►B

KOMISSION PÄÄTÖS,

tehty 26 päivänä heinäkuuta 2000,

Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti yksityisyyden suojaa koskevien safe harbor -periaatteiden antaman suojan riittävyydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista tavallisimmista kysymyksistä

(tiedoksiannettu numerolla K(2000) 2441)

(ETA:n kannalta merkityksellinen teksti)

(2000/520/EY)

(EYVL L 215, 25.8.2000, s. 7)

Oikaistu:

►C1 Oikaisu, EYVL L 115, 25.4.2001, s. 14 (2000/520/EY)

▼B

KOMISSION PÄÄTÖS,

tehty 26 päivänä heinäkuuta 2000,

Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti yksityisyyden suojaa koskevien safe harbor -periaatteiden antaman suojan riittävyydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista tavallisimmista kysymyksistä

(tiedoksiannettu numerolla K(2000) 2441)

(ETA:n kannalta merkityksellinen teksti)

(2000/520/EY)

EUROOPAN YHTEISÖJEN KOMISSIO, joka

ottaa huomioon Euroopan yhteisön perustamissopimuksen,

ottaa huomioon yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY [1], ja erityisesti sen 25 artiklan 6 kohdan,

sekä katsoo seuraavaa:

(1) Direktiivin 95/46/EY mukaan jäsenvaltioiden on säädettävä siitä, että henkilötietoja voidaan siirtää kolmanteen maahan vain, jos kyseisessä kolmannessa maassa turvataan tietosuojan riittävä taso ja direktiivin muiden säännösten täytäntöönpanemiseksi annettuja jäsenvaltioiden lakeja noudatetaan ennen tietojen siirtämistä.

(2) Komissio voi todeta, että kolmas maa turvaa tietosuojan riittävän tason. Henkilötietojen siirtäminen jäsenvaltioista voidaan tässä tapauksessa sallia ilman lisätakeita.

(3) Direktiivin 95/46/EY mukaisesti tietosuojan taso olisi arvioitava kaikkien tiettyyn siirtoon tai siirtojen ryhmään liittyvien olosuhteiden osalta. Direktiivin mukaisesti perustettu tietosuojatyöryhmä [2] on antanut arvioinnin tekemistä koskevia ohjeita [3].

(4) Koska kolmannet maat suhtautuvat eri tavoin tietosuojaan, tietosuojan riittävyyden arviointi olisi suoritettava ja kaikki direktiivin 95/46/EY 25 artiklan 6 kohtaan perustuvat päätökset olisi pantava täytäntöön tavalla, joka ei mielivaltaisesti tai epäoikeudenmukaisesti syrji mitään kolmatta maata tai tee eroa niiden välillä, jos niissä vallitsevat samanlaiset olosuhteet, tai muodosta peiteltyä kaupan estettä yhteisön nykyiset kansainväliset sitoumukset huomioon ottaen.

(5) Tämän päätöksen mukainen riittävä suojan taso tietojen siirrolle yhteisöstä Yhdysvaltoihin pitäisi saada, jos organisaatiot noudattavat jäsenvaltioista Yhdysvaltoihin siirrettävien henkilötietojen suojan osalta yksityisyyden suojaa koskevia safe harbor -periaatteita, jäljempänä ”periaatteet”, ja tavallisimpien kysymysten -ohjetta periaatteiden täytäntöönpanemiseksi, jäljempänä ”FAQ”, jotka Yhdysvaltain hallitus on laatinut 21 päivänä heinäkuuta 2000. Organisaatioiden on lisäksi julkistettava yksityisyyden suojaa koskeva toimintalinjansa ja kuuluttava Federal Trade Commission Act -lain, jossa kielletään kauppaa koskevat tai kauppaan vaikuttavat sopimattomat tai harhaanjohtavat toimet tai käytännöt, 5 pykälän nojalla Federal Trade Commissionin (FTC) tai muun, FAQ:iden mukaisesti sovellettavien periaatteiden noudattamisesta vastaavan lakisääteisen elimen toimivallan piiriin.

---

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

[2] Ks. internet-osoite http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

[3] WP 12: Henkilötietojen siirto kolmansiin maihin: EU:n tietosuojadirektiivin 25 ja 26 artiklan soveltaminen. Työryhmän 24 päivänä heinäkuuta 1998 hyväksymä.

▼B

(6) Alat ja/tai tietojenkäsittelytoimet, jotka eivät kuulu tämän päätöksen liitteessä VII lueteltujen valtiollisten elinten toimivaltaan Yhdysvalloissa, eivät kuulu tämän päätöksen soveltamisalaan.

(7) Tämän päätöksen asianmukaisen soveltamisen varmistamiseksi asianomaisten osapuolten, kuten rekisteröityjen, tiedonviejien ja tietosuojaviranomaisten, on voitava tunnistaa periaatteita ja FAQ:ita noudattavat organisaatiot; sen vuoksi Yhdysvaltojen kauppaministeriön tai sen edustajan olisi otettava tehtäväkseen ylläpitää ja pitää yleisesti saatavilla luetteloa organisaatioista, jotka ilmoittavat noudattavansa FAQ:iden mukaisesti sovellettavia periaatteita ja jotka kuuluvat ainakin yhden tämän päätöksen liitteessä VII luetellun valtiollisen elimen toimivallan piiriin.

(8) Avoimuuden saavuttamiseksi ja sen varmistamiseksi, että jäsenvaltioiden toimivaltaiset viranomaiset kykenevät turvaamaan yksityishenkilöiden suojan henkilötietoja käsiteltäessä, tässä päätöksessä on tarpeen määritellä poikkeukselliset olot, joissa tiettyjen tiedonsiirtojen keskeyttäminen olisi oikeutettua siitä huolimatta, että tietosuojan taso on todettu riittäväksi.

(9) Safe harbor -periaatteiden ja FAQ:iden tarkistaminen saattaa olla tarpeen yksityisyyden suojaan liittyvien kokemusten ja kehityksen perusteella, kun teknologia jatkuvasti yksinkertaistaa henkilötietojen siirtoa ja käsittelyä, ja niiden kertomusten perusteella, joita saadaan asiaa käsitteleviltä täytäntöönpanoviranomaisilta.

(10) Direktiivin 95/46/EY 29 artiklalla perustettu tietosuojatyöryhmä on antanut lausuntoja safe harbor -periaatteiden tarjoamasta tietosuojan tasosta Yhdysvalloissa. Lausunnot on otettu huomioon tämän päätöksen valmistelussa ([1]).

(11) Tässä päätöksessä säädetyt toimenpiteet ovat direktiivin 95/46/EY 31 artiklalla perustetun komitean lausunnon mukaiset.

▼C1

(12) Neuvoston päätöksen 1999/468/EY ja erityisesti sen 8 artiklan nojalla Euroopan parlamentti antoi 5 päivänä heinäkuuta 2000 päätöslauselman A5-0177/2000 komission päätösluonnoksesta yksityisyyden suojaa koskevien safe harbor -periaatteiden ja niihin liittyvien Yhdysvaltojen kauppaministeriön julkaisemien tavallisimpien kysymysten (FAQ) antaman suojan riittävyydestä ([2]). Tarkasteltuaan uudelleen päätösluonnosta mainitun päätöslauselman johdosta komissio tuli siihen tulokseen, että vaikka Euroopan parlamentti katsoi, että safe harbor -periaatteisiin ja niihin liittyviin tavallisimpiin kysymyksiin tulisi tehdä joitakin parannuksia ennen kuin niiden voitaisiin katsoa antavan ”riittävän suojan”, se ei todennut, että komissio ylittäisi toimivaltansa tehdessään kyseisen päätöksen,

([1]) WP 15: Lausunto 1/99 tietosuojan tasosta Yhdysvalloissa ja Euroopan komission ja Yhdysvaltain hallituksen välillä käynnissä olevista keskusteluista.
WP 19: Lausunto 2/99 Yhdysvaltain kauppaministeriön 19 päivänä huhtikuuta 1999 julkaisemien kansainvälisten safe harbor -periaatteiden riittävyydestä.
WP 21: Lausunto 4/99 tavallisimmista kysymyksistä, jotka Yhdysvaltain kauppaministeriö julkaisee ehdotettujen kansainvälisten safe harbor -periaatteiden riittävyyteen liittyen.
WP 23: Euroopan komission ja Yhdysvaltain hallituksen välillä käytävien kansainvälisiä safe harbor -periaatteita käsittelevien neuvottelujen etenemistä koskeva valmisteluasiakirja.
WP 27: Lausunto 7/99 Yhdysvaltain kauppaministeriön 15 ja 16 päivänä marraskuuta 1999 julkaisemien safe harbor -periaatteiden ja niiden yhteydessä julkaistujen tavallisimpien kysymysten (FAQ) ja muiden näihin liittyvien asiakirjojen mukaisesta tietosuojan tasosta.
WP 31: Lausunto 3/2000 safe harbor -järjestelyä koskevasta EU:n ja Yhdysvaltojen vuoropuhelusta.
WP 32: Lausunto 4/2000 safe harbor -periaatteiden tarjoaman tietosuojan tasosta.

