. § 1012(b). Bestämmelserna i Federal Trade Commission Act är dock tillämpliga på försäkringsbranschen ”i den mån denna verksamhet inte regleras av delstatslagstiftning”, *Id*. Det bör också noteras att McCarran-Ferguson ger befogenheter till delstaterna bara när det gäller försäkringsverksamhet. Därför har FTC kvar sina befogenheter när det gäller illojala eller bedrägliga metoder som försäkringsbolag använder utanför sin försäkringsverksamhet. Ett exempel på detta skulle kunna vara när försäkringsbolag säljer personuppgifter om sina försäkringstagare till företag som ägnar sig åt direktmarknadsföring av annat än försäkringar ([11]).

Allmänna teleoperatörer och transportföretag

Det andra undantaget enligt paragraf 5 avser sådana allmänna teleoperatörer och transportföretag som ”omfattas av de lagar som syftar till reglering av handeln”, se 15 U.S.C. § 45(a)(2). I det här fallet avses med ”de lagar som syftar till reglering av handeln” delkapitel (subtitle) IV i kapitel (Title) 49 i Förenta staternas lag (United States Code) samt Lagen om kommunikationer (Communications Act of 1934, 47 U.S.C. § 151 f.), se 15 U.S.C. § 44.

Kapitel 49 delkapitel IV i U.S.C. (Transport mellan delstater) gäller järnvägs-, landsvägs- och vattenvägstransportföretag, mäklare, speditörer och rörledningstransportföretag, se 49 U.S.C. § 10101 f. Föreskrifter för dessa olika typer av allmänna transportföretag meddelas av Surface Transportation Board, ett oberoende organ inom transportministeriet, se 49 U.S.C. §§ 10501, 13501 och 15301. För samtliga typer gäller att transportföretaget inte får lämna ut information om lastens karaktär, bestämmelseort och andra egenskaper som kan användas till förfång för avsändaren, se 49 U.S.C. §§ 11904, 14908 och 16103. Vi noterar att dessa bestämmelser avser information om försändelsen och således inte förefaller gälla personuppgifter som avsändaren som saknar samband med den berörda försändelsen.

I Communications Act sägs att ”handel mellan delstater och med utlandet avseende kommunikation per tråd och radio” skall regleras av Federal Communications Commission (FCC), se 47 U.S.C. §§ 151 och 152. Förutom allmänna teleoperatörer gäller Communciations Act även televisions- och radioutsändningsföretag och kabeloperatörer, vilka inte är allmänna teleoperatörer och således inte omfattas av undantaget enligt paragraf 5. Detta innebär att FTC har jurisdiktion att undersöka om företag i dessa tre kategorier använder illojala metoder och bedrägligt beteende, medan FCC har konkurrerande jurisdiktion att utöva sina oberoende befogenheter på detta område enligt beskrivningen nedan.

Enligt Communications Act är ”alla teleoperatörer”, inbegripet lokalväxelföretag, skyldiga att skydda privata uppgifter om kunderna ([12]), se 47 U.S.C § 222(a). Vid sidan av denna allmänna integritetsskyddande bestämmelse infördes år 1984 i Communications Act, genom Lagen om kabelkommunikationer (Cable Communications Policy Act of 1984, 47 U.S.C. § 521 f.) (Cable Act), en uttrycklig skyldighet för kabeloperatörer att skydda ”uppgifter som kan identifieras med avseende på person” om abonnenter på kabeltjänster, se 47 U.S.C. § 551 ([13]). Enligt Cable Act måste kabeloperatörernas insamling av personuppgifter hålla sig inom vissa ramar, och kabeloperatörerna måste informera abonnenterna om vilka slags uppgifter som samlas in och hur dessa kommer att användas. Cable Act ger också abonnenterna rätt att få tillgång till uppgifterna om dem själva och tvingar kabeloperatörerna att förstöra dessa uppgifter när de inte längre behövs.

Communications Act ger FCC befogenhet att säkerställa efterlevnaden av de båda ovannämnda bestämmelserna om integritetsskydd, antingen på eget initiativ eller som uppföljning av utifrån kommande klagomål ([14]), se 47 U.S.C., §§ 205, 403; *Idem*, § 208. När FCC finner att teleoperatörer (inbegripet kabeloperatörer) har brutit mot integritets-

([10]) Försäkringsverksamhet, och alla personer som är sysselsatta i sådan, skall omfattas av de enskilda delstaternas lagar om tillsyn över och beskattning av sådan verksamhet, se 15 U.S.C. § 1012(a).

([11]) FTC har utövat sin jurisdiktion över försäkringsbolag i olika sammanhang. I ett fall väckte FTC talan mot ett bolag för vilseledande reklam i en delstat där bolaget saknade näringstillstånd. Domstolen godkände FTC:s jurisdiktion med motiveringen att det saknades verkningsfulla delstatsföreskrifter, eftersom bolaget i själva verket befann sig utom räckhåll för delstaten. Se FTC v. Travelers Health Association, 362 U.S. 293 (1960).
Av delstaterna har 17 infört lagen om integritetsskydd av försäkringsinformation (Insurance Information and Privacy Protection Act), ett förslag till lag som utarbetats av National Association of Insurance Commissioners (NAIC). Denna lag innehåller bestämmelser om information till berörda, om användning och utlämnande av uppgifter och om berördas tillgång till uppgifterna. Dessutom har nästan alla delstaterna infört NAIC:s föreslagna Lag om illojala metoder inom försäkringsbranschen (Unfair Insurance Practices Act), som särskilt avser illojala metoder inom försäkringsbranschen.

([12]) Med begreppet ”privata uppgifter om kundens nätanvändning” (customer proprietary network information) avses uppgifter om en kunds ”användning av en telekommunikationstjänst i fråga om kvantitet, teknisk konfiguration, typ, mottagare och belopp” samt telefonräkningsuppgifter, se 47 U.S.C. § 222(f)(1). Däremot innefattar begreppet inte uppgifter i abonnentförteckningar, *idem*.

([13]) Lagen innehåller ingen uttrycklig definition av ”uppgifter som kan identifieras med avseende på person”.

([14]) Denna befogenhet inbegriper rätten till gottgörelse för överträdelser av reglerna om integritetsskydd enligt antingen paragraf 222 i Communications Act eller, i fråga om kabeltjänstabonnenter, enligt paragraf 551 i Cable Act (om ändring av Communications Act). Se även 47 U.S.C. § 551(f)(3). (Civilrättslig talan i federal underrätt utesluter inte gottgörelse av annat slag utan står till förfogande utöver varje annan laglig form av gottgörelse som kan komma i fråga för en kabeltjänstabonnent.)

skyddsreglerna i paragraf 222 eller paragraf 551, finns det tre grundläggande åtgärder som FCC kan vidta. För det första kan FCC, efter att ha anordnat förhör och fastställt att en överträdelse har skett, ålägga företaget att betala skadestånd i pengar ([15]), se 47 U.S.C. § 209. För det andra kan FCC ålägga företaget att upphöra med den felaktiga metoden eller underlåtenheten, se 47 U.S.C. § 205(a). Och för det tredje kan FCC ålägga företaget att ”tillämpa föreskrifter eller metoder” som FCC bestämmer, *idem*.

Privatpersoner som tror att en teleoperatör eller en kabeloperatör har brutit mot de relevanta bestämmelserna i Communications Act eller Cable Act kan antingen inge ett klagomål till FCC eller väcka talan i en federal underrätt, se 47 U.S.C. § 207. Om rätten finner att teleoperatören har underlåtit att skydda privata kunduppgifter enligt den allmännare paragraf 222 i Communications Act, kan klaganden tilldömas ersättning för den faktiska skadan och advokatarvoden, se 47 U.S.C. § 206. Den som väcker talan om brott mot integritetsskyddet enligt den för kabeltjänster specifika paragraf 551 i Cable Act kan utöver ersättning för den faktiska skadan och advokatarvoden även tilldömas straffskadestånd och ersättning för rimliga rättegångskostnader, se 47 U.S.C. § 551f.

FCC har antagit detaljerade regler för genomförandet av paragraf 222, se 47 CFR 64.2001-2009. Dessa regler innehåller konkreta åtgärder som skall förhindra att obehöriga personer får tillgång till privata uppgifter om kunders nätanvändning. Teleoperatörerna måste bland annat

— utveckla och införa datorprogram som gör att uppgifter som gäller huruvida en kund har informerats respektive givit sitt medgivande kommer upp på datorskärmen så snart någon hämtar fram uppgifter om den kunden,

— föra ett elektroniskt register över åtkomsten av kunduppgifterna, bland annat avseende när, av vem och varför uppgifter om en viss kund hämtas fram,

— utbilda sin personal i vad som är tillåten användning av privata uppgifter om kunders nätanvändning och införa lämpliga disciplinförfaranden,

— skapa en kontrollprocess som säkerställer att reglerna följs i samband med extern marknadsföring och

— årligen avge en rapport till FCC om hur de efterlever dessa regler.

Lufttransportföretag

Amerikanska och utländska lufttransportföretag som omfattas av Lagen om federal flygfart (Federal Aviation Act of 1958) är också undantagna från paragraf 5 i Federal Trade Commission Act, se 15 U.S.C. § 45(a)(2). Detta inbegriper var och en som tillhandahåller gods- eller passagerartransporter med luftfartyg mellan delstater eller mellan USA och andra länder samt var och en som transporterar post med luftfartyg, se 49. U.S.C. § 40102. Lufttransportföretag sorterar under transportministeriet, och transportministern har befogenhet att vidta åtgärder för att ”förhindra illojala, bedrägliga, prisdumpande (predatory) eller konkurrenshämmande metoder inom lufttransportsektorn”, se 49 U.S.C. § 40101(a)(9). Transportministern får, om detta gynnar allmänintresset, undersöka om ett amerikanskt eller utländskt lufttransportföretag eller en biljettagent har använt en illojal eller bedräglig metod, se 49 U.S.C. § 41712. Efter förhör kan transportministern beordra det berörda företaget at upphöra med den olagliga metoden, *idem*, Såvitt vi känner till har transportministern inte utövat denna befogenhet i fråga om skydd av personuppgifter om flygbolagens kunder ([16]).

Det finns två bestämmelser om skydd av personuppgifter som är tillämpliga på lufttransportföretag under särskilda omständigheter. För det första innehåller Federal Aviation Act regler om integritetsskydd för den som söker anställning som pilot, se 49 U.S.C. § 44936(f). Transportföretagen ges visserligen rätten att skaffa sig information om den sökandes tidigare anställningar men den sökande tillerkänns också vissa rättigheter: han skall underrättas om att någon har begärt att få ut sådan information, han måste godkänna en sådan begäran, han har rätt att korrigera eventuella felaktigheter och informationen får inte lämnas ut till andra än dem som medverkar i anställningsbeslutet. För det andra säger transportministeriets föreskrifter att de passagerarlistor som är avsedda att användas av staten i händelse av en flygkatastrof ”skall hållas hemliga och får överlämnas bara till Förenta staternas utrikesministerium. National Transportation Board (på NTSP:s begäran) och Förenta staternas transportministerium”, se 14 CFR del 243, § 243.9(c) (med tillägg genom 63 FR 8258).