([2]) Päätöslauselmaa ei ole vielä julkaistu EYVL:ssä.

▼B

ON TEHNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

1. Direktiivin 95/46/EY 25 artiklan 2 kohdan soveltamiseksi ja kaikkien direktiivin soveltamisalaan kuuluvien toimintojen osalta yksityisyyden suojaa koskevien, tämän päätöksen liitteenä I olevien safe harbor -periaatteiden, jäljempänä ”periaatteet”, joita sovelletaan Yhdysvaltojen kauppaministeriön 21 päivänä heinäkuuta 2000 julkaisemien ja tämän päätöksen liitteenä II olevien tavallisimpien kysymysten (Frequently Asked Questions, FAQ), jäljempänä ”FAQ”, tarjoaman ohjauksen mukaisesti, katsotaan varmistavan yhteisöstä Yhdysvaltoihin sijoittautuneille organisaatioille siirrettyjen henkilötietojen riittävän suojelun tason, ottaen huomioon seuraavat Yhdysvaltain kauppaministeriön julkaisemat asiakirjat:

a) periaatteiden noudattamista käsittelevä katsaus (esitetään liitteessä III);

b) muistio yksityisyyden loukkausten aiheuttamista vahingoista ja Yhdysvaltain lainsäädännön mukaiset täsmälliset valtuudet (esitetään liitteessä IV);

c) Federal Trade Commissionin kirje (esitetään liitteessä V);

d) Yhdysvaltain liikenneministeriön kirjelomake (esitetään liitteessä VI).

2. Jokaisen tietojen siirron on täytettävä seuraavat edellytykset:

a) tiedot vastaanottava organisaatio on yksiselitteisesti ja julkisesti ilmoittanut sitoutuvansa noudattamaan FAQ:iden mukaisesti sovellettuja periaatteita; ja

b) organisaatio kuuluu sellaisen tämän päätöksen liitteessä VII luetellun Yhdysvaltojen valtiollisen elimen lakisääteisen toimivallan piiriin, jolla on valtuudet tutkia valituksia ja määrätä korvauksia sopimattomista tai harhaanjohtavista käytännöistä sekä tarjota oikeuskeinoja yksityisille heidän asuinmaastaan tai kansallisuudestaan riippumatta, jos FAQ:iden mukaisesti sovellettavia periaatteita ei noudateta.

3. Edellä 2 kohdassa mainittujen edellytysten katsotaan kunkin organisaation, joka on ilmoittanut noudattavansa FAQ:iden mukaisesti sovellettavia periaatteita, osalta täyttyvän siitä päivästä alkaen, jona organisaatio antaa Yhdysvaltojen kauppaministeriölle (tai sen nimeämälle) tiedoksi edellä 2 kohdan a alakohdassa tarkoitetun julkisesti ilmoitetun sitoumuksensa ja edellä 2 kohdan b alakohdassa tarkoitetun valtiollisen elimen nimen.

2 artikla

Tämä päätös koskee ainoastaan Yhdysvalloissa FAQ:iden mukaisesti sovellettavien periaatteiden tietosuojan riittävyyttä siinä tarkoituksessa, että direktiivin 95/46/EY 25 artiklan 1 kohdan vaatimukset täytettäisiin, eikä sillä ole vaikutusta direktiivin muiden, henkilötietojen käsittelyä jäsenvaltioissa koskevien säännösten, myöskään 4 artiklan, soveltamiseen.

3 artikla

1. Rajoittamatta jäsenvaltioiden toimivaltaisten viranomaisten valtuuksia toteuttaa toimenpiteitä direktiivin 95/46/EY muiden säännösten kuin 25 artiklan noudattamiseksi annettujen kansallisten säännösten noudattamisen varmistamiseksi, jäsenvaltioiden toimivaltaiset viranomaiset voivat käyttää nykyisiä toimivaltuuksiaan keskeyttää organisaatiolle, joka on ilmoittanut noudattavansa FAQ:iden mukaisesti sovellettavia periaatteita, suunnatut tietovirrat yksityishenkilöiden suojelemiseksi heitä koskevien henkilötietojen käsittelemisen osalta tapauksissa, joissa:

a) tämän päätöksen liitteessä VII tarkoitettu Yhdysvaltojen valtiollinen elin tai tämän päätöksen liitteessä I esitetyn täytäntöönpanoperi-

▼B

aatteen a luetelmakohdassa tarkoitettu riippumaton valitusmenettelyjärjestely on todennut, että organisaatio loukkaa FAQ:iden mukaisesti sovellettavia periaatteita; tai

b) on huomattavan todennäköistä, että periaatteita loukataan; on kohtuullinen syy uskoa, että asianomainen täytäntöönpano-organisaatio ei ole ryhtynyt tai ryhdy riittäviin ja ajankohtaisiin toimenpiteisiin kyseessä olevan tapauksen ratkaisemiseksi; tietojen siirron jatkaminen aiheuttaisi välittömän vakavan haitan vaaran rekisteröidyille; ja jäsenvaltion toimivaltaiset viranomaiset ovat olosuhteisiin nähden kohtuullisessa määrin pyrkineet antamaan organisaatiolle ilmoituksen ja tilaisuuden vastata siihen.

Keskeytystoimenpide lakkaa heti, kun FAQ:iden mukaisesti sovellettavien periaatteiden noudattaminen on varmistunut ja asianomaisille toimivaltaisille viranomaisille yhteisössä on siitä ilmoitettu.

2. Jäsenvaltiot ilmoittavat viipymättä komissiolle 1 kohdan nojalla toteutetuista toimenpiteistä.

3. Jäsenvaltiot ja komissio tiedottavat toisilleen myös tapauksista, joissa periaatteiden noudattamisesta Yhdysvalloissa vastuussa olevien elinten toiminta ei varmista FAQ:iden mukaisesti sovellettavien periaatteiden noudattamista.

4. Jos 1, 2 ja 3 kohdan mukaisesti saadut tiedot osoittavat, että jokin FAQ:iden mukaisesti sovellettavien periaatteiden noudattamisesta Yhdysvalloissa vastuussa oleva elin ei tosiasiallisesti täytä tehtäväänsä, komissio tiedottaa asiasta Yhdysvaltojen kauppaministeriölle ja esittää tarvittaessa direktiivin 95/46/EY 31 artiklassa säädetyn menettelyn mukaisesti luonnoksen toimenpiteistä, joiden tarkoituksena on kumota tämä päätös tai lykätä sen soveltamista tai rajoittaa sen soveltamisalaa.

4 artikla

1. Tätä päätöstä voidaan muuttaa milloin tahansa täytäntöönpanosta saatujen kokemusten perusteella ja/tai jos Yhdysvaltojen lainsäädäntö antaa periaatteita ja FAQ:ita paremman suojan.

Komissio arvioi tämän päätöksen täytäntöönpanon käytettävissä olevien tietojen perusteella kolme vuotta sen jälkeen, kun se on annettu tiedoksi jäsenvaltioille, ja toimittaa kaikki tärkeät huomiot direktiivin 95/46/EY 31 artiklalla perustetulle komitealle, myös kaiken aineiston, joka voi vaikuttaa tämän päätöksen 1 artiklan säännösten arviointiin direktiivin 95/46/EY 25 artiklassa tarkoitetun riittävän suojan osalta ja kaikki osoitukset siitä, että tätä päätöstä pannaan täytäntöön syrjivästi.

2. Komissio esittää tarvittaessa luonnoksen toimenpiteistä 31 artiklassa säädetyn menettelyn mukaisesti.

5 artikla

Jäsenvaltioiden on toteutettava kaikki tämän päätöksen noudattamisen edellyttämät toimenpiteet yhdeksänkymmenen päivän kuluessa siitä päivästä, jona se annettiin tiedoksi jäsenvaltioille.

6 artikla

Tämä päätös on osoitettu kaikille jäsenvaltioille.

▼B

LIITE I

Yhdysvaltojen kauppaministeriön 21 päivänä heinäkuuta 2000 antamat
SAFE HARBOR -PERIAATTEET

Tietosuojaa koskeva Euroopan unionin direktiivi (jäljempänä ”direktiivi”) tuli voimaan 25. lokakuuta 1998. Siinä edellytetään, että henkilötietoja voidaan siirtää ainoastaan sellaisiin kolmansiin maihin, joissa on riittävä tietosuojataso. Yhdysvaltoja ja Euroopan unionia yhdistää sama tavoite: kansalaisten yksityisyyden suojelu. Yhdysvalloissa on kuitenkin omaksuttu asiaan erilainen lähestymistapa kuin Euroopan unionissa. Yhdysvalloissa käytetään alakohtaista lähestymistapaa, jossa yhdistyvät lainsäädäntö, sääntely ja itsesääntely. Näiden eroavaisuuksien vuoksi monet yhdysvaltalaiset organisaatiot ovat suhtautuneet epäilevästi vaikutuksiin, joita EU:n riittävän tietosuojan vaatimuksilla olisi EU:sta Yhdysvaltoihin siirrettäviin henkilötietoihin.