([15]) Det faktum att den klagande inte har lidit någon direkt skada är dock inte grund för att avfärda ett klagomål, se 47 U.S.C. § 208(a).

([16]) Vi har förstått att man inom branschen har börjat ta itu med frågan om integritetsskydd. Branschföreträdare har diskuterat de föreslagna *safe harbor*-principerna och möjligheten att tillämpa dem på flygbolag. Bland annat har det föreslagits att man skulle anta en integritetsskyddspolicy på branschnivå som innebar att de deltagande företagen uttryckligen underställde sig transportministeriets myndighet.

Förpackningsföretag och operatörer av boskapsdepåer

Enligt Lagen om förpackningsföretag och operatörer av boskapsdepåer (Packers and Stockyards Act of 1921, 7 U.S.C. § 181 f.) är det olagligt för ”förpackningsföretag (packers), vad gäller boskap, kött, köttbaserade livsmedel eller boskapsprodukter i oförädlad form, och för företag som handlar med levande fjäderfä, vad gäller levande fjäderfä, att medverka i eller använda någon illojal, orättvist diskriminerande eller bedräglig metod eller plan”, se 7 U.S.C. § 192(a); se även 7 U.S.C. § 213(a) (om förbud mot ”varje illojal, orättvist diskriminerande eller bedräglig metod eller plan” med anknytning till boskap). Jordbruksministern har det primära ansvaret för att se till att dessa bestämmelser efterlevs, medan FTC har jurisdiktion över detaljhandelstransaktioner och över transaktioner där fjäderfäbranschen är involverad, se 7 U.S.C § 227(b)(2).

Det är oklart om jordbruksministern skulle tolka ett förpackningsföretags eller en boskapsdepåoperatörs underlåtenhet att skydda integriteten för personuppgifter i överensstämmelse med sin angivna policy som en ”bedräglig” metod enligt Packers and Stockyards Act. Emellertid är undantaget enligt paragraf 5 tillämpligt på personer och bolag bara ”i den utsträckning som de omfattas av Packers and Stockyards Act”. Detta innebär att om integritetsskyddet för personuppgifter inte är en fråga som omfattas av Packers and Stockyards Act, är det högst sannolikt att undantaget enligt paragraf 5 inte är tillämpligt, vilket skulle betyda att förpackningsföretag och operatörer av boskapsdepåer i detta avseende är underställda FTC:s myndighet.

Delstaternas befogenheter vad gäller ”illojala metoder och bedrägligt beteende”

Enligt en undersökning som gjorts av FTC:s personal har ”alla femtio delstaterna samt District of Columbia, Guam, Puerto Rico och amerikanska Virgin Islands infört lagar, mer eller mindre lika Federal Trade Commission Act (FTCA), för att förhindra illojala eller bedrägliga affärsmetoder”. Faktablad från FTC, omtryckt i ”Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation”, 59 Tul. L. Rev. 427 (1984). I samtliga fall finns det en tillsynsmyndighet med befogenhet att ”genomföra undersökningar och därvid använda stämningar (subpoenas) eller civilrättsliga åligganden, att utkräva åtaganden om frivillig efterrättelse och att meddela förvaltningsbeslut om förbud eller ansöka hos domstolar om förbudsföreläggande för att förhindra användningen av illojala, oskäliga eller bedrägliga affärsmetoder” *idem*. I 46 jurisdiktioner tillåter lagen civilrättslig talan om skadestånd motsvarande den faktiska skadan, två eller tre gånger detta belopp eller straffskadestånd samt, i några fall, ersättning för rättegångskostnader och advokatarvoden, *idem*.

Ett exempel är Floridas Lag om bedrägliga och illojala affärsmetoder (Deceptive and Unfair Trade Practices Act), som ger delstatens justitiekansler (attorney general) befogenhet att undersöka och väcka civilrättsligt åtal avseende ”illojala konkurrensmetoder, illojala, oskäliga eller bedrägliga affärsmetoder”, inbegripet felaktig eller vilseledande reklam, vilseledande franchise- eller affärsmöjligheter, bedräglig telefonförsäljning och pyramidspel. Se även delstaten New Yorks Allmänna handelslag (N.Y. General Business Law) § 349 (om förbud mot illojala handlingar och bedrägliga metoder i affärsverksamhet).

En enkät som National Association of Attorneys General (NAAG) gjort i år bekräftar dessa slutsatser. Av de 43 delstater som svarade har samtliga ”mini-FTC”-regler eller andra regler som ger ett jämförbart skydd. I samma enkät uppgav 39 stater att de skulle ha befogenhet att ta upp klagomål från personer som inte var bosatta i deras delstat. När det specifikt gällde integritetsskyddet för konsumenter uppgav 37 av de 41 delstater som svarade att de skulle vidta åtgärder om de fick in klagomål om att ett företag inom deras jurisdiktion inte följde den integritetsskyddspolicy som företaget självt angivit.

BILAGA IV

Integritetsskydd och skadestånd, befogenhet i lag (Legal Authorizations) samt fusioner och övertrag i amerikansk lag

Detta är ett svar på EU:s begäran om förtydliganden av amerikansk lag när det gäller a) krav på skadestånd för integritetsintrång, b) uttryckliga befogenheter i amerikansk lag att använda personuppgifter på ett sätt som inte överensstämmer med *safe harbor*-principerna samt c) verkan av fusioner och övertag på *safe harbor*-åtaganden.

A. **Skadestånd för integritetsintrång**

Underlåtenhet att iaktta *safe harbor*-principerna kan vara grund för olika typer av civilrättslig talan beroende på vilka de relevanta omständigheterna i det enskilda fallet är. Först och främst kan talan väckas mot *safe harbor*-organisationer för missvisande information (misrepresentation), om de underlåter att följa sina egna angivna integritetsregler. I rättspraxis finns även grunder för civilrättslig talan om skadestånd för integritetsintrång. Många lagar på federal nivå eller delstatsnivå ger också enskilda möjlighet att kräva skadestånd för intrång.

Rätten till skadestånd för intrång i den enskildes personliga integritet är väl etablerad i amerikansk rättspraxis.

Att använda personuppgifter på ett sätt som strider mot *safe harbor*-principerna kan leda till skadeståndsansvar ur flera olika rättsperspektiv. Till exempel kan både den uppgiftsöverförande registeransvarige och de personligen berörda stämma en *safe harbor*-organisation för missvisande information om den underlåter att iaktta, sina *safe harbor*-åtaganden. Enligt Restatement of the Law, Second, Torts [1] gäller följande:

> Envar som i bedrägligt syfte lämnar missvisande information om fakta, åsikter, avsikter eller lagar för att förmå någon annan att handla eller avstå från att handla i förlitan på denna information, kan dömas att betala skadestånd till denne andre, som blivit vilseledd, för sådan materiell skada som denne har lidit och som har förorsakats av dennes befogade förlitan på den missvisande informationen.

Restatement, § 525. En information lämnas "i bedrägligt syfte" (fraudulent) om den lämnas i vetskap om eller i tro att den är falsk, *idem*, § 526. Som allmän regel gäller att den som informerar i bedrägligt syfte kan hållas skadeståndsansvarig gentemot alla som han tänker sig eller förväntar sig ska lita på den missvisande informationen för all materiell skada som de kan drabbas av på grund av den, *idem*, § 531. Vidare kan en part som lämnat missvisande information i bedrägligt syfte hållas ansvarig gentemot en tredje part om den felande parten tänkte sig eller förväntade sig att den missvisande informationen skulle kunna upprepas och förmå en tredje part att handla, *idem*, § 533.

När det gäller *safe harbor* är den relevanta informationen organisationens offentliga försäkran att den kommer att följa *safe harbor*-principerna. Efter ett sådant åtagande kan medveten underlåtenhet att iaktta dessa principer vara skälig grund för dem som litade på informationen att väcka talan om missvisande information. Eftersom åtagandet görs till allmänheten i stort har både de enskilda som informationen riktar sig till och den registeransvarige i Europa som överför uppgifter till den amerikanska organisationen grund för talan mot denna organisation om missledande information [2]. Vidare förblir den amerikanska organisationen skadeståndsansvarig för "fortgående missvisande information", så länge de fortsätter att lita på den missvisande informationen och detta skadar dem. Restatement, § 535.

---

[1] Second Restatement of the Law – Torts; American Law Institute (1997).

[2] Detta kan t.ex. vara fallet om de enskilda förlitade sig på den amerikanska organisationens *safe harbor*-åtagande när de godkände att den registeransvarige överförde personuppgifter till Förenta staterna.

De som litar på missvisande information som lämnats i bedrägligt syfte har rätt till skadestånd. Enligt Restatement gäller följande:

> Den som mottar missvisande information som lämnats i bedrägligt syfte har rätt att genom ett bedrägerimål mot förövaren erhålla skadestånd som svarar mot den materiella skada som han har lidit och som kan hänföras till den missvisande informationen.

Restatement, § 549. Som skada räknas rena utlägg samt utebliven ”förtjänst på bra affär” i en handelstransaktion. Idem, se t.ex. Boling mot Tennessee State Bank, 890 S.W.2d 32 (1994) (banken dömdes att betala 14 825 US-dollar i skadestånd till låntagare för att ha avslöjat låntagarnas personuppgifter och affärsplaner för bankens ordförande som hade motsatta intressen).

För missvisande information i bedrägligt syfte krävs vetskap om eller åtminstone ett antagande om att information är falsk. Men skadestånd kan också utdömas för missvisande information på grund av försumlighet. Enligt Restatement kan den som lämnar felaktig information i egenskap av näringsidkare, yrkesutövare eller anställd eller i samband med någon penningtransaktion dömas till skadestånd ”om han inhämtar eller lämnar ut information utan tillbörlig noggrannhet eller skicklighet”. Restatement, § 552(1). Till skillnad från vad som gäller när syftet är bedrägligt, kan skadestånd vid försumligt hanterad information bara utgå för rena utlägg, *idem*, § 552B(1).

I ett nyligen avgjort fall biföll högsta domstolen in Connecticut talan om missvisande information när en elfirma hade låtit bli att informera om hur kundfordringar rapporterades till nationella kreditupplysningsföretag. Se Brouillard mot United Illuminating Co., 1999 Conn. Super. LEXIS 1754. I detta fall fick käranden avslag på en låneansökan därför att svaranden rapporterade fordringar som ”betalningsförseningar” 30 dagar efter faktureringsdagen. Käranden hävdade att han inte hade informeras om detta när han öppnade ett bostadselkonto hos svaranden. Domstolen angav särskilt att ”ett yrkande om missvisande information på grund av försumlighet kan baseras på svarandens underlåtenhet att tala när han är skyldig att göra det”. Detta fall visar också att bedrägligt uppsåt inte är någon nödvändig komponent i talan om försumlig informationshantering. Om en organisation av försumlighet underlåter att redovisa öppet hur den kommer att använda personuppgifter som den erhållit inom ramen för sitt *safe harbor*-åtagande kan den således hållas ansvarig för missvisande information.