Yhdysvaltojen kauppaministeriö haluaa hälventää tällaisia epäilyksiä ja luoda ennustettavammat puitteet tällaisille tiedonsiirroille, ja tämän vuoksi se on laatinut tämän asiakirjan ja tietosuojaperiaatteisiin liittyvät tavallisimmat kysymykset (Frequently Asked Questions, FAQ) osana lakisääteisiä valtuuksiansa tukea, edistää ja kehittää kansainvälistä kauppaa. Periaatteet on laadittu yhdessä elinkeinoelämän ja kuluttajien edustajien kanssa Yhdysvaltojen ja Euroopan unionin välisen kaupankäynnin helpottamiseksi. Ne on tarkoitettu käytettäviksi yksinomaan yhdysvaltalaisissa yrityksissä, jotka saavat henkilötietoja Euroopan unionista ja jotka käyttävät periaatteiden noudattamista keinona safe harbor -järjestelmään osallistumiselle asetettujen kelpoisuusvaatimusten täyttämiseksi ja sen luoman tietosuojan riittävyyden olettamuksen saavuttamiseksi. Koska periaatteet on laadittu nimenomaan tätä tarkoitusta varten, niiden käyttö muissa yhteyksissä saattaa olla epäasianmukaista. Periaatteet eivät korvaa direktiivin täytäntöönpanoa varten annettuja kansallisia säädöksiä, joita sovelletaan henkilötietojen käsittelyyn jäsenvaltioissa.

Organisaatiot päättävät täysin vapaaehtoisesti, haluavatko ne liittyä safe harbor -järjestelmään, ja ne voidaan hyväksyä järjestelmään eri tavoin. Järjestelmään liittyvien organisaatioiden on noudatettava kyseisiä periaatteita saadakseen ja säilyttääkseen safe harbor -etuudet ja sitouduttava tähän julkisesti. Jos organisaatio esimerkiksi liittyy yksityissektorilla kehitettyyn, kyseisten periaatteiden mukaiseen tietosuojaohjelmaan, se saavuttaa kelpoisuuden safe harbor -järjestelmään. Organisaatio voi päästä mukaan myös kehittämällä omat tietosuojaa koskevat toimintalinjansa, mikäli ne ovat safe harbor -periaatteiden mukaiset. Jos periaatteiden noudattaminen perustuu organisaatiossa osittain tai kokonaan itsesääntelyyn ja jos organisaatio ei noudata kyseistä itsesääntelyä, noudattamatta jättämisestä on voitava nostaa kanne Federal Trade Commission Act -lain 5 pykälän nojalla, jossa kielletään kauppaa koskevat tai kauppaan vaikuttavat sopimattomat tai harhaanjohtavat toimet, tai vastaavan muun lain nojalla, jossa kielletään kyseiset toimet. (Ks. liite, jossa on luettelo EU:n tunnustamista Yhdysvaltojen lakisääteisistä elimistä). Lisäksi organisaatiot, joihin sovelletaan yleistä, sääntelevää, hallinnollista tai muuta lainsäädäntöä taikka säännöstöä, joka takaa tehokkaan henkilötietosuojan, voivat liittyä safe harbor -järjestelmään. Joka tapauksessa safe harbor -etuuksia sovelletaan siitä päivästä, jona järjestelmään haluava organisaatio ilmoittaa Yhdysvaltojen kauppaministeriölle (tai sen nimeämälle edustajalle), että se noudattaa kyseisiä periaatteita omaa varmennusta (self certification) koskevan FAQ:n mukaisesti.

Näiden periaatteiden noudattamista voidaan rajoittaa a) siinä määrin, kuin se on tarpeen kansallisen turvallisuuden, yleisen edun ja lainsäädännön vaatimusten vuoksi, b) lainsäädännöllä, hallituksen asetuksilla tai oikeuskäytännöllä, joilla syntyy ristiriitaisia velvoitteita tai joilla selkeästi annetaan lupa tiettyyn toimintaan, sillä edellytyksellä, että aina tällaista lupaa käyttäessään organisaatio voi osoittaa, että periaatteiden noudattamatta jättäminen rajoittuu siihen, mikä on tarpeen tällaisen lupaan liittyvän oikeutetun ja ensisijaisen tavoitteen täyttämiseksi, c) jos direktiivissä tai jäsenvaltion lainsäädännössä sallitaan poikkeuksia ja jos tällaisia poikkeuksia sovelletaan vastaavissa yhteyksissä. Yksityisyyden suojan kohentamista koskevan tavoitteen mukaisesti organisaatioiden tulisi pyrkiä toteuttamaan nämä periaatteet täysimittaisesti ja avoimesti ja osoittamaan yksityisyyden suojaa koskevassa politiikassaan, missä kohdin edellä b kohdassa sallittuja periaatteiden poikkeuksia sovelletaan säännönmukaisesti. Jos vaihtoehto on sallittu periaatteiden ja/tai Yhdysvaltojen lainsäädännön nojalla, organisaatioiden odotetaan samasta syystä noudattavan tiukempaa suojaa, kun tämä on mahdollista.

Organisaatiot saattavat haluta käytännöllisistä tai muista syistä soveltaa tietosuojaperiaatteita kaikkeen käsittelemäänsä tietoon, muuta ne ovat velvoitettuja soveltamaan niitä tietoon, joka on siirretty vasta niiden liityttyä safe harbor -järjestelmään. Tullakseen hyväksytyiksi safe harbor -järjestelmään organisaatioiden ei tarvitse soveltaa näitä periaatteita manuaalisesti käsiteltävissä rekis-

▼B

teröintijärjestelmissä oleviin henkilötietoihin. Organisaatioiden, jotka haluavat hyödyntää safe harbor -periaatteita tietojen saamiseksi manuaalisesti käsiteltävistä rekisteröintijärjestelmistä EU:sta, on sovellettavaperiaatteita kaikkiin tällaisiin tietoihin safe harbor -järjestelmään liittymisen jälkeen. Organisaation, joka haluaa hyödyntää safe harbor -järjestelmän etuja myös henkilöstöä koskeviin tietoihin, jotka on siirretty EU:sta työsuhteen yhteydessä käytettäviksi, on ilmoitettava tästä antaessaan oman varmennuksensa Yhdysvaltojen kauppaministeriölle (tai sen edustajalle) ja noudatettava omaa varmennusta koskevassa FAQ:ssa asetettuja vaatimuksia.

Organisaatiot voivat myös taata direktiivin 26 artiklan mukaiset tarpeelliset suojatoimet käyttämällä periaatteita kirjallisissa sopimuksissa, joita ne tekevät EU:sta tietoa siirtävien osapuolten kanssa riittävästä yksityisyyden suojasta, kun komissio ja jäsenvaltiot ovat hyväksyneet mallisopimuksen muut säännöt.

Yhdysvaltojen lainsäädäntöä sovelletaan kysymyksiin, jotka liittyvät safe harbor -periaatteiden (myös FAQ:iden) ja tietosuojaa koskevien toimintalinjojen tulkintaan ja noudattamiseen safe harbor -järjestelmään kuuluvissa organisaatioissa. Poikkeuksena ovat organisaatiot, jotka ovat sitoutuneet yhteistyöhön Euroopan tietosuojaviranomaisten kanssa. Ellei toisin mainita, sovelletaan kaikkia safe harbor -periaatteiden ja tavallisimpien kysymysten (FAQ:t) asianmukaisia sääntöjä.

Henkilötiedoilla tarkoitetaan jossakin muodossa rekisteröityjä tunnistetun tai tunnistettavan henkilön tietoja, joihin sovelletaan direktiiviä ja jotka yhdysvaltalainen organisaatio on vastaanottanut EU:sta.

ILMOITUS

Organisaation on ilmoitettava yksityishenkilöille, mihin tarkoitukseen se kerää ja käyttää heitä koskevia tietoja, miten organisaatioon saa yhteyden lisätietoja ja valituksia varten, minkälaisille kolmansille osapuolille se antaa tietoja sekä minkälaisia valintoja ja keinoja organisaatio tarjoaa henkilöille tietojen käytön ja luovuttamisen rajoittamiseksi. Ilmoitus on tehtävä selkeästi ja yksiselitteisesti samassa yhteydessä, kun henkilöitä ensimmäisen kerran pyydetään antamaan henkilötietoja organisaatiolle tai niin pian tämän jälkeen kuin mahdollista. Ilmoitus on joka tapauksessa tehtävä ennen kuin organisaatio käyttää tällaisia tietoja muuhun tarkoitukseen kuin siihen, mitä varten tiedot on alun perin kerätty tai mitä varten tiedot siirtävä organisaatio on ne käsitellyt tai luovuttaa ne ensimmäisen kerran kolmannelle osapuolelle. ([1]).

VALINTA

Organisaation on tarjottava rekisteröidyille mahdollisuus valita (opt out), voiko heidän henkilötietojaan a) antaa kolmannelle osapuolelle ([1]) tai b) käyttää tarkoitukseen, joka ei vastaa tietojen keruun alkuperäistä tarkoitusta tai tarkoitusta, johon rekisteröity on myöhemmin antanut luvan. Rekisteröidyille on annettava selkeät, yksiselitteiset, helposti käytettävissä olevat ja kustannuksiltaan kohtuulliset keinot valintamahdollisuuden käyttämiseen.

Arkaluonteisten tietojen osalta (esim. henkilötiedot, jotka koskevat henkilön terveydentilaa, rotua tai etnistä alkuperää, poliittista kantaa, uskonnollista tai eettistä vakaumusta, kuulumista ammattiliittoon tai sukupuolista suuntautumista) kyseisten henkilöiden on tehtävä myönteinen tai selkeästi ilmaistu (opt in) valinta, jos tietoja aiotaan antaa kolmannelle osapuolelle tai käyttää muuhun kuin alkuperäiseen tarkoitukseen kuin mihin henkilö on aiemmin antanut selkeän suostumuksensa tehdessään valinnan (opt in). Organisaation on joka tapauksessa pidettävä arkaluontoisina kaikkia kolmannelta osapuolelta saatuja tietoja, jos kyseinen kolmas osapuoli ilmoittaa tiedot arkaluonteisiksi ja pitää niitä sellaisina.

TIEDON SIIRTÄMINEN EDELLEEN

Organisaatio voi antaa tietoja kolmannelle osapuolelle ainoastaan ilmoitus- ja valintaperiaatteiden mukaisesti. Organisaatio voi halutessaan antaa tietoja kolmannelle osapuolelle, joka toimii kyseisen organisaation puolesta (kuten alaviitteessä kuvataan), jos se ensin varmistaa, että kolmas osapuoli noudattaa safe harbor -periaatteita tai on direktiivin tai muun tietosuojan riittävyyden takaavan säädöksen alainen, taikka jos organisaatio tekee kolmannen osapuolen kanssa kirjallisen sopimuksen, jossa vaaditaan, että kolmas osapuoli tarjoaa vähintään

([1]) Ilmoitusta tai valintamahdollisuutta ei tarvita, kun tiedot annetaan kolmannelle osapuolelle, joka toimii kyseisen organisaation puolesta ja sen ohjeiden mukaisesti suorittaessaan tiettyä tehtävää (tai tehtäviä). Tällaiseen tietojen antamiseen sovelletaan kuitenkin tiedon edelleen siirtämistä koskevaa periaatetta.

▼B

samantasoisen suojan kuin vastaavilla safe harbor -periaatteilla taataan. Jos organisaatio noudattaa näitä edellytyksiä, sitä ei pidetä vastuullisena (ellei organisaatio itse toisin sovi), jos kolmas osapuoli, jolle se siirtää tietoja, käsittelee niitä rajoitusten tai ehtojen vastaisesti, lukuun ottamatta tapauksia, joissa organisaatio tietää tai sen pitäisi tietää, että kolmas osapuoli aikoo käsitellä tietoja periaatteiden vastaisesti eikä se ole ryhtynyt kohtuullisiin toimiin estääkseen tai keskeyttääkseen tällaisen tietojen käsittelyn.

TURVALLISUUS

Organisaatioiden, jotka luovat, säilyttävät, käyttävät tai toimittavat edelleen henkilötietoja, on toteutettava riittävät varotoimet tietojen katoamisen, väärinkäytösten ja vääriin käsiin joutumisen, paljastumisen, muuttamisen ja hävittämisen ehkäisemiseksi.

TIETOJEN KOSKEMATTOMUUS

Näiden periaatteiden mukaisesti henkilötietojen on liityttävä siihen tarkoitukseen, johon niitä on määrä käyttää. Organisaatio ei saa käsitellä henkilötietoja tavalla, joka ei sovi niiden alkuperäiseen käyttötarkoitukseen tai johon kyseinen henkilö ei ole antanut suostumustaan. Organisaation on toteutettava tarvittavat toimet sen varmistamiseksi, että tiedot ovat käyttötarkoitukseensa nähden luotettavia ja että ne ovat tarkkoja, täydellisiä ja ajantasaisia.

TIEDONSAANTI

Henkilöiden on saatava itseään koskevat tiedot organisaatiolta ja voitava korjata, muuttaa tai poistaa tiedot, jotka eivät ole paikkansapitäviä. Tätä ei kuitenkaan sovelleta, jos tiedonsaannista aiheutuvat ongelmat tai kustannukset olisivat suhteettoman suuret verrattuina tietosuojaan kohdistuviin riskeihin kyseisessä tapauksessa tai jos muun kuin kyseisen henkilön lakisääteisiä oikeuksia loukattaisiin.

TÄYTÄNTÖÖNPANO

Tehokkaaseen tietosuojaan on sisällyttävä menettelyt, joilla varmistetaan tietosuojaperiaatteiden noudattaminen ja organisaatiolle koituvat seuraamukset niiden noudattamatta jättämisestä. Siihen on myös sisällyttävä valitusmenettely, johon henkilö voi vedota silloin, kun häntä koskeviin tietoihin ei ole sovellettu periaatteita. Tällaisiin menettelyihin on sisällyttävä vähintäänkin seuraavat seikat: a) helposti käytettävissä oleva ja kohtuuhintainen riippumaton valitusmenettely, jolla tutkitaan kunkin henkilön valitus ja ratkaistaan kiistat tietosuojaperiaatteita noudattaen sekä myönnetään vahingonkorvaukset sovellettavan lainsäädännön tai yksityissektorin aloitteiden mukaisesti, b) seurantamenettelyt, joilla varmistetaan, että yritysten antamat vakuutukset niiden noudattamasta yksityisyyden suojasta pitävät paikkansa ja että yksityisyyden suoja on toteutettu esitetyllä tavalla ja c) organisaatioille asetettava velvoite korjata ongelmat, jotka johtuvat siitä, että ne eivät noudata ilmoittamallaan tavalla periaatteita, ja tällaisille organisaatioille koituvat seuraamukset. Seuraamusten on oltava riittävän vakavat, jotta niillä voidaan varmistaa, että organisaatiot noudattavat periaatteita.

▼B

Liite

Luettelo Euroopan unionin tunnustamista Yhdysvaltojen valtiollisista elimistä

Euroopan unioni tunnustaa, että seuraavilla Yhdysvaltojen valtiollisilla elimillä on valtuudet tutkia valituksia ja määrätä korvauksia sopimattomista ja harhaanjohtavista käytännöistä sekä tarjota oikeuskeinoja yksityisille, jos FAQ:iden mukaisesti sovellettavia periaatteita ei noudateta:

— Federal Trade Commission, jonka toimivalta perustuu Federal Trade Commission Act -lain 5 pykälään,

— Department of Transportation (Yhdysvaltojen liikenneministeriö), jonka toimivalta perustuu United States Coden 49 osaston 41712 pykälään.

▼B

LIITE II

TAVALLISIMMAT KYSYMYKSET (FAQ:t)

FAQ 1 — Arkaluonteiset tiedot

Kysymys: *Onko organisaation aina annettava nimenomainen valintamahdollisuus "opt in" arkaluonteisten tietojen osalta?*

Vastaus: Ei, tällaista valintaa ei vaadita, kun tietojen käsittely 1) on tarpeen rekisteröidyn tai muun henkilön elintärkeän edun suojaamiseksi; 2) on tarpeen oikeusvaateen laatimiseksi tai puolustamiseksi; 3) on tarpeen lääketieteellisen hoidon antamiseksi tai diagnoosin tekemiseksi; 4) suoritetaan poliittisen, filosofisen, uskonnollisen tai ammattiyhdistystoimintaan liittyvän säätiön, yhdistyksen tai minkä tahansa muun voittoa tavoittelemattoman elimen laillisen toiminnan yhteydessä ja sillä edellytyksellä, että käsittely koskee ainoastaan näiden elinten jäseniä tai henkilöitä, joilla on niihin säännölliset elinten tarkoituksiin liittyvät yhteydet ja että tietoja ei luovuteta sivullisille ilman rekisteröityjen suostumusta; 5) on tarpeen organisaation velvoitteiden noudattamiseksi työoikeuden alalla; tai 6) koskee tietoja, jotka henkilö on nimenomaisesti saattanut julkisiksi.

FAQ 2 — Journalistiset poikkeukset

Kysymys: *Sovelletaanko safe harbor -periaatteita journalistisia tarkoituksia varten kerättyihin, ylläpidettyihin tai levitettyihin henkilötietoihin ottaen huomioon Yhdysvaltojen perustuslain takaama lehdistön vapaus ja direktiivin journalistista aineistoa koskeva poikkeussääntö?*

Vastaus: Jos Yhdysvaltojen perustuslain ensimmäisessä muutoksessa ilmaistut vapaan lehdistön oikeudet ovat ristiriidassa yksityisyyden suojaan liittyvien etujen kanssa, perustuslain ensimmäisen muutoksen on ohjattava näiden etujen tasapainottamista yhdysvaltalaisten henkilöiden ja organisaatioiden toimien osalta. Safe harbor -periaatteiden vaatimukset eivät koske henkilötietoja, jotka on kerätty julkaisemista, radiolähetystoimintaa tai muuta journalistisen aineiston julkista viestintää varten siitä riippumatta, käytetäänkö tietoja vai ei, eivätkä tietoa, joka löytyy aikaisemmin julkaistusta tiedotusvälineiden arkistoista levitetystä aineistosta.