Om ett brott mot *safe harbor*-principerna skulle innebära att personuppgifter missbrukades, hade den registrerade med stöd av rättspraxis kunnat stämma för integritetskränkning. Sedan lång tid tillbaka erkänner det amerikanska rättssystemet integritetskränkning som grund för talan. I ett fall från 1905 ([3]) ansåg högsta domstolen i Georgia att en rätt till personlig integritet grundad i naturrätt och rättspraxis gällde för en enskild medborgare när ett försäkringsbolag, utan medgivande eller vetskap från den berörde, hade använt ett foto av denne i en annons. Domstolen gav uttryck för numera väletablerade värderingar i amerikansk rättspraxis när den bedömde sättet att använda fotografiet som ”illasinnat”, ”falskt” och avsett att ”göra käranden löjlig inför omvärlden” ([4]). Skälen för Pavesich-beslutet har bestått med smärre variationer och är nu den fasta grund som amerikansk rätt vilar på. Domstolarna i delstaterna har systematiskt godkänt talan om integritetskränkning, och rättspraxis i minst 48 delstater godkänner idag någon slags talan av den typen ([5]) Vidare har minst 12 delstater bestämmelser i författningen som skyddar medborgarens rätt att slippa intrång ([6]), vilket i vissa fall även kan omfatta skydd mot intrång från organ som inte är statliga. Se t.ex. Hill mot NCAA, 865 P.2d 633 (Ca. 1994); se även S. Ginder, Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet, 34 S.D. L. Rev. 1153 (1997) (”Vissa författningar på delstatsnivå omfattar integritetsskydd som går längre än integritetsskyddet i Förenta staternas konstitution. Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina och Washington har ett mera vittgående integritetsskydd”).

I Second Restatement of Torts finns en auktoritativ översikt över rättstillämpningen på området. Där anges att enligt rättspraxis omfattar ”rätten till personlig integritet” (right to privacy) fyra distinkta grunder för talan. Se Restatement, § 652 A. För det första kan ”intrång i privatlivet” (intrusion upon seclusion) vara grund för talan mot någon som avsiktligt, fysiskt eller på något annat sätt, tränger sig på när någon annan valt avskildhet eller ensamhet, eller blandar sig i

([3]) Pavesich mot New England Life Ins. Co., 50 S.E. 68/Ga. 1905).

([4]) Idem 69.

([5]) En sökning i databasen Westlaw gav 2 703 civilrättsliga fall i delstatsdomstolar på området personlig integritet sedan 1995. Vi har tidigare lämnat resultaten av sökningen till kommissionen.

([6]) Se t.ex. Alaskas konstitution, artikel 1.22; Arizona, artikel 2.8; Kalifornien, artikel 1.1; Florida, artikel 1.23; Hawaii, artikel 1.5; Illinois, artikel 1.6; Louisiana, artikel 1.5; Montana, artikel 2.10; New York, artikel 1.12; Pennsylvania, artikel 1.1; South Carolina, artikel 1.10 samt Washington, artikel 1.7.

dennes privata affärer eller angelägenheter ([7]). För det andra kan man stämma för ”personintrång” (appropriation) om någon lägger sig till med en annans namn eller utseende och använder det för egna syften eller egen vinning ([8]). För det tredje finns ”publicering av privata uppgifter” (publication of private facts) som gäller som grund för talan när publicerat material är mycket stötande för en omdömesgill person och saknar intresse för allmänheten ([9]) Slutligen kan man stödja sig på ”publicitet i falsk belysning” (false light publicity) när svaranden avsiktlig eller tanklöst exponerar någon offentligt i falsk belysning på ett sätt som hade varit mycket stötande för en omdömesgill person ([10]).

Mot bakgrund av *safe harbor*-principerna skulle ”intrång i privatlivet” kunna omfatta otillåten insamling av personuppgifter, medan otillåten användning av personuppgifter för affärer skulle kunna vara grund för talan om personintrång. På samma sätt skulle spridning av personuppgifter som är felaktiga kunna leda till talan om ”publicitet i falsk beslysning”, om uppgifterna uppfyller villkoret att vara mycket stötande för en omdömesgill person. Slutligen skulle in integritetskränkning som beror på att känslig information publicerats eller avslöjats kunna vara grund för talan om ”publicering av privata uppgifter”. (Se belysande exempel på fall nedan.)

När det gäller skadestånd ger integritetskränkningar den skadelidande rätt att erhålla skadestånd för

a) skada till följd av kränkningen på den skadelidandes intresse av personlig integritet

b) psykiskt lidande som han bevisligen utstått, om det är en normal reaktion på den aktuella kränkningen,

c) särskild skada som kan hänföras till kränkningen.

Restatement, § 652H. Eftersom skadeståndsrättsliga regler (tort law) är allmänt tillämpliga och det finns så många olika grunder för talan om integritetsfrågor, är det troligt att de som drabbas av integritetskränkningar på grund av underlåtenhet att iaktta *safe harbor*-principer kommer att kunna begära skadestånd i pengar.

Domstolarna i delstaterna handlägger många fall där integritetskränkning hävdas föreligga i liknande situationer. *Ex parte* AmSouth Bancorporation *et al.*, 717 So. 2d 357 gällde t.ex. en grupptalan (class action) där det hävdades att svaranden ”utnyttjade fondmedel som var placerade i banken genom att lämna ut sekretessbelagd information om spararna och deras konton” till en dotterbank, så att den kunde sälja fonder och andra investeringsobjekt. Skadestånd utgår ofta i sådana här fall. I Vassiliades mot Garfinckel's, Brooks Bros., 492 A.2d 580 (D.C. App. 1985), ändrade en appellationsdomstol en lägre domstols dom och beslutade att fotografier av käranden ”före” och ”efter” en plastikoperation när de visades i ett varuhus utgjorde en integritetskränkning genom att privata uppgifter av slöjades. I Candebat mot Flanagan, 487 So.2d 207 (Miss. 1986), använde det svarande försäkringsbolaget en olycka, i vilken kärandens fru skadades allvarligt, i en reklamkampanj. Käranden stämde för integritetskränkning. Domstolen gav käranden rätt till skadestånd för känslomässigt lidande och personintrång. Talan om personintrång kan väckas även om käranden inte är berömd. Se t.ex. Staruski mot Continental Telephone Co., 154 Vt. 568 (1990) (svaranden drog affärsmässig nytta av att använda den anställdes namn och fotografi i en tidningsannons). I Pulla mot Amoco Oil Co., 882 F.Supp. 836 (S.D. Iowa 1995), gjorde en arbetsgivare intrång i den anställdes privatliv genom att låta en annan anställd undersöka hans kortbetalningar för att kontrollera hans sjukfrånvaro. Domstolen beslutade om jurytilldelning på 2 dollar i faktiskt skadestånd och 500 000 dollar i straffskadestånd. En annan arbetsgivare dömdes till skadestånd för att ha publicerat ett reportage i företagstidningen om en anställd som fick avsked för att han enligt uppgift hade förfalskat sin meritförteckning. Se Zinda mot Louisiana-Paficic Corp., 140 Wis.2d 277)(Wis. App. 1987). Reportaget var en kränkning av kärandens integritet genom publiceringen av privata uppgifter, eftersom tidningen spreds i samhället. En skola som HIV-testade studenter efter att ha uppgett att blodprovet bara var för röda hund dömdes slutligen till skadestånd för intrång i privatlivet. Se Doe mot High-Tech Institute, Inc., 972 P.2d 1060 (Colo.App. 1998). (För övriga återgivna fall, se Restatement, § 652H, bilaga.)

USA får ofta kritik för att konflikter alltför ofta löses i domstol, men detta betyder också att enskilda faktiskt kan gå till doms, och gör det, när de anser sig kränkta. Det amerikanska rättssystemet gör det på många sätt lätt för käranden att

([7]) Idem, kapitel 28, avsnitt 652B.
([8]) Idem, kapitel 28, avsnitt 652C.
([9]) Idem, kapitel 28, avsnitt 652D.
([10]) Idem, kapitel 28, avsnitt 652 E.

föra sin talan, antingen som enskild eller i grupp. Advokatkåren, som är förhållandevis större än i de flesta andra länder, erbjuder lättillgänglig och yrkeskunnig hjälp. Biträden som företräder enskilda käranden i civilmål arbetar normalt mot ersättning i procent av eventuellt skadestånd, vilket innebär att även fattiga kärande kan söka upprättelse. Detta leder fram till en viktig punkt: I USA bär varje sida normalt sina egna kostnader för advokater eller annat. Detta står i kontrast till vad som generellt gäller i Europa där den tappande parten måste ersätta den andra sidans kostnader. Utan att gå in på för- eller nackdelar med dessa två system är det mindre risk att det amerikanska systemet avskräcker en enskild från att driva en rättsak för att han inte skulle kunna betala båda sidors kostnader om han förlorade.

Enskilda kan driva sin sak inför rätta även om tvisten rör små summor. De flesta, eller kanska alla, amerikanska domsagor har domstolar som handlägger smärre mål enligt enkla och biliga förfaranden för tvister om värden under lagstadgade gränser ([11]) Möjligheten att utdöma straffskadestånd ger också ett ekonomiskt incitament åt enskilda, som kanske lidit liten skada, att föra klandervärda handlingar inför rätta. Slutligen kan enskilda som drabbats på samma sätt samordna sina resurser och krav i en rättegång med grupptalan.

Ett bra exempel på enskildas möjligheter att ansöka om stämning för att få upprättelse är den pågående rättegången mot Amazon.com för integritetskränkning. Amazon.com, den stora nätbutiken, är föremål för talan från en grupp som hävdar att de inte fick reda på, och inte samtyckte till att personuppgifter samlades in om dem när de använde en programvara som Amazon äger och som heter ”Alexa”. I detta fall åberopar de kärande brott mot Lagen om datorbedrägeri (Computer Fraud and Abuse Act) genom olaglig tillgång till deras lagrade meddelanden och mot Lagen om elektronisk brevhemlighet (Electronic Communications Privacy Act) genom olaglig avlyssning av deras dator- eller kabelförmedlade meddelanden. De hävdar också att de utsatts för en integritetskränkning enligt rättspraxis. Stämningsansökan lämnades ursprungligen in i december av en expert på Internetsäkerhet. I ansökan yrkas 1 000 dollar i skadestånd per gruppmedlem samt advokatarvode och vinsten på lagbrotten. Eftersom miljontals personer kan ingå i gruppen kan skadeståndet bli på flera miljarder dollar. FTC (Federal Trade Commission) utreder också anklagelserna.

Integritetslagstiftningen på federal nivå och på delstatsnivå ger ofta grund för civilrättslig talan om kontant skadestånd.