FAQ 3 — Toissijainen vastuu

Kysymys: *Ovatko Internet-palveluntarjoajat, televiestinnän harjoittajat tai muut organisaatiot safe harbor -periaatteiden mukaan vastuussa, jos ne toisen organisaation puolesta pelkästään siirtävät, reitittävät, välittävät tai varastoivat tietoja, jotka saattavat loukata näitä periaatteita?*

Vastaus: Eivät. Safe harbor -periaatteet eivät luo toissijaista vastuuta, mikä pitää paikkansa myös itse direktiivin osalta. Siinä määrin kuin organisaatio toimii pelkästään kolmansien osapuolien siirtämän tiedon kanavana eikä itse määrittele henkilötietojen käsittelyn tarkoitusta ja tapaa, se ei ole vastuussa.

FAQ 4 — Investointipankit ja tilintarkastukset

Kysymys: *Tilintarkastajien ja investointipankkien toimintaan saattaa sisältyä henkilötietojen käsittelyä ilman, että asianomainen henkilö on antanut siihen suostumuksensa tai tietää siitä. Millä edellytyksillä tämä on sallittua ilmoitusta, valintaa ja tiedonsaantia koskevien periaatteiden puitteissa?*

Vastaus: Investointipankit tai tilintarkastajat voivat käsitellä tietoja asianomaisen tietämättä ainoastaan siinä määrin ja niin kauan kuin on tarpeen lakisääteisten tai yleisen edun mukaisten vaatimusten täyttämiseksi, sekä lisäksi olosuhteissa, joissa näiden periaatteiden soveltaminen vaikuttaisi haitallisesti organisaation oikeutettuihin etuihin. Oikeutettuja etuja ovat muun muassa oikeus valvoa, että yritykset noudattavat lainmukaisia velvoitteitaan ja tilintarkastusmenettelyä, samoin kuin luottamuksellisuus, kun on kyse

▼B

mahdollisista yritysostoista, sulautumisista, yhteisyrityksistä, tai muista vastaavista investointipankkien tai tilintarkastajien toteuttamista toimista.

FAQ 5 ►C1 (1) ◄ — Tietosuojaviranomaisten tehtävä

Kysymys: *Miten EU-maiden tietosuojaviranomaisten kanssa tehtävään yhteistyöhön sitoutuvat yritykset tekevät sitoumuksensa ja miten ne pannaan täytäntöön?*

Vastaus: EU:sta henkilötietoja vastaanottavien yhdysvaltalaisten organisaatioiden on safe harbor -järjestelmässä sitouduttava käyttämään tehokkaita menettelyjä varmistaakseen safe harbor -periaatteiden noudattamisen. Niiden on etenkin, kuten täytäntöönpanoperiaatteessa on mainittu, a) järjestettävä valitusmahdollisuus henkilöille, joita tiedot koskevat, b) varmistettava seurannan avulla, että organisaatioiden antamat vakuutukset niissä noudatettavasta yksityisyyden suojaa koskevasta käytännöstä pitävät paikkansa, ja c) velvoitettava organisaatiot korjaamaan periaatteiden noudattamatta jättämisestä aiheutuvat ongelmat ja määrättävä organisaatioille tästä aiheutuvat seuraamukset. Organisaatio voi täyttää täytäntöönpanoperiaatteen a ja c kohdan vaatimukset noudattamalla tämän FAQ:n vaatimuksia yhteistyöstä tietosuojaviranomaisten kanssa.

Organisaatio voi sitoutua yhteistyöhön tietosuojaviranomaisten kanssa ilmoittamalla kauppaministeriölle osoittamassaan safe harbor -varmennuksessa (katso omaa varmennusta koskeva FAQ 6), että se

1) on päättänyt täyttää safe harbor -järjestelmän täytäntöönpanoperiaatteen a ja c kohdan mukaiset vaatimukset sitoutumalla yhteistyöhön tietosuojaviranomaisten kanssa;

2) tutkii ja ratkaisee safe harbor -järjestelmän mukaisesti tehdyt valitukset yhteistyössä tietosuojaviranomaisten kanssa; ja

3) noudattaa kaikkia tietosuojaviranomaisten antamia ohjeita, joiden mukaan sen on safe harbor -periaatteiden noudattamiseksi toteutettava erityistoimia, joihin kuuluvat myös oikeuskeinot ja korvaukset niiden asianosaisten hyväksi, joihin periaatteiden noudattamatta jättäminen on vaikuttanut, sekä antaa tietosuojaviranomaisille kirjallisen vahvistuksen edellä mainittujen toimien toteuttamisesta.

Tiedotuksesta ja neuvonnasta muodostuva tietosuojaviranomaisten yhteistyö järjestetään seuraavasti:

— Neuvonnasta vastaa Euroopan tasoinen epävirallinen tietosuojaviranomaisten paneeli, joka muun muassa auttaa yhtenäisen ja johdonmukaisen lähestymistavan varmistamisessa.

— Paneeli antaa yhdysvaltalaisille organisaatioille ohjeita yksityishenkilöiden tekemistä, ratkaistavina olevista valituksista, jotka koskevat Euroopasta safe harbor -järjestelmän mukaisesti siirrettyjen henkilötietojen käsittelyä. Näillä ohjeilla on tarkoitus varmistaa, että safe harbor -periaatteita sovelletaan asianmukaisesti. Ohjeet sisältävät myös tiedot asianosaiselle (asianosaisille) tarjottavista oikeuskeinoista, joita tietosuojaviranomaiset pitävät asianmukaisina.

— Paneeli antaa ohjeita tapauksista, joita organisaatiot ovat siirtäneet sen käsiteltäviksi, ja/tai tietosuojaviranomaisten kanssa safe harbor -yhteistyöhön sitoutuneita organisaatioita koskevista valituksista, jotka se saa suoraan yksityishenkilöiltä. Samalla se kannustaa ja tarvittaessa auttaa valituksen tekijöitä turvautumaan ensin organisaation sisäisiin valitusmenettelyihin.

— Ohjeet annetaan vasta, kun kiistan molemmilla osapuolilla on ollut asianmukainen tilaisuus esittää haluamansa huomiot ja todistusaineisto. Paneeli pyrkii antamaan ohjeet niin nopeasti kuin asianmukainen menettely sallii. Yleissääntönä on, että

(1) Tämän FAQ:n sisällyttäminen pakettiin riippuu tietosuojaviranomaisten suostumuksesta. Nämä ovat keskustelleet tästä tekstistä 29 artiklan mukaisessa työryhmässä, ja valtaosa pitää sitä hyväksyttävänä. Tietosuojaviranomaiset päättävät kuitenkin lopullisesta kannastaan yleisen lausunnon yhteydessä, jonka työryhmä antaa lopullisesta paketista.

▼B

paneeli antaa ohjeet 60 päivän kuluessa valituksen tai sille siirretyn tapauksen vastaanottamisesta tai mahdollisuuksien mukaan lyhyemmässä ajassa.

— Paneeli julkistaa vastaanottamiensa valitusten käsittelyn tulokset, jos se katsoo tämän tarpeelliseksi.

— Ohjeiden antaminen ei aseta paneelia tai yksittäisiä tietosuojaviranomaisia minkäänlaiseen vastuuseen.

Kuten edellä todettiin, tämän riitojenratkaisumenettelyn valitsevien organisaatioiden on sitouduttava noudattamaan tietosuojaviranomaisten ohjeita. Jos organisaatio ei noudata periaatteita 25 päivän kuluessa ohjeiden antamisesta eikä ole antanut tyydyttävää selitystä viivästykselle, paneeli ilmoittaa, että se siirtää asian Federal Trade Commissionille tai muulle Yhdysvaltain liitto- tai osavaltion elimelle, jolla on lakisääteiset täytäntöönpanovaltuudet vilpillistä tai harhauttavaa menettelyä koskevissa asioissa, tai että se pitää yhteistyösopimusta vakavan sopimusrikkomuksen vuoksi mitättömänä. Jälkimmäisessä tapauksessa paneeli ilmoittaa mitättömyydestä Yhdysvaltain kauppaministeriölle (tai sen nimeämälle edustajalle), jotta safe harbor -järjestelmään osallistuvien organisaatioiden luetteloa voidaan muuttaa tarvittavalla tavalla. Jos sitoumusta tietosuojaviranomaisten kanssa tehtävästä yhteistyöstä tai safe harbor -periaatteita ei noudateta, voidaan nostaa vilpillistä menettelyä koskeva kanne Federal Trade Commissionista annetun lain 5 pykälän tai muun vastaavan lain säännöksen nojalla.

Tämän vaihtoehdon valitsevilta organisaatioilta veloitetaan vuosimaksu, jolla on tarkoitus kattaa paneelin toimintakulut, ja organisaatioilta voidaan tämän lisäksi veloittaa tarpeelliset käännöskulut, joita aiheutuu, kun paneeli käsittelee niitä vastaan tehtyjä valituksia. Vuosimaksu on enintään 500 Yhdysvaltain dollaria, ja se on pienempi pienille yhtiöille.

Tietosuojaviranomaisten kanssa tehtävän yhteistyön voivat valita organisaatiot, jotka liittyvät safe harbor -järjestelmään sen kolmen toimintavuoden aikana. Tietosuojaviranomaiset tarkastelevat tätä vaihtoehtoa uudelleen kolmivuotisjakson lopulla, jos sen valinneiden yhdysvaltalaisten organisaatioiden määrä osoittautuu liian suureksi.

FAQ 6 — Oma varmennus

Kysymys: *Miten organisaatio voi käyttää omaa varmennusta todistaakseen, että se noudattaa safe harbor -periaatteita?*

Vastaus: Safe harbor -järjestelmän edut taataan siitä päivästä lähtien, kun organisaatio itse, jäljempänä esitettävien ohjeiden mukaisesti, ilmoittaa kauppaministeriölle (Department of Commerce) tai sen tähän tarkoitukseen nimeämälle edustajalle noudattavansa periaatteita.

Todistaakseen itse kelpoisuutensa osallistua safe harbor -järjestelmään organisaatiot voivat toimittaa kauppaministeriölle tai sen nimeämälle edustajalle järjestelmään liittyvää organisaatiota edustavan toimihenkilön allekirjoittaman kirjeen, joka sisältää vähintään seuraavat tiedot:

1) organisaation nimi, postiosoite, sähköpostiosoite, puhelin- ja faksinumerot;

2) kuvaus organisaation toiminnoista, jotka liittyvät EU:sta saataviin henkilötietoihin;

3) kuvaus tällaisia henkilötietoja koskevasta organisaation yksityisyyspolitiikasta, myös seuraavat tiedot: a) missä sitä koskevaa tietoa on yleisön saatavilla; b) sen tosiasiallinen täytäntöönpanopäivä; c) yhteystoimisto valitusten käsittelyä, tiedonsaantipyyntöjä ja muiden safe harbor -järjestelmään liittyvien kysymysten käsittelyä varten; d) erityinen lakisääteinen elin, joka on toimivaltainen käsittelemään kaikki mahdollisesti harhauttavia tai vilpillisiä käytäntöjä ja yksityisyyden suojaa koskevien lakien tai asetusten rikkomisia koskevat organisaatioon kohdistetut vaatimukset (ja joka mainitaan periaatteiden liitteessä); e) kaikkien niiden yksityisyyttä suojaavien ohjelmien nimet, joihin organisaatio on

▼B

liittynyt; f) todentamismenetelmä (esim. sisäinen tai sivullisen suorittama todentaminen) ([1]); ja g) riippumaton valitusmenettely, joka on käytettävissä ratkaisemattomien valitusten tutkimiseksi.

Jos organisaatio haluaa, että sen safe harbor -edut kattavat henkilöstöä koskevat tiedot, joita siirretään EU:sta käytettäväksi työsuhteen yhteydessä, se voi saada tällaisen kattavuuden siellä, missä on erityinen lakisääteinen elin, joka on toimivaltainen käsittelemään henkilöstöä koskevien tietojen suojaa koskevat organisaatioon kohdistetut vaatimukset ja joka mainitaan periaatteiden liitteessä. Lisäksi organisaation on ilmoitettava omassa varmennuksessaan, että se haluaa kattaa tällaiset henkilöstöä koskevat tiedot, että se sitoutuu tekemään yhteistyötä EU:n viranomaisten kanssa FAQ 9:n ja FAQ 5:n mukaisesti ja että se noudattaa näiden viranomaisten ohjeita.

Jos organisaatio haluaa, että sen safe harbor -edut kattavat henkilöstöä koskevat tiedot, joita siirretään EU:sta käytettäväksi työsuhteen yhteydessä, sen on ilmoitettava omassa varmennuksessaan, että se haluaa kattaa tällaisethenkilöstöä koskevat tiedot, että se sitoutuu tekemään yhteistyötä EU:n viranomaisten kanssa FAQ 9:n ja FAQ 5:n mukaisesti ja että se noudattaa näiden viranomaisten ohjeita.

Kauppaministeriö (tai sen nimeämä edustaja) pitää luetteloa kaikista organisaatioista, jotka ovat toimittaneet tällaisia kirjeitä, jolloin varmistetaan safe harbor -etujen käytettävyys. Se myös päivittää luettelon vuosittain toimitettavien kirjeiden ja FAQ 11:n mukaisesti saatujen ilmoitusten perusteella. Omaa varmennusta koskeva kirje on toimitettava vähintään vuosittain. Jos kirjettä ei toimiteta, kyseinen organisaatio poistetaan luettelosta eikä sille enää myönnetä safe harbor -etuja. Sekä luettelo että organisaatioiden toimittamat omaa varmennusta koskevat kirjeet saatetaan yleisesti saataville. Kaikkien organisaatioiden, jotka antavat oman varmennuksensa safe harbor -järjestelmää varten, on myös ilmoitettava julkaistavissa, tämän alan yksityisyyden suojaohjelmaa koskevissa lausunnoissaan, että ne noudattavat safe harbor -periaatteita.

Sitoutumista safe harbor -periaatteiden noudattamiseen ei rajoiteta ajallisesti niiden tietojen osalta, jotka organisaatio on saanut ollessaan oikeutettu safe harbor -etuihin. Sitoutuminen merkitsee, että organisaatio soveltaa periaatteita tällaisiin tietoihin niin kauan kuin organisaatio tallentaa, käyttää tai luovuttaa niitä, vaikka se olisi myöhemmin mistä tahansa syystä jättäytynyt safe harbor -järjestelmän ulkopuolelle.

Organisaation, joka lakkaa olemasta erillinen oikeudellinen yksikkö sulautumisen tai yritysoston seurauksena, on ilmoitettava kauppaministeriölle (tai sen nimeämälle edustajalle) tästä etukäteen. Ilmoitukseen on myös sisällyttävä tieto siitä, onko organisaation haltuun ottava yksikkö tai sulautumisessa muodostuva yksikkö 1) edelleen sidoksissa safe harbor -periaatteisiin yritysostoa tai sulautumista koskevan oikeustoimen kautta tai 2) haluaako se antaa oman varmennuksen safe harbor -periaatteiden noudattamisesta tai toteuttaa muita suojatoimenpiteitä, kuten kirjallisen sopimuksen, jolla taataan safe harbor -periaatteiden noudattaminen. Siinä tapauksessa, että kumpikaan vaihtoehdoista 1 ja 2 ei sovellu, kaikki safe harbor -järjestelyn kautta saadut tiedot on viipymättä tuhottava.

Organisaation ei tarvitse soveltaa safe harbor -periaatteita kaikkiin henkilötietoihin, mutta sen on sovellettava safe harbor -periaatteita kaikkiin niihin henkilötietoihin, jotka se saa EU:sta safe harbor -järjestelmään liittymisensä jälkeen.

Jos organisaatio antaa yleisölle vääriä tietoja safe harbor -periaatteiden noudattamisesta, liittovaltion kauppakomissio (Federal Trade Commission) tai muu asianomainen hallintoelin voi nostaa organisaatiota vastaan kanteen. Kauppaministeriölle (tai sen nimeämälle edustajalle) toimitetut väärät tiedot voivat johtaa toimiin vääristä ilmoituksista annetun False Statements Act -lain (18USC § 1001) nojalla.

([1]) Ks. todentamista koskeva FAQ 7.

▼B

FAQ 7 — Todentaminen

Kysymys: *Miten organisaatiot järjestävät seurantamenettelyn, jolla varmistetaan, että niiden antamat vakuutukset safe harbor -järjestelmän mukaisesta yksityisyyden suojasta pitävät paikkansa ja että tällainen yksityisyyden suoja on toteutettu esitetyllä tavalla ja safe harbor -periaatteiden mukaisesti?*

Vastaus: Täyttääkseen täytäntöönpanoperiaatteen mukaiset todentamisvaatimukset organisaatio voi todentaa annettujen vakuutusten paikkansapitävyyden arvioinnilla, jonka suorittaa organisaatio itse tai jokin ulkopuolinen taho.

Itsearvioinnista olisi käytävä ilmi, että organisaation ilmoittaman, EU:n alueelta saatuja henkilötietoja koskeva yksityisyyden suojamenettely on täsmällinen, kattava, selkeästi esitetty, täydellisesti toteutettu ja helposti käytettävissä. Lisäksi arvioinnin olisi osoitettava, että organisaation menettely on safe harbor -periaatteiden mukainen, että rekisteröidylle kerrotaan organisaation sisäisestä valitusmenettelystä ja käytettävissä olevista organisaatiosta riippumattomista valitusmenettelyistä, että organisaation henkilöstö saa koulutusta menettelyn toteuttamiseksi ja laiminlyöntitapauksia varten on kurinpitomenettely ja että organisaatiolla on sisäiset menettelyt, joilla ajoittain arvioidaan objektiivisesti edellä mainittujen vaatimusten täyttymistä. Yrityksen toimihenkilön tai muun valtuutetun edustajan on vähintään kerran vuodessa allekirjoitettava itsearviointia koskeva ilmoitus, joka on saatettava rekisteröityjen tietoon joko heidän pyynnöstään taikka tutkinnan tai periaatteiden noudattamatta jättämistä koskevan valitusmenettelyn yhteydessä.