Safe harbor-principerna ger inte bara upphov till skadeståndsansvar enligt skadeståndsrättsliga regler (tort law), underlåtenhet att iaktta principerna kan också vara ett brott mot någon av hundratals lagar om integritetsskydd på federal nivå eller delstatsnivå. Många av dessa lagar, som gäller både offentlig och privat hantering av personuppgifter, ger den enskilde rätt att stämma och kräva skadestånd om de överträds. Till exempel:

ECPA, Lagen om elektronisk brevhemlighet, 1986 (Electronic Communications Privacy Act). Enligt ECPA är det förbjudet att utan tillåtelse avlyssna mobiltelefonsamtal och överföringar mellan datorer. En överträdelse kan leda till skadestånd på inte mindre än 100 dollar per dag som överträdelsen består. Skyddet i kraft av ECPA omfattar också att utan tillåtelse ha tillgång till eller avslöja lagrade elektroniska meddelanden. Överträdaren kan dömas att ersätta den uppkomna skadan eller att avstå den vinst överträdelsen skapade.

Lagen om telekommunikationer, 1996 (Telecommunications Act). Enligt avsnitt 702 får privata uppgifter om kundens nätanvändning (customer proprietary network information), CPNI, inte användas för något annat ändamål än att tillhandahålla teletjänster. Drabbade abonnenter kan antingen lämna ett klagomål till Federal Communications Commission eller lämna in en stämningsansökan i en federal underrätt och kräva skadestånd och ersättning för advokatkostnader.

Lagen om ändring av bestämmelser om konsumentkreditrapportering, 1996 (Consumer Credit Reporting Reform Act). Lagen från 1996 ändrar Lagen om rättvis kreditrapportering (Fair Credit Reporting Act) från 1970, FCRA, i syfte att ge de registrerade bättre information och informationstillgång. Ändringsförfattningen innehåller också nya krav på dem som säljer registerutdrag om konsumentkrediter. I händelse av överträdelse kan konsumenter kräva skadestånd och ersättning för advokatkostnader.

([11]) Vi har tidigare gett kommissionen information om handläggning av små mål.

Även på delstatsnivå finns det lagar som ger integritetsskydd i ett brett register av situationer. Bland de områden där delstaterna har lagstiftat återfinns bankregister, kabelteveabonnemang, kreditregister, personalregister, offentliga register, genetisk information och patientjournaler, försäkringsregister, skolbetyg, elektroniska meddelanden och register över videouthyrning ([12]).

B. **Uttryckliga befogenheter i lag**

Safe-harbor-principerna innehåller ett undantag när lagar och andra författningar eller rättspraxis skapar ”motstridiga skyldigheter eller uttryckliga befogenheter, förutsatt att organisationen då den utövar dessa befogenheter kan visa att avvikelsen från principerna begränsar sig till vad som är nödvändigt för att de övergripande legitima intressen som är beroende av dessa befogenheter skall kunna tillgodoses”. Självklart måste amerikanska organisationer, om de i amerikansk lag har en motstridig skyldighet, oberoende av om de anslutit sig till *safe harbor* eller inte, följa lagen. Vad gäller uttryckliga befogenheter, så är målsättningen med *safe harbor* att överbrygga skillnaderna mellan det amerikanska och det europeiska sättet att hantera integritetsskydd, men vi måste respektera den lagstiftande makt våra valda politiska ombud har. Detta smärre undantag från strikt iakttagande av *safe harbor*-principerna är ett försök att hitta en lämplig balansgång mellan berättigade intressen på båda sidor.

Undantaget inskränker sig till att gälla när det finns uttryckliga befogenheter. Som minsta gemensam nämnare måste därför den relevanta texten (lag, annan författning eller domstolsbeslut) uttryckligen tillåta *safe harbor*-organisationer att utföra den aktuella handlingen ([13]). Med andra ord kan undantaget inte göras gällande om det inte står något i lagen. Vidare kan undantaget bara gälla om de uttryckliga befogenheterna står i strid med *safe harbor*-principerna. Även i detta fall skall undantaget begränsas ”till vad som är nödvändigt för att de övergripande legitima intressen som är beroende av dessa befogenheter skall kunna tillgodoses”. Exempelvis skulle undantaget inte gälla om lagen bara tillåter ett företag att lämna ut personuppgifter till statliga organ. Om lagen å andra sidan särskilt tillåter företaget att lämna personuppgifter till statliga organ utan den enskildes samtycke, så är detta en ”uttrycklig befogenhet” att agera på ett sätt som strider mot *safe harbor*-principerna. Alternativt kommer särskilda undantag från uttryckliga krav på meddelande och samtycke att omfattas av undantaget (eftersom det är samma sak som en särskild tillåtelse att avslöja informationen utan meddelande och samtycke). Till exempel skulle en lagparagraf som tillåter läkare att lämna ut patientjournaler till hälsovårdsmyndigheter utan föregående samtycke från patienterna kunna motivera ett undantag från principen om meddelande och valmöjlighet. Denna tillåtelse hade inte inneburit att läkaren fått rätt att lämna ut patientjournaler till friskvårdsorganisationer eller affärsdrivande laboratorier för läkemedelsforskning, vilka hade legat utanför räckvidden för den lagstadgade tillåtelsens ändamål och därför utanför undantagets räckvidd ([14]). Den aktuella rättsliga grunden kan vara en ”isolerad” tillåtelse att göra vissa saker med personuppgifter, men, vilket framgår av exemplen nedan, är förmodligen ett undantag från en bredare lag som förbjuder insamling, användning eller spridning av personuppgifter.

Lagen om telekommunikationer, 1996

För det mesta är den tillåtna användningen i överensstämmelse med kraven i direktivet och i principerna, eller hade tillåtits i kraft av något av de andra tillåtna undantagen. Till exempel har teleoperatörer enligt avsnitt 702 i Lagen om telekommunikationer (kodifiering: 47 U.S.C. § 222) tystnadsplikt när det gäller personuppifter som de tar emot i samband med sin tjänsteverksamhet. I bestämmelsen tillåts teleoperatörer särskilt att

1) använda kunduppgifter för att erbjuda teletjänster, särskilt telefonkataloger,

2) lämna kunduppgifter till andra på skriftlig begäran från kunden och

3) lämna ut kunduppgifter i form av aggregat.

([12]) En nyligen genomförd sökning i Westlawdatabasen gav 994 fall på delstatsnivå med koppling till skadestånd och integritetskränkning.

([13]) I klargörande syfte kan nämnas att det inte krävs att rättsmyndigheten hänvisar särskilt till *safe harbor*-principerna.

([14]) På samma sätt hade läkaren i exemplet inte kunnat räkna med att lagen undanröjde den enskildes rätt att välja bort direkt marknadsföring enligt FoS 12 Räckvidden för ett undantag för ”uttryckliga befogenheter” kan aldrig gå utanför räckvidden för tillåtelsen i den aktuella lagen.

Se 47 U.S.C. § 222(c)(1)–(3). Lagen medger också teleoperatörerna undantag från förbudet att använda kunduppgifter när det gäller att

1) initiera, tillhandahålla, fakturera och ta betalt för tjänster,

2) skydda mot bedrägeri, missbruk eller olagligt bruk samt

3) lämna produktinformation, hänvisnings- eller upplysningstjänster under ett anrop som kunden har tagit initiativ till ([15]).

Idem, § 222(d)(1)–(3). Slutligen är teleoperatörer skyldiga att lämna listor med abonnentuppgifter, vilka endast får omfatta namn, adress, telefonnummer och bransch om det är en företagskund, till förlag som ger ut telefonkataloger. *Idem*, § 222(e).

Undantaget för ”uttryckliga befogenheter” kan få betydelse när teleoperatörer använder CPNI för att motverka bedrägeri eller olagliga handlingar. Också i detta fall skulle man kunna hävda att det rör sig om åtgärder i det allmännas intresse som således är tillåtna enligt principerna.

Regler som föreslagits av ministeriet för omsorg och vård

Ministeriet för hälso- och människovård (Department of Health and Human Services), HHS, har föreslagit regler när det gäller integritetsskydd för individuellt identifieringsbara uppgifter om människors hälsa. Se 64 Fed. Reg. 59,918 (Nov. 3, 1999) (kommande kodifiering: 45 C.F.R. punkterna (160–164). Reglerna innebär en tillämpning av integritetskraven i Lagen om rätt till sjukförsäkring och ersättning (Health Insurance Portability and Accountability Act), 1996, Pub. L. 104–191. I korthet går de föreslagna reglerna ut på att förbjuda alla enheter som omfattas (dvs. sjukkassor, clearinginstanser och sjukvårdsproducenter som hanterar hälsouppgifter i elektroniskt format) från att använda eller avslöja några skyddade hälsouppgifter utan föregående tillåtelse. Se förslag till 45 C.F.R. § 164.506. Enligt förslaget skulle skyddade hälsouppgifter bara få lämnas ut för två ändamål: 1) tillåta enskilda att kontrollera och kopiera hälsouppgifter om sig själva, se *idem*, § 164.514, och 2) övervaka att reglerna tillämpas, se *idem*, § 164.522.

De föreslagna reglerna skulle tillåta att skyddade hälsouppgifter användes eller lämnades ut, utan särskild tillåtelse från den registrerade, i ett begränsat antal fall. Dessa omfattar till exempel reform av sjukförsäkringssystemet, brottsbekämpning och nödlägen. Se *idem*, § 164.510. Reglerna specificerar noggrant var gränserna för tillåten användning och spridning går. Vidare skulle tillåten användning och spridning av skyddade hälsouppgifter begränsas till det minsta antal som krävs. Se *idem* § 164.506.

När särskild användning uttryckligen tillåts enligt de föreslagna reglerna är detta i allmänhet förenligt med *safe harbor*-principerna eller tillåtet i kraft av något annat undantag. Till exempel är brottsbekämpning och rättsvård tillåtna användningar, liksom även medicinsk forskning. Andra användningsområden, såsom reform av sjukförsäkringssystemet, offentlig sjukvård och centrala sjukvårdsdatasystem, tjänar allmänintresset. Betalningar och premier i samband med sjukvård kräver vissa uppgifter som måste lämnas ut för att det skall gå att tillhandahålla sjukvård. I nödlägen, när man behöver rådgöra med nära anhöriga för att patientens samtycke ”inte kan inhämtas på ett praktiskt eller rimligt sätt”, eller när man måste fastställa identitet eller dödsorsak för en avliden, skyddar man vitala intressen för den registrerade och andra. Användningar som rör hanteringen av militärer i aktiv tjänst eller andra särskilda grupper av enskilda gör det lättare att utföra militära uppdrag och andra krävande uppgifter på ett riktigt sätt; för övrigt har denna typ av användning liten eller ingen tillämpning på konsumenter i allmänhet.

Återstår endast användning av personuppgifter inom hälso- och sjukvården för att sammanställa patientkataloger. Det rör sig kanske inte om något ”vitalt” intresse, men katalogerna är till nytta för patienterna, deras vänner och anhöriga.

([15]) Detta undantag har mycket begränsad räckvidd. Enligt vad som står får teleoperatören bara använda CPNI under ett anrop från kunden. Vidare har FCC informerat oss om att teleoperatören inte får använda CPNI för att marknadsföra andra tjänster än dem kunden frågar om. Eftersom kunden slutligen måste godkänna att CPNI används på detta sätt, är bestämmelsen egentligen inte något undantag alls.