Organisaatioiden on pidettävä kirjaa safe harbor -järjestelmän mukaisten yksityisyyden suojaa koskevien käytänteidensä täytäntöönpanosta, jotta tutkinnan tai valitusmenettelyn yhteydessä tietoja voidaan pyynnöstä toimittaa valituksia käsittelevälle riippumattomalle elimelle tai elimelle, jolla on toimivalta sopimattomia ja harhaanjohtavia käytäntöjä koskevissa asioissa.

Jos organisaatio on valinnut ulkopuolisen suorittaman arvioinnin, siitä on käytävä ilmi, että EU:n alueelta saatuja henkilötietoja koskeva yksityisyyden suojamenettely on safe harbor -periaatteiden mukainen, että menettelyä noudatetaan ja että asianomaisille kerrotaan valitusmenettelyistä. Arviointimenetelmille ei ole rajoituksia: arviointiin voidaan käyttää haastatteluja, sattumanvaraisia tarkastuksia, houkuttimia, teknisiä apuvälineitä tai muita sopivia keinoja. Arvioinnista laaditaan vähintään kerran vuodessa ilmoitus, josta käy ilmi, että arviointion viety onnistuneesti loppuun. Ilmoituksessa on oltava arvioijan, yrityksen toimihenkilön tai muun sen valtuuttaman edustajan allekirjoitus. Ilmoituksen on pyynnöstä oltava asianomaisten saatavilla, ja sen on oltava käytettävissä periaatteiden noudattamista koskevan tutkinnan tai valitusmenettelyn yhteydessä.

FAQ 8 — Tiedonsaanti

Tiedonsaantiperiaate

Henkilöiden on saatava itseään koskevat tiedot organisaatiolta ja voitava korjata, muuttaa tai poistaa tiedot, jotka eivät ole paikkansapitäviä. Tätä ei kuitenkaan sovelleta, jos tiedonsaannista aiheutuvat ongelmat tai kustannukset olisivat suhteettoman suuret verrattuina tietosuojaan kohdistuviin riskeihin kyseisessä tapauksessa tai jos muun kuin kyseisen henkilön lakisääteisiä oikeuksia loukattaisiin.

Kysymys 1: *Onko tiedonsaantioikeus absoluuttinen?*

Vastaus 1: Ei. Safe harbor -periaatteiden mukaan tiedonsaanti on yksityisyyden suojan perusoikeuksia. Sen perusteella rekisteröity voi tarkistaa häntä itseään koskevan tiedon paikkansapitävyyden. Kuitenkin organisaation velvollisuuteen antaa henkilölle häntä itseään koskevaa tietoa sovelletaan suhteellisuus- tai kohtuusperiaatetta, ja tietyissä tapauksissa oikeutta on lievennettävä. Vuonna 1980 hyväksytyistä yksityisyyden suojaa koskevien OECD:n suuntaviivojen perusteluista käy selkeästi ilmi, ettei organisaation tiedonantovelvollisuus ole absoluuttinen. Velvollisuus ei edellytä esimerkiksi haasteen vaatimaa äärimmäisen

▼B

perusteellista tiedonhakua tai tiedonsaantia kaikista organisaation rekisterimuodoista.

Kokemus on pikemminkin osoittanut, että rekisteröidyn tiedonsaantipyyntöön vastatessaan organisaation on kiinnitettävä huomiota siihen, miksi tietoja halutaan. Jos tiedonsaantipyyntö on esimerkiksi epämääräinen tai laaja-alainen, organisaatio voi tiedustella asiaa kyseiseltä henkilöltä, jotta tilanne ymmärrettäisiin paremmin ja jotta halutut tiedot löytyisivät helpommin. Organisaatio saattaa haluta tietää, minkä osaston kanssa rekisteröity on ollut yhteydessä ja millaisesta tiedosta on kyse (tai mikä on sen käyttötarkoitus). Rekisteröidyn ei kuitenkaan tarvitse perustella pyyntöään saada häntä itseään koskevat tiedot.

Kustannukset ja tietojen antamisesta aiheutuvat rasitteet on tärkeinä tekijöinä otettava huomioon, mutta niiden perusteella ei päätetä, onko tiedon antaminen kohtuullista. Jos tietoa esimerkiksi käytetään yksityishenkilöä koskevan tärkeän päätöksen tekemiseen (merkittävien etujen myöntäminen tai kieltäminen, vakuutus, laina, työpaikka jne.), organisaation on annettava tiedot muiden FAQ-kysymysten mukaisesti, vaikka tietojen hankkiminen olisi suhteellisen vaikeaa tai kallista.

Jos pyydetty tieto ei ole arkaluonteista tai sitä ei käytetä rekisteröidyn elämään merkittävästi vaikuttavaan päätöksentekoon (esim. ei-arkaluonteinen markkinointitieto, jonka avulla päätetään, lähetetäänkö henkilölle myyntiluettelo vai ei), vaan tieto on helposti saatavilla ja tiedonhaku on edullista, organisaation on annettava rekisteröidylle hallussaan olevat rekisteröityä koskevat tiedot. Näihin tietoihin voi kuulua tietoja, jotka on saatu henkilöltä itseltään tai ulkopuolisilta tai hänen kanssaan tehtyjen liiketoimien yhteydessä.

Tiedonsaantiperiaatteen perimmäisen luonteen mukaisesti organisaatioiden olisi aina vilpittömästi pyrittävä antamaan tietoja. Mikäli esimerkiksi tietyt tiedot on suojattava ja ne voidaan helposti erottaa muusta haettavasta tiedosta, organisaation on erotettava suojattu tieto ja julkistettava muu tieto. Jos organisaatio päättää, että tietoja ei anneta yksittäisessä tapauksessa, päätös on perusteltava tietoja pyytävälle rekisteröidylle ja ilmoitettava, mistä tai keneltä saa asiasta lisätietoja.

Kysymys 2: *Mikä on luottamuksellista kaupallista tietoa, ja voiko organisaatio kieltäytyä antamasta tällaista tietoa suojellakseen sitä?*

Vastaus 2: Luottamuksellinen kaupallinen tieto (termiä käytetään Yhdysvaltojen liittovaltion säännöissä Federal Rules of Civil Procedure on discovery) on yrityksen suojelemaa tietoa, jonka julkaiseminen auttaisi kilpailijan toimintaa markkinoilla. Yrityksen käyttämä tietty tietokoneohjelma (kuten mallinnusohjelma) tai sen osat voivat olla luottamuksellista kaupallista tietoa. Jos luottamuksellinen kaupallinen tieto on erotettavissa muusta tiedonsaantipyynnön kohteena olevasta tiedosta, organisaation on erotettava luottamuksellinentieto ja julkistettava ei-luottamuksellinen tieto. Organisaatio voi kieltää tiedonsaannin tai rajoittaa sitä, jos tietoja antamalla paljastettaisiin (edellä annetun määritelmän mukaisesti) sen omaa luottamuksellista kaupallista tietoa, esimerkiksi kyseisen organisaation markkinapäätelmiä tai luokituksia taikka toisen organisaation luottamuksellista kaupallista tietoa, jos tällaista tietoa koskee sopimukseen perustuva luottamuksellisuusvelvoite tilanteessa, jossa tällainen luottamuksellisuusvelvoite yleensä on voimassa tai määrätään.

Kysymys 3: *Voiko organisaatio luovuttaessaan rekisteröidylle häntä itseään koskevia tietoja antaa hänelle tietokannasta haettuja tietoja vai pitääkö organisaation antaa kyseiselle henkilölle mahdollisuus käyttää itse tietokantaa?*

Vastaus 3: Organisaatio luovuttaa rekisteröidylle halutut tiedot; tiedonsaanti ei edellytä mahdollisuutta käyttää organisaation tietokantaa.

Kysymys 4: *Onko organisaation järjestettävä tietokantansa uudelleen, jotta tiedonsaanti olisi mahdollista?*

Vastaus 4: Tietoja on annettava vain siinä määrin kuin organisaatio tallentaa tietoja. Tiedonsaantiperiaate ei sinänsä velvoita säilyttämään tai ylläpitämään henkilötietoja, järjestämään niitä uudelleen tai muuttamaan tietokantojen rakennetta.

Kysymys 5: *Vastauksista käy selvästi ilmi, että tiedonsaanti voidaan estää tietyissä tapauksissa. Missä muissa tapauksissa organisaatio voi*

▼B

kieltäytyä antamasta rekisteröidylle häntä itseään koskevaa henkilötietoa?