Vidare är räckvidden för denna tillåta användning av naturliga skäl begränsad. Därför utgör undantaget i principerna för ”uttryckliga befogenheter” i lag för detta ändamål en minimal integritetsrisk för patienterna.

FCRA, Lagen om rättvis kreditrapportering (Fair Credit Reporting Act)

Europeiska kommissionen undrar om undantaget för ”uttryckliga befogenheter” skulle kunna ”i praktiken ge ett konstaterande om adekvat” skydd för FCRA. Detta kan inte inträffa. Om det saknas beslut om adekvat skyddsnivå för FCRA, måste amerikanska organisationer som annars hade förlitat sig på ett sådant beslut åta sig att iaktta *safe harbor*-principerna på alla sätt. Detta innebär att om FCRA-kraven går längre än skyddet enligt principerna räcker det att amerikanska organisationer följer FCRA. I motsatt fall, om FCRA ger ett sämre skydd, måste dessa organisationer göra sina rutiner för uppgiftsbehandling förenliga med principerna. Undantaget ändrar inte på denna grundsats. Enligt undantaget kan det bara tillämpas när en handling som strider mot *safe habor*-principerna uttryckligen tillåts i den relevanta lagen. Undantaget täcker inte situationer där FCRA-krav helt enkelt kommer till korta jämfört med *safe harbor*-principerna ([16]).

Med andra ord är det inte meningen att undantaget skall uppfattas som att allt som inte krävs är ”uttryckligen tillåtet”. Dessutom gäller undantaget bara när sådant som är uttryckligen tillåtet i amerikansk lag strider mot kraven i *safe harbor*-principerna. Den relevanta lagen måste uppfylla bägge dessa kriterier för att det ska vara tillåtet att bryta mot principerna.

Avsnitt 604 i FCRA innehåller till exempel en uttrycklig tillåtelse för kreditupplysningsföretag att lämna upplysningar om konsumenter i olika särskilt angivna situationer. Se FCRA, § 604. Om avsnitt 604 därmed tillåter kreditupplysningsföretagen att agera i strid med *safe harbor*-principerna, så måste de göra det i kraft av undantaget (såvida inte något annat undantag gäller naturligtvis). Kreditupplysningsföretagen måste lyda domstolsbeslut och beslut från undersökningskommissioner (grand jury subponeas), och när kreditupplysningar används av tillståndsmyndigheter, sociala myndigheter och myndigheter som driver in underhåll till barn rör det sig om ett allmänt intresse. *Idem*, § 604(a)(1), (3)(D). Följaktligen behöver kreditupplysningsföretagen inte förlita sig på undantaget för ”uttryckliga befogenheter” i dessa fall. När kreditupplysningsföretaget agerar enligt skrivna instruktioner från konsumenten följer det *safe harbor*-principerna helt och fullt. *Idem*, § 604(a)(2). På samma sätt kan kreditupplysningar bara lämnas ut för anställningsändamål om konsumenten har lämnat en skriftlig tillåtelse (*idem*, § 604(a)(3)(B) och § 604(b)(2)(A)(ii); för kredit- eller försäkringstransaktioner utan inledande konsumentinitiativ bara om konsumenten inte valt bort sådan marknadsföring (*idem*, § 604(c)(1)(B). I FCRA förbjuds vidare kreditupplysningsföretagen att lämna hälsoupplysningar för anställningsändamål utan konsumentens samtycke. *Idem*, § 604(g). Sådan användning är förenlig med principen om meddelande och valmöjlighet. Andra ändamål som tilllåts enligt avsnitt 604 leder till transaktioner som konsumenten deltar i och hade tillåtits av principerna av den anledningen. Se *idem* § 604(a)(3)(A) och (F).

Den användning som för övrigt ”tillåts” i avsnitt 604 gäller kreditmarknader i andra hand. *Idem*, § 604(a)(3)(E). Det finns här i sig ingen konflikt mellan användning av upplysningar om konsumenter och *safe harbor*-principerna. Det är riktigt att FCRA inte kräver att till exempel kreditupplysningsföretag skall meddela konsumenterna och inhämta deras samtycke när de lämnar upplysningar för dessa ändamål. Men vi vill erinra om att avsaknad av krav inte betyder ”uttryckliga befogenheter” att handla på ett annat sätt än vad som anges. På samma sätt får kreditupplysningsföretag enligt avsnitt 608 lämna personuppgifter till statliga organ. Denna befogenhet innebär inte att ett kreditupplysningsföretag kan avstå från att iaktta sitt åtagande att följa *safe harbor*-principerna. Detta står i kontrast mot våra tidigare exempel där undantag från krav på meddelande och valmöjlighet innebär att det är uttryckligen tillåtet att använda personuppgifter utan meddelande och valmöjlighet.

Slutsats

Även efter denna begränsade översikt över lagstiftningen framträder följande tydliga mönster:

— De ”uttryckliga befogenheterna” i lagen innebär i allmänhet en tillåtelse att använda eller lämna ut personuppgifter utan den enskildes föregående samtycke; därmed begränsas undantaget till att gälla principen om meddelande och valmöjlighet.

([16]) Vår framställning på denna punkt skall inte tas som intäkt för att FCRA inte skulle ge ”adekvat” skydd. En bedömning av FCRA måste se till det skydd hela lagen ger och inte inriktas uteslutande på undantagen som vi gör här.

— För det mesta är de lagstadgade undantagen snävt utformade så att de passar i särskilda situationer för särskilda ändamål. För övrigt gäller generellt lagstadgat förbud mot otillåten användning eller spridning av personuppgifter som inte faller inom dessa ramar.

— För det mesta, vilket speglar lagstiftningens ändamål, ligger den tillåtna användningen eller spridningen i det allmännas intresse.

— Nästan alltid är den tillåtna användningen förenlig med *safe harbor*-principerna eller sammanfaller med något annat tillåtet undantag.

Sammanfattningsvis kommer undantaget för ”uttryckliga befogenheter” i lagen förmodligen att få ganska begränsad räckvidd, på grund av sina inneboende drag.

C. **Fusioner och övertag**

Artikel 29-arbetsgruppen uttrycker farhågor för vad som händer när en *safe harbor*-organisation köps upp av eller går samman med ett företag som inte har åtagit sig att följa *safe harbor*-principerna. Arbetsgruppen tycks förutsätta att det kvarvarande företaget inte är bundet att tillämpa *safe harbor*-principerna på personuppgifter i det företag som tas över, men detta är inte nödvändigtvis fallet enligt amerikansk lag. Den allmänna regeln i USA när det gäller fusioner och övertag är att när ett företag köper återstående aktier i ett annat företag, så tar det som regel över detta företags skyldigheter och åtaganden. Se 15 Fletcher Cyclopedia of the law of Private Corporations § 7117 (1990), se också Model Bus. Corp. Act § 11.06(3) (1979) (”det kvarvarande företaget tar över alla åtaganden från varje företag som är part i fusionen”). Med andra ord blir det kvarvarande företaget efter en fusion eller ett övertag som gäller en *safe harbor*-organisation enligt denna princip bundet att iaktta det övertagna företagets *safe harbor*-åtagande.

Även om fusioner eller övertagandet gjordes genom uppköp av tillgångar, skulle det uppköpta företaget i alla fall binda det uppköpande under vissa omständigheter. 15 Fletcher, § 7122. Och i sådana fall där åtagandena inte hade överlevt fusionen, hade de heller inte överlevt en fusion efter uppgiftsöverföring från Europa på kontraktsbasis, vilket är det enda trovärdiga alternativet till *safe harbor* för uppgiftsöverföring till USA. Vidare gäller enligt de omarbetade *safe harbor*-handlingarna att *safe habor*-organisationer skall underrätta Förenta staternas handelsministerium om övertag samt att uppgifterna endast fortsatt får överföras till den nya organisationen om denna efterföljare ansluter sig till *safe harbor*. Se FoS 6. USA har t.o.m. arbetat om *safe harbor*-principerna, så att amerikanska organisationer i denna situation kommer att tvingas att radera uppgifter de erhållit inom ramen för *safe harbor* om *safe harbor*-åtagandet inte kommer att bestå eller andra lämpliga skyddsåtgärder vidtas.

BILAGA V

14 juli 2000

John Mogg
Direktör, GD XV
Europeiska kommissionen
Kontor C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Bryssel

Herr generaldirektör,

Jag förstår att min skrivelse till Er av den 29 mars 2000 gav upphov till många frågor. Denna skrivelse skickar jag för att klargöra vad vi har för befogenheter på de områden som frågorna gäller, men, för att underlätta framtida hänvisning, bygger den också vidare på och tar till viss del om stycken ur tidigare skriftväxling.

Under Era besök på vårt kontor och i Era skrivelser har Ni ställt många frågor om de befogenheter Federal Trade Commission (FTC) har över integritetsskydd i webbmiljö. Det förefaller lämpligt att börja med ett sammandrag av mina tidigare svar samt ge ytterligare information om FTC:s befogenheter när det gäller de frågor om integritetsskydd för konsumenter som Ni tog upp i Er senaste skrivelse. Ni frågar närmare bestämt om 1. FTC har befogenhet när överföring av personuppgifter om anställda sker i strid mot principerna om *safe harbor*, 2. FTC har befogenhet över ideell integritetsmärkning, 3. Federal Trade Commission Act gäller både utanför webbmiljön och i webbmiljö samt 4. vad som händer när FTC:s behörighetsområde överlappar andra rättsskipande instansers.

Tillämpningen av Federal Trade Commission Act på integritetsskydd

På detta område stödjer sig FTC juridiskt på avsnitt 5 i Federal Trade Commission Act som innehåller ett förbud mot ”illojala eller bedrägliga handlingar eller metoder” i eller som påverkar handel ([1]). En bedräglig metod definieras som en handling, ett utelämnande eller en metod som antas kunna vilseleda förnuftiga konsumenter på ett konkret sätt. En metod är illojal om den framkallar, eller kan antas framkalla, väsentlig skada för konsumenter och skadan varken går att undvika på ett rimligt sätt eller uppvägs av fördelar för konsumenterna eller för konkurrensen ([2]).

Vissa metoder för att inhämta information är sannolikt ett brott mot Federal Trade Commission Act. Om det t.ex. felaktigt hävdas att en webbplats är förenlig med en angiven integritetsskyddspolicy eller ett antal självregleringsnormer ger avsnitt 5 i Federal Trade Commission Act en rättslig grund för att beivra sådan felaktig information såsom bedräglig. Vi har faktiskt lyckats med att tillämpa lagen så att denna princip förankrats ([3]). Vidare tillämpar FTC förhållningssättet att särskilt uppenbara integritetskränkande metoder kan beivras med hänvisning till att de är illojala enligt avsnitt 5 när de riktas mot barn eller innebär att särskilt känslig information, t.ex. ekonomisk ([4]) eller medicinsk information, utnyttas. FTC har bedrivit och kommer även fortsättningsvis att bedriva denna typ av rättsskipande verksamhet med hjälp av ett aktivt övervaknings- och utredningsarbete, samt med hjälp av fall som självregleringsorgan eller andra, även EU-länder, remitterar till FTC.

([1]) 15 U.S.C. § 45. Lagen Fair Credit Reporting Act torde också vara tillämplig på inhämtning och försäljning av Internetdata som svarar mot den lagstadgade definitionen av konsumentrapport (consumer report) och konsumentrapportinstans (consumer reporting agency).

([2]) 15 U.S.C. § 45(n).

([3]) Se GeoCities, Docket No. C-3849 (Slutligt beslut den 12 februari 1999) (Internetadress: http://www.ftc.gov/os/1999/9902/9823015d%26o.htm); Liberty Financial Cos., Docket No. C-3891 (Slutligt beslut den 12 augusti 1999) (Internetadress: http://www.ftc.gov/opa/1999/9905/younginvestor.htm). Se även COPPA (Children's Online Privacy Protection Act Rule), 16 C.F.R. Del 312 (Internetadress http://www.ftc.gov/opa/1999/9910/childfinal.htm). Enligt COPPA-reglerna, som trädde i kraft förra månaden, skall företag som har webbplatser inriktade på barn under 13, eller som vet att de inhämtar personuppgifter från barn under 13, tillämpa COPPA-reglerna om sunda informationsmetoder.

([4]) Se FTC mot Touch Tone, Inc., civilmål nr 99-WM-783 (D.Co) (registrerat den 21 april 1999), Internetadress: http://www.ftc.gov/opa/1999/9904/touchtone.htm. Skrivelse (Staff Opinion Letter) den 17 juli 1997 som svar på en inlaga från Center för Media Education, Internetadress: http://www.ftc.gov/os/1997/9707/cenmed.htm.

Stöd till självreglering

FTC kommer att prioritera fall som kommer från sådana organisationer som BBBOnline och TRUSTe och som gäller underlåtenhet att följa självregleringsnormer ([5]). Detta är ett arbetssätt som ligger i linje med vårt väletablerade samarbete med National Advertising Review Board (NARB) på Better Business Bureau, varifrån FTC tar emot klagomål mot reklam. National Advertising Division (NAD) på NARB avgör klagomål, genom ett beslutsförfarande, som rör reklam på nationell nivå. Om en part vägnar att följa ett NAD-beslut, överlämnas fallet till FTC. På FTC får fallet förtur och den lagförda reklamen granskas så att man kan avgöra om den bryter mot Federal Trade Commission Act. FTC lyckas ofta med att sätta stopp för den lagförda metoden eller med att återföra parten till NARB-förfarandet.

På samma sätt kommer FTC att prioritera fall som kommer från EU-länderna och som gäller underlåtenhet att följa *safe-harbor*-principerna. Precis som när fallen kommer från självregleringsorgan i USA kommer personalen på FTC att undersöka alla uppgifter som rör frågan om huruvida de handlingar klagomålet gäller är ett brott mot Federal Trade Commission Act. Detta åtagande finns också i *safe harbor*-principerna i Frågor och svar (FoS 11) om genomförande och uppföljning (enforcement).

GeoCities: FTC:s första fall om integritetsskydd i webbmiljö

FTC:s första fall om integritetsskydd på Internet, GeoCities, handlades med stöd av FTC:s befogenheter enligt avsnitt 5 ([6]). FTC hävdade att GeoCities gav både vuxna och barn en felaktig bild av hur personuppgifterna skulle användas. I sitt klagomål hävdade FTC att GeoCities gav intrycket att vissa personuppgifter som samlades in på webbplatsen bara skulle användas internt eller för att ge konsumenterna särskilda reklamerbjudanden och att viss ytterligare ”valfri” information inte skulle lämnas vidare till någon annan utan konsumentens godkännande. I verkligheten lämnades uppgifterna ut till utomstående som använde dem för riktade erbjudanden som gick längre än vad medlemmen hade accepterat. I klagomålet framhölls vidare att GeoCities använde bedrägliga metoder vid insamling av uppgifter från barn. Enligt FTC:s klagomål gav GeoCities ett intryck av att bedriva barnverksamhet på en del av sin webbplats och att de uppgifter som inhämtades där förvaltades av GeoCities. I själva verket sköttes de delarna på webbplatsen av utomstående som samlade in och förvaltade uppgifterna.

Enligt förlikningen förbjuds GeoCities att ge en felaktig bild av syftet med insamlingen av personuppgifter från eller om konsumenter, även barn. I beslutet föreskrevs att företaget skulle lägga ut ett tydligt och iögonfallande Integritetsmeddelande (Privacy Notice), där konsumenter skulle informeras om vilka uppgifter som samlades in, för vilket ändamål och till vem de skulle lämnas, samt hur konsumenter kunde komma åt och avlägsna uppgifterna. För att trygga föräldrarnas överinseende går förlikningen vidare ut på att GeoCities måste inhämta föräldrarnas samtycke innan personuppgifter samlas in från barn under tolv år. Enligt beslutet skall GeoCities informera sina medlemmar och erbjuda dem en möjlighet att radera personuppgifter från GeoCities och varje tredje parts databaser. I förlikningen anges särskilt att GeoCities skall informera föräldrar till barn under tolv år och radera personuppgifterna, såvida föräldern inte uttryckligen godkänner att personuppgifterna sparas och används. Slutlingen skall GeoCities dessutom kontakta utomstående som tagit emot uppgifter och begära att de raderar uppgifterna ([7]).

ReverseAuction.com

I januari 2000 godkände FTC ett klagomål och ett samförståndsavtal när det gällde ReverseAuction.com, en auktionswebbplats som uppgavs ha fått konsumenternas personuppgifter från en konkurrerande webbplats (eBay.com) och därefter skickat vilseledande, obeställd e-postreklam till de konsumenter som vände sig till företaget ([8]). I vårt klagomål häv-

([5]) Inför den federala distriktsdomstolen anförde FTC nyligen klagomål mot ett företag som åtagits sig att följa TRUSTe-principerna, Toysmart.com. I detta mål yrkar FTC på förbudsförläggande och fastställelse i syfte att förhindra försäljning av konfidentiella kunduppgifter som hade insamlats på företagets webbplats i strid med företagets egen policy för integritetsskydd. FTC fick höra talas om denna eventuella lagöverträdelse direkt från TRUSTe. FTC mot Toysmart.com, LLC, civilmål nr 00-11341-RGS (D.Ma.) (registrerat den 11 juli 2000) (Internetadress: http://www.ftc.gov/opa/2000/07/toysmart.htm).

([6]) GeoCities. Docket No. C-3849 (Slutligt beslut den 12 februari 1999) (Internetadress: http://www.ftc.gov/os/1999/9902/9823015d%26o.htm).

([7]) Senare avgjorde FTC ett annat ärende som gällde insamling av personuppgifter på nätet från barn. Liberty Financial Companies Inc. drev webbplatsen Young Investor som riktade sig till barn och ungdomar, och fokuserade på frågor om pengar och kapitalförvaltning. FTC hävdade att webbplatsen felaktigt gav intryck av att personuppgifter som samlades in från barn genom en enkät skulle vara anonyma och att deltagarna skulle få ett nyhetsbrev via e-post samt erhålla priser. I verkligheten sparades personuppgifterna om barnet och familjens ekonomi på ett identifierbart sätt och varken nyhetsbrev eller priser skickades. I förlikningen förbjuds sådana vilseledande metoder för framtiden och Liberty Financial tvingas att lägga ut ett integritetsmeddelande på sin webbplats för barn samt inhämta bevis föra att föräldrarna samtycker innan personuppgifter från barn samlas in. Liberty Financial Cos., Docket No. C-3891 (Slutligt beslut den 12 augusti 1999) (Internetadress http://www.ftc.gov/opa/1999/9905/younginvestor.htm).

([8]) Se ReverseAuction.com, Inc., civilmål nr 000032 (D.D.C.) (reg.datum 6 januari 2000) (pressrelease och rättegångshandlingar på Internetadress http://www.ftc.gov/opa/2000/01/reverse4.htm).

dades att ReverseAuction brutit mot avsnitt 5 i Federal Trade Commission Act genom att dels tillskansa sig personuppgifter, inklusive eBay-användarnas e-postadresser och personliga användaridentiteter (user IDs), dels sända ut de vilseledande e-postmeddelandena.

Som också beskrivs i klagomålet hade ReverseAuction – innan man tagit del av de här uppgifterna – registrerat sig som eBay-användare och förklarat sig införstådd med att följa eBays användaravtal och regler för integritetsskydd. Genom dessa skyddas konsumenternas integritet eftersom eBay-användare förbjuds att insamla och använda personuppgifter för otillåtna ändamål, som att sända ut vilseledande, obeställd e-postreklam. I vårt klagomål hävdades för det första att ReverseAuction felaktigt utgivit sig för att vilja följa eBays användaravtal och regler för integritetsskydd, vilket är ett bedrägligt beteende enligt avsnitt 5. I klagomålet hävdades också att ReverseAuctions utnyttjande av uppgifterna för att skicka ut vilseledande, obeställd e-postreklam, i strid med användaravtalet och reglerna för integritetsskydd, kunde sägas vara illojala handelsmetoder enligt avsnitt 5.

För det andra hävdades att e-postmeddelandena till konsumenterna innehöll en vilseledande ärenderad om att deras eBay-användaridentitet "snart skulle upphöra att gälla". Slutligen hävdades att e-postmeddelandena utan någon saklig grund kunde ge intryck av att eBay direkt eller indirekt lämnade ut eBay-användarnas personuppgifter till ReverseAuction eller på annat vis deltog i spridningen av obeställd e-post.

Den förlikning som FTC lyckades uppnå hindrar ReverseAuction från att begå liknande överträdelser i framtiden. ReverseAuction måste också skicka ut ett meddelande till alla konsumenter som redan har registrerat sig hos ReverseAuction eller tänkt göra det efter att ha fått ReverseAuctions e-post. I meddelandet informeras dessa konsumenter om att det inte stämde att deras eBay-användaridentiteter skulle upphöra att gälla på eBay och att eBay varken kände till eller hade givit sitt tillstånd till ReverseAuctions spridning av den obeställda e-posten. Genom meddelandet får konsumenterna också möjlighet att avregistrera sig från ReverseAuction och få sina personuppgifter raderade från ReverseAuctions databas. Enligt beslutet måste ReverseAuction dessutom radera och avstå från att använda eller röja personuppgifter för de eBay-medlemmar som hade tagit emot ReverseAuctions e-postmeddelande, men inte registrerat sig hos ReverseAuction. Liksom när det gäller myndighetens tidigare beslut som rör integritetsskydd innehåller förlikningen krav på att ReverseAuction skall lägga ut sina egna integritetsregler på sin webbplats samt ingående bestämmelser när det gäller posthantering för att FTC skall kunna övervaka att reglerna följs.