Vastaus 5: Tällaiset tapaukset on rajattu, ja kaikki tiedonsaannin estämisen syyt on eriteltävä. Organisaatio voi kieltäytyä antamasta tietoja, jos tietojen luovuttaminen todennäköisesti vaarantaa yleisen edun, esimerkiksi valtion turvallisuuden, puolustuksen tai yleisen turvallisuuden. Lisäksi tiedonsaanti voidaan estää, kun tietoja käsitellään pelkästään tutkimus- tai tilastotarkoituksiin. Muita tiedonsaannin estäviä tai sitä rajoittavia syitä ovat seuraavat:

a) tietojen luovuttaminen haittaa lain täytäntöönpanoa, mukaan luettuina rikosten ehkäisy, tutkinta ja selville saaminen tai oikeus puolueettomaan oikeudenkäyntiin;

b) tietojen luovuttaminen haittaa oikeudenkäynnin perustetta siviilioikeudellisessa asiassa, mukaan luettuina oikeusvaateiden estäminen, tutkinta tai selvittäminen tai oikeus puolueettomaan oikeudenkäyntiin;

c) luotettavat henkilötiedot sisältävät viittauksia muihin henkilöihin, ja tällaisia viittauksia ei voida poistaa;

d) tietojen luovuttaminen rikkoo lainmukaista tai muuta ammatillista etuoikeutta tai velvoitetta;

e) tietojen luovuttaminen rikkoo luottamuksellisuuden, jota tulevat tai meneillään olevat neuvottelut edellyttävät, esimerkkinä pörssiyhtiöiden hankintaan liittyvät neuvottelut;

f) tietojen luovuttaminen vaarantaa työntekijöihin liittyvät turvallisuustutkimukset tai valitusten käsittelyn;

g) tietojen luovuttaminen vaarantaa tiettynä rajoitettuna aikana vaaditun luottamuksellisuuden esimerkiksi henkilöstösuunnittelussa ja yrityksen uudelleenorganisoinnissa;

h) tietojen luovuttaminen vaarantaa luottamuksellisuuden, joka voi olla tarpeen terveeseen talous- ja rahoitushallintoon liittyvän johtamisen, tutkinnan tai sääntelytoimien yhteydessä; tai

i) muut olosuhteet, joissa tietojen antamisesta aiheutuvat rasitteet tai kustannukset olisivat suhteettoman suuret tai tietojen antaminen loukkaisi muiden laillisia oikeuksia tai etuja.

Organisaation, joka kieltäytyy luovuttamasta tietoja, on osoitettava, että kieltäytyminen on asianmukainen (kuten tavallisesti menetellään). Kuten edellä todettiin, rekisteröidylle on kerrottava syyt, miksi tietoja ei anneta tai niiden saantia rajoitetaan, ja ilmoitettava yhteystiedot lisätiedusteluja varten.

Kysymys 6: *Voiko organisaatio vaatia maksun, joka kattaa tiedonhaun kustannukset?*

Vastaus 6: Kyllä. OECD:n suuntaviivoissa todetaan, että organisaatio voi periä maksun edellytyksellä, että maksu ei ole kohtuuton. Organisaatio voi siis periä tiedonsaannista kohtuullisen maksun. Maksun periminen saattaa olla hyödyksi pyrittäessä vähentämään toistuvia ja kiusalla esitettyjä hakupyyntöjä.

Yleisesti saatavilla olevia tietoja myyvät organisaatiot voivat periä tiedonhausta normaalisti perimänsä maksun. Rekisteröidyt voivat vaihtoehtoisesti pyytää tiedot suoraan organisaatiolta, joka alun perin keräsi ne.

Tiedonsaantia ei voida estää kustannussyihin vetoamalla, jos rekisteröity tarjoutuu maksamaan kustannukset.

Kysymys 7: *Onko organisaation annettava julkisista rekistereistä saatuja henkilötietoja?*

Vastaus 7: Ensiksikin on täsmennettävä, että julkisilla rekistereillä tarkoitetaan kaikkia hallinnon tasoja edustavien viranomaisten ylläpitämiä rekistereitä, jotka ovat suurelle yleisölle avoimia. Tiedonsaantia tai edelleen siirtoa koskevia periaatteita ei tarvitse soveltaa tällaiseen tietoon, mikäli siihen ei ole yhdistetty muuta henkilötietoa, joksi ei katsota pienten ei-julkisten henkilötietomäärien käyttöä julkisen rekisteritiedon luettelointiin tai järjestämiseen. Kaikkia toimivaltaisen viranomaisen vahvistamia rekisterin käytön edellytyksiä on kuitenkin noudatettava. Kun julkisten rekisterien sisältämää tietoa yhdistetään näihin rekistereihin kuulumattomiin tietoihin (muuhun

▼B

kuin edellä mainittuun tietoon), organisaation on kuitenkin sallittava tiedonsaanti edellyttäen, ettei kyseiseen tietoon sovelleta muita sallittuja poikkeuksia.

Kysymys 8: *Onko tiedonsaantiperiaatetta sovellettava yleisesti saatavilla oleviin henkilötietoihin?*

Vastaus 8: Samoin kuin julkisista rekistereistä saatujen tietojen kohdalla (katso kysymys 7) tiedonsaantiperiaatetta ei tarvitse soveltaa tietoon, joka jo on julkisesti yleisön saatavilla, sillä edellytyksellä, että tällaista tietoa ei ole yhdistetty tietoon, joka ei ole yleisesti saatavilla.

Kysymys 9: *Kuinka organisaatio voi suojautua toistuvilta tai kiusalla esitetyiltä tiedonsaantipyynnöiltä?*

Vastaus 9: Organisaation ei tarvitse vastata tällaisiin tiedonsaantipyyntöihin. Näistä syistä organisaatio voi periä tiedonhausta kohtuullisen maksun ja asettaa kohtuulliset rajoitukset sille, kuinka moneen saman henkilön tiedonsaantipyyntöön voidaan vastata tiettynä ajanjaksona. Asettaessaan rajoituksia organisaation on otettava huomioon, kuinka usein tietoja päivitetään, mihin tarkoitukseen tietoja käytetään ja minkä luonteista tieto on.

Kysymys 10: *Kuinka organisaatio voi suojautua vilpillisiltä tiedonsaantipyynnöiltä?*

Vastaus 10: Organisaation ei tarvitse antaa tietoja, ellei se saa tarpeeksi tietoa voidakseen varmistua tiedonsaantipyynnön esittäneen henkilöllisyydestä.

Kysymys 11: *Onko tiedot annettava tietyn ajan kuluessa tiedonsaantipyynnön vastaanottamisesta?*

Vastaus 11: Kyllä. Organisaation on vastattava ilman aiheetonta viivytystä kohtuullisen ajan kuluessa. Tämä vaatimus voidaan täyttää monella tavalla, kuten vuonna 1980 hyväksyttyjen yksityisyyden suojaa koskevien OECD:n suuntaviivojen perusteluista käy ilmi. Rekisteröidyille säännöllisesti tietoa antavan rekisterinpitäjän ei esimerkiksi välttämättä tarvitse heti vastata yksittäisiin kyselyihin.

FAQ 9 — Henkilöstö

Kysymys 1: *Sovelletaanko safe harbor -periaatteita EU:sta Yhdysvaltoihin siirrettäviin henkilötietoihin, jotka on kerätty työsuhteen vuoksi?*

Vastaus 1: Kyllä. Kun EU:ssa toimiva yritys siirtää henkilöstöltään työsuhteen yhteydessä (entisistä tai nykyisistä työntekijöistä) kerättyjä henkilötietoja Yhdysvalloissa sijaitsevalle emo- tai tytäryhtiölle tai riippumattomalle palvelujen tarjoajalle, joka osallistuu safe harbor -järjestelmään, tiedon siirtoon sovelletaan safe harbor -periaatteita.Näissä tapauksissa tietojen keräämiseen ja niiden käsittelyyn ennen siirtoa on sovellettu kyseisen EU-maan kansallista lainsäädäntöä, ja kaikkia tämän lainsäädännön mukaisia tietojen siirtoa koskevia ehtoja ja rajoituksia on noudatettava.

Safe harbor -periaatteita sovelletaan vain silloin kun yksittäinen, tunnistettava rekisteritieto siirretään tai annetaan käyttöön. Aggregoituun työllisyystietoon perustuvat tilastotiedot ja/tai tiedot, joista nimet on poistettu tai muutettu, eivät aiheuta yksityisyyden suojaan liittyviä ongelmia.

Kysymys 2: *Miten ilmoitusta ja valintaa koskevia periaatteita sovelletaan tällaiseen tietoon?*

Vastaus 2: Henkilöstöä koskevia tietoja EU:sta safe harbor -järjestelmän mukaisesti vastaanottanut yhdysvaltalainen organisaatio voi luovuttaa tiedot kolmannelle osapuolelle ja/tai käyttää niitä muuhun kuin alkuperäiseen käyttötarkoitukseen ainoastaan ilmoitusta ja valintaa koskevien periaatteiden mukaisesti. Jos organisaatio aikoo esimerkiksi käyttää työsuhteen vuoksi kerättyjä henkilötietoja muuhun kuin työsuhteeseen liittyvään tarkoitukseen, kuten markkinointiin, kyseisen yhdysvaltalaisen organisaation on tarjottava työntekijöille valintamahdollisuus ennen tietojen käyttämistä, elleivät työntekijät ole jo aiemmin antaneet lupaa tietojen käyttöön tällaisiin tarkoituksiin. Jos työntekijät kieltävät tietojen käyttämisen, heidän tekemänsä valinta ei saa rajoittaa heidän uramahdollisuuksiaan eikä heitä saa rangaista siitä.

On huomattava, että joistakin jäsenvaltioista tehtäviin tiedonsiirtoihin sovelletaan tiettyjä yleisiä ehtoja, jotka voivat rajoittaa

▼B

tällaisten tietojen muuta käyttöä myös sen jälkeen, kun tiedot on siirretty