ReverseAuction-fallet visar att FTC verkligen utövar tillsyn i syfte att stödja sektorns självreglerande insatser för att skydda konsumenternas integritet i webbmiljö. I det här fallet anfördes besvär direkt mot de metoder som underminerar de särskilda integritetsregler och användaravtal som har till uppgift att skydda konsumenternas integritet, vilket skulle kunna skada konsumenternas förtroende för webbföretagens integritetsskydd. Eftersom det här fallet omfattade ett företags ovarsamma spridning av uppgifter om konsumenter som skyddas av ett annat företags integritetsregler, kan det också vara särskilt betydelsefullt med tanke på integritetsfrågor som kan uppkomma vid dataöverföring mellan företag i olika länder.

Trots FTC:s insatser för att se till att lagen verkligen efterlevs i fallen GeoCities, Liberty Financial Cos. och ReverseAuction, är myndighetens befogenheter mer begränsade när det gäller andra områden som rör integritetsskydd i webbmiljö. Som tidigare nämnts måste det antingen röra sig illojala eller bedrägliga metoder för att Federal Trade Commission Act skall kunna tillämpas på insamling och användning av personsuppgifter utan samtycke. Federal Trade Commission Act skulle därför förmodligen inte omfatta en webbplats som samlar in personuppgifter från konsumenter, men inte felaktigt utger sig för att ha ett visst syfte med att insamla dessa uppgifter eller använder/lämnar vidare uppgifterna på ett sådant sätt att det sannolikt skulle åsamka konsumenterna större skada. Det hör kanske inte heller till FTC:s nuvarande befogenheter att rent allmänt kräva att organisationer som samlar in uppgifter på Internet har regler för integritetsskydd eller en viss typ av regler ([9]). Som tidigare nämnts är det däremot sannolikt att det rör sig om en bedräglig handling när ett företag underlåter att följa vissa angivna regler för integritetsskydd.

([9]) Av denna anledning påpekade FTC vid ett kongressförhör att det antagligen skulle krävas ytterligare lagstiftning för att få alla kommersiella webbplatser i USA som riktar sig diekt till konsumenterna att följa vissa rimliga informationsmetoder. "Consumer Privacy on the World Wide Web," Inför Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce United States House of Representatives, 21 juli 1998 (uttalandet finns på Internetadress: http://www.ftc.gov/os/9807/privac98.htm). FTC ville avvakta med att kräva sådan lagstiftning för att se till att webbplatserna genom självreglering får möjlighet att i större utsträckning använda sig av rimliga informationsmetoder. I FTC:s rapport till kongressen om integritetsskydd i webbmiljö, "Privacy Online: A Report to Congress", juni 1998 (rapporten finns på Internetadress: http://www.ftc.gov/reports/privacy3/toc.htm) rekommenderade FTC att det i lagstiftningen skulle införas krav på att kommersiella webbplatser skulle få föräldrarnas godkännande innan de fick rätt att inhämta personuppgifter från barn under 13 år. Se fotnot 3. Förra året konstaterade FTC i sin rapport "Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress", juli 1999 (rapporten finns på Internetadress: http://www.ftc.gov/os/1999/9907/index.htm#13,) att självregleringen hade resulterat i tillräckliga framsteg och valde därför att inte förorda någon lagstiftning vid den här tidpunkten.
I maj 2000 lade FTC fram en ny rapport för kongressen "Privacy Online: Fair Information Practices in the Electronic Marketplace" (rapporten finns på Internetadress: http://www.ftc.gov/os/2000/05/index.htm#22), där man behandlar FTC:s nyligen genomförda undersökning av kommersiella webbplatser och hur dessa följer reglerna om rättvisande information. I rapporten rekommenderas också (av en majoritet av FTC) att kongressen skall anta en lag om ett grundläggande integritetsskydd när det gäller kommersiella webbplatser som riktar sig till konsumenter.

FTC:s befogenheter på det här området omfattar dessutom endast illojala eller bedrägliga handlingar eller metoder som sker ”i eller som påverkar handeln”. Informationsinsamling av kommersiella enheter som saluför varor eller tjänster – inklusive insamling och användning av uppgifter för kommersiella ändamål – skulle antagligen uppfylla handelskriterier. Å andra sidan kan många privatpersoner eller organisationer samla in information på nätet utan något kommersiellt syfte och i så fall hamna utanför FTC:s behörighetsområde. Ett exempel på denna begränsning är bl.a. chat rooms som drivs av icke-kommersiella organisationer, t.ex. välgörenhetsorganisationer.

Slutligen finns det en rad fullständiga eller partiella lagstadgade undantag från FTC:s grundbefogenheter över näringslivet, vilket gör att FTC inte kan ge ett helt uttömmande svar när det gäller integritetsskyddet på Internet. Detta omfattar t.ex. undantag för många informationsintensiva konsumentföretag, som banker, försäkringsbolag och flygbolag. Som Ni väl känner till övergår ju i så fall befogenheten över sådana enheter till andra federala eller statliga organ, som federala bankmyndigheterna eller Förenta staternas transportministerium.

Inom de områden där FTC verkligen har befogenhet tar man emot de klagomål som konsumenterna har lämnat per post och telefon till dess konsumentforum Consumer Response Center (CRC) och på senare tid även till dess webbplats ([10]) och vidtar åtgärder i den utsträckning som resurserna medger. På CRC tar man emot klagomål från alla konsumenter, även konsumenter bosatta i EU:s medlemsstater. Enligt Federal Trade Commission Act har FTC billighetsrättslig befogenhet att utfärda förbudsföreläggande mot framtida överträdelser av Federal Trade Commission Act samt rätt att få tillgång till domstolsprövning för drabbade konsumenters räkning. Eftersom vi inte löser enskilda konsumenttvister, skulle vi i så fall undersöka om företaget har ägnat sig åt oegentligheter i större utsträckning. Tidigare har FTC kunnat bistå med domstolsprövning för medborgare både i USA och andra länder ([11]). Inom ramen för sina befogenheter kommer FTC även i fortsättningen att hävda sin maktbefogenhet för att ge medborgare i andra länder som har drabbats av bedrägliga metoder tillgång till domstolsprövning i de fall där detta anses vara lämpligt.

Personuppgifter om anställda

Enligt Er senaste skrivelse skulle Ni vilja ha ytterligare klargöranden i fråga om FTC:s befogenhet när det gäller personuppgifter om anställda. För det första ställer Ni frågan om huruvida FTC enligt avsnitt 5 kan vidta åtgärder mot ett företag som säger sig efterleva *safe harbor*-principerna, men som överför eller använder anställningsrelaterade uppgifter på ett sätt som strider mot dessa principer. Vi vill försäkra Er om att vi noggrant har gått igenom den lagstiftning som reglerar FTC:s verksamhet, relaterade handlingar och rättspraxis och vi drar slutsatsen att FTC har samma befogenhet när det gäller anställningsrelaterade uppgifter som vi allmänt sett har enligt avsnitt 5 i Federal Trade Commission Act ([12]). Met detta menas att om vi antar att ett ärende uppfyller de kriterierna (illojala eller bedrägliga handlingar) som skall vara uppfyllda för att vi skall vidta rättsliga åtgärder i fråga om integritetsskydd, skulle vi kunna vidta åtgärder i ärendet om personuppgifter om anställda.

Vi skulle även vilja skingra alla tvivel om huruvida FTC:s möjligheter att vidta rättsliga åtgärder i frågor om integritetsskydd är begränsade till situationer där ett företag har uppträtt bedrägligt gentemot enskilda konsumenter. Såsom klart framgår av FTC:s insats i ReverseAuction-fallet ([13]) kommer åtgärder att vidtas i integritetsskyddsärenden i de fall som gäller uppgiftsöverföring mellan företag, där ett företag påstås ha agerat orättmätigt mot det andra företaget, vilket skulle ha skadat både konsumenterna och företaget. Vi anser att detta är ett exempel på ett fall där det är mest sannolikt att frågor om personuppgifter om anställda kommer upp, eftersom anställningsuppgifter om européer överförs från företag i EU till företag i USA som har bundit sig att följa *safe harbor*-principerna.

Vi vill dock påpeka att det finns en situation där FTC:s befogenhet att agera är begränsad. Denna situation skulle kunna uppstå när ett ärende redan är föremål för en traditionell arbetsrättlig tvist – med största sannolikhet ett klagomåls-skiljedomsförfarande eller ett klagomål om otillåten behandling av arbetstagare hos National Labor Relations Board (NLRB).

([10]) Se FTC:s klagomålsblankett som finns på nätet: http://www.ftc.gov/ftc/complaint.htm.

([11]) I ett aktuellt mål gällande pyramidspel på Internet lyckades FTC t.ex. utkräva återbetalning till 15 622 konsumenter till ett sammanlagt belopp av cirka 5,5 miljoner US-dollar. Konsumenterna var bosatta i USA och 70 andra länder. Se http://www.ftc.gov/opa/9807/fortunar.htm samt http://www.ftc.gov/opa/9807/ftcrefund01.htm.

([12]) Förutom vad som särskilt exkluderas enligt FTC:s stadga, har FTC enligt FTC-lagen befogenhet över metoder ”i eller som påverkar handeln” i samma utsträckning som kongressens grundlagsenliga makt enligt Commerce Clause, United States mot American Building Maintenance Industries, 422 U.S. 271, 277 n. 6 (1975). FTC:s befogenhet skulle alltså omfatta anställningsrelaterade metoder i de företag och branscher som bedriver utrikeshandel.

([13]) Se ”Online Auction Site Settles FTC Privacy Charges”, pressmeddelande från FTC, 6 januari 2000, tillgänglig på Internetadress http://www.ftc.gov/opa/2000/01/reverse4.htm.

Detta skulle kunna hända om till exempel en arbetsgivare i ett kollektivavtal har gjort ett åtagande i fråga om användningen av uppgifter om personalen och en anställd eller ett fackförbund hävdar att arbetsgivaren har brutit mot avtalet. FTC skulle troligen ta hänsyn till det förfarandet ([14]).

Befogenhet i fråga om integritetsskyddsmärkning

För det andra frågade Ni om FTC har någon befogenhet över de prgoram för integritetsskyddsmärkning (seal programs) som förvaltar tvistlösningsmekanismer i USA, om ett sådan program gör en oriktig framställning av sin roll när det gäller att genomdriva *safe harbor*-principerna och att handlägga enskilda klagomål, även om denna enhet tekniskt sett var ideell. För att avgöra om vi har befogenhet i fråga om en enhet som ger sig ut för att vara ideell, analyserar FTC noggrant om enheten bidrar till sina medlemmars vinster, även om den inte för egen del drivs i vinstsyfte. FTC har med framgång gjort sin befogenhet gällande över sådana enheter och senast den 24 maj 1999 bekräftade Förenta staternas högsta domstol enhälligt i fallet California Dental Association mot Federal Trade Commission FTC:s befogenhet över en frivillig ideell sammanslutning av lokala tandläkarföretag i ett antitrust-mål. Domstolen fastslog:

> I Federal Trade Commission Act vinnlägger man sig verkligen om att inte bara omfatta enheter ”som är organiserade så att de bedriver verksamhet för egen vinning” (15 U.S.C. § 44), utan även de som bedriver verksamhet för ”sina medlemmars” vinning … Det är knappast troligt att kongressen skulle ha avsett att vara så begränsad i sin definition av omfattade stödorganisationer med tanke på de möjligheter detta skulle medföra att kringgå denna befogenhet, då syftet med Federal Trade Commission Act uppenbarligen skulle vara att befogenheten utövades.

Att avgöra om vi kan göra gällande vår befogenhet över en viss ideell enhet som driver ett program för integritetsskyddsmärkning skulle alltså kräva en saklig genomgång av i vad mån den enheten gav sina medlemmar ekonomiska fördelar. Om en sådan enhet drev sitt program på ett sådant sätt att det ledde till ekonomiska fördelar för dess medlemmar, skulle FTC troligtvis använda sig av sin befogenhet. FTC skulle dessutom sannolikt ha befogenhet över ett bedrägligt program för integritetsskyddsmärkning som oriktigt framställer sig som en ideell enhet.

Integritetsskydd utanför webbmiljön

För det tredje påpekar Ni att vår tidigare skriftväxling har varit inriktad på integritetsskydd i webbmiljö. Integritetsskydd i webbmiljö är mycket riktigt en viktig fråga för FTC eftersom det är en avgörande faktor i utveckling av den elektroniska handeln, men Federal Trade Commission Act är från 1914 och gäller alltså även utanför webbmiljön. Vi kan alltså vidta åtgärder mot de företag utanför webbmiljön som ägnar sig åt illojalt eller bedrägligt handelsbruk avseende skyddet av konsumenternas integritet ([15]). I en talan som FTC väckte förra året, FTC mot TouchTone Information Inc. ([16]) åtalades en informationsmäklare för att olagligt hå fått tag i och sålt privatekonomiska uppgifter om konsumenterna. FTC hävdade att TouchTone hade fått tag i konsumentinformationen genom pretexting, ett begrepp som myntades inom privatdetektivbranschen för att beskriva hur man får tag på personuppgifter om någon annan genom falska förespeglingar, framför allt via telefonsamtal. I målet, som lämnades in den 21 april 1999 till en federal domstol i Colorado, är FTC:s krav ett förbudsföreläggande samt återbetalning av alla olagligt gjorda vinster.

Dessa insatser för att säkerställa efterlevnaden av lagarna, men också oron inför sammanslagningen av databaser i och utanför webbmiljö, den oklara linjen mellan handel i och utanför webbmiljö och det faktum att en stor mängd personuppgifter insamlas och används utanfør webbmiljö visar klart att betydande vikt måste läggas vid frågor som rör integritetsskydd utanför webbmiljö.

Överlappande befogenheter

Slutligen ställer Ni en fråga om samspelet mellan FTC:s befogenhet och andra rättskipande instansers befogenheter, särskilt i fall där det kan röra sig om överlappande befogenheter. Vi har mycket goda, välfungerande relationer med många

([14]) Avgörandet om ett beteende utgör en otillåten behandling av arbetstagare eller ett brott mot ett kollektivavtal är en teknisk fråga som vanligen förbehålls de experter i arbetsdomstolarna som prövar klagomålen, t.ex. skiljedomare eller NRLB.

([15]) Som Ni känner till från tidigare diskussioner ger lagen Fair Credit Reporting Act FTC befogenhet att skydda konsumenterna mot insyn i deras privatekonomi inom ramen för lagen, och FTC utfärdade nyligen ett beslut i denna fråga. Se In the Matter of Trans Union, Docket No. 9255 (1 mars 2000) (pressmeddelande och yttrande tillgängligt på Internetadress http://www.ftc.gov/os/2000/03/index.htm#1).

([16]) Civilmål 99-WM-783 (D. Colo.) (tillgängligt på Internetadress http://www.ftc.gov/opa/1999/9904/touchtone.htm) (Ett preliminärt billighetsrättsligt beslut är under förhandling.)

andra rättsskipande instanser, däribland de federala bankmyndigheterna och justitiekanslern i delstaterna. Vi samordnar mycket ofta våra undersökningar för att dra maximal nytta av våra resurser då det föreligger överlappande befogenheter. Vi hänskjuter dessutom ofta ärenden till den berörda federala eller delstatliga myndigheten för utredning.

Jag hoppas att denna översikt skall vara till hjälp. Vi står till Ert förfogande, om Ni skulle behöva ytterligare upplysningar.

Med vänlig hälsning,

Robert Pitofsky

BILAGA VI

John Mogg
Generaldirektör, GD Inre marknaden
Europeiska kommissionen
Kontor C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Bryssel

Herr generaldirektör,

Detta brev sänds till Er på uppdrag av Förenta staternas handelsministerium (U.S. Department of Commerce) för att förklara vilken roll Förenta staternas transportministerium (Department of Transportation) har när det gäller skydd av konsumenternas integritet avseende information som lämnats av dem till flygbolag.

Förenta staternas transportministerium förordar självreglering eftersom det är ett mindre ingrepp som ger det effektivaste skyddet för den information som konsumenter lämnar till flygbolag. Därmed stöder vi ett införande av ett *safe harbor*-system som gör det möjligt för flygbolag att följa kraven i Europeiska unionens direktiv om skydd av personuppgifter vid överföringar utanför EU. Förenta staternas transportministerium inser emellertid att för att självreglering skall fungera är det viktigt att de flygbolag som ansluter sig till principerna för skydd av personuppgifter i *safe harbor*-systemet också verkligen följer dem. Därför bör bristande efterlevnad beivras. Genom att använda gällande konsumentskyddslagstiftning kommer Förenta staternas transportministerium att se till att flygbolagen följer de utfästelser man gjort till allmänheten när det gäller integritetsskydd, och beivra fall av påståenden om att de inte följs som ministeriet erhåller från självregleringsorganisationer och andra, inklusive EU:s medlemsstater.

Förenta staternas transportministeriums behörighet att vidta korrektiva åtgärder på området stöds av 49 artikeln i United States Code 41712 vilken förbjuder ett flygbolag att tillämpa illojala metoder eller bedrägligt beteende eller illojal konkurrens vid försäljning av lufttransporttjänster som skadar eller kan skada en konsument. Section 41712 är utformad efter section 5 i Federal Trade Commission Act (15 U.S.C. 45). Flygbolag är emellertid genom Federal Trade Commission undantagna från section 5-reglerna under 15 U.S.C. 45(a)(2).

Min enhet undersöker och beivrar olika fall med stöd av 49 U.S.C. 41712. (Se t.ex. DOT Orders 99-11-5 av den 9 november 1999; 99-8-23 av den 26 augusti 1999; 99-6-1 av den 1 juni 1999; 98-6-24 av den 22 juni 1998; 98-6-21 av den 19 juni 1998; 98-5-31 av den 22 maj 1998 och 97-12-23 av den 18 december 1997). Vi kan initiera sådana fall utgående från egna undersökningar men också efter formella eller informella klagomål som vi får in från privatpersoner, resebyråer, flygbolag samt statliga organ i USA och utlandet.

Jag vill påpeka att om ett flygbolag bryter sekretessen kring uppgifter det erhållit av en passagerare inte i sig innebär att man brutit mot section 41712. Så snart som ett flygbolag emellertid formellt och offentligt anslutit sig till *safe harbor*-principerna för skydd av personuppgifter som man erhållit från konsumenter, skall Förenta staternas transportministerium vara behörigt att tillämpa lagstiftningen i section 41712 för att säkerställa att dessa principer följs. Det innebär att har väl en passagerare lämnat information till ett flygbolag, som har åtagit sig att respektera *safe harbor*-principerna, medför underlåtenhet att göra detta troligen att en konsument lider skada och det är därmed ett brott mot section 41712. Min enhet kommer i ett sådant fall att ge hög prioritet åt att undersöka varje sådan påstådd handling och lämna till åtal varje fall där sådant bevisas. Vi kommer också att meddela Förenta staternas handelsministerium om resultatet av varje sådant fall.

Brott mot section 41712 kan innebära ett förvaltningsbeslut som förbjuder dessa handlingar och vite om dessa förbud sedan inte följs. Vi har inte befogenhet att besluta om skadestånd eller ersättningsbelopp till enskilda klagande, men vi har ändå befogenhet att godkänna uppgörelser som framkommer genom utredning och åtal av Förenta staternas transportministerium och som kan komma konsumenten tillgodo antingen som nedsättning eller kvittning av straffavgifter som annars skulle betalats. Vi har gjort så tidigare och vi kommer att kunna göra så i samband med *safe harbor*-principerna när det är befogat. Upprepade brott mot section 41712 som något amerikanskt flygbolag begår kommer också att ifrågasätta flygbolagets ”compliance disposition” som i flagranta fall kan resultera i att flygbolaget inte längre kan anses ägnat att driva flygverksamhet och kunna förlora sitt tillstånd (economic operating authority).

(Se DOT Orders 93-6-34 av den 23 juni 1993 och 93-6-11 av den 9 juni 1993. Även om denna handläggning inte utgår från section 41712, blev dock resultatet att ett flygbolag blev fråntaget sitt tillstånd (operating authority) efter att fullständigt ha ignorerat bestämmelserna i den federala luftfartslagen (Federal Aviation Act), som är en ömsesidig överenskommelse, samt ministeriets regler och förordningar.)

Jag hoppas denna information är till nytta för Er. Har Ni frågor eller behöver ytterligare information står jag till Ert förfogande.

Med vänlig hälsning

Samuel Podberesky

Biträdande chefsjurist (Assistant General Counsel)
Tillsynsenheten för luftfart (Aviation Enforcement and Proceeding)

BILAGA VII

Med hänvisning till artikel 1.2 b är de myndigheter i Förenta staterna som är bemyndigade att handlägga klagomål och ge upprättelse vid användning av illojala och bedrägliga metoder och att utverka skadestånd åt enskilda, oberoende av deras bosättningsland eller nationalitet, om principerna tillämpade i överensstämmelse med FoS inte följs, följande:

1. Federal Trade Commission.

2. Förenta staternas transportministerium.

Federal Trade Commission handlar med stöd av sin behörighet enligt avsnitt 5 i Federal Trade Commission Act. Federal Trade Commission saknar enligt avsnitt 5 behörighet när det gäller följande branscher: banker, spar-, låne- och kreditinstitut, telekommunikation, transportföretag med mellanstatlig verksamhet, flygföretag, lastnings- och lagerföretag. Försäkringsbranschen finns inte med på listan över undantag i avsnitt 5, men genom McCarran-Ferguson Act [1], överlåts regleringen av försäkringsbranschen åt de enskilda delstaterna. Bestämmelserna i FTC Act behåller dock försäkringsbranschen i den mån som den branschen inte omfattas av delstatslagar. FTC Act gäller även tillsynsbehörigheten över försäkringsbolag som använder sig av illojala och bedrägliga metoder i annan verksamhet än försäkringsverksamhet.

Förenta staternas transportministerium handlar med stöd av sin behörighet enligt kapitel 49 i United States Code Section 41712. Det amerikanska transportministeriet kan inleda ett förfarande på grundval av egna undersökningar såväl som efter formella och informella klagomål från enskilda personer, resebyråer, flygföretag och amerikanska och utländska myndigheter.

[1] 15 U.S.C. § 1011 *et seq*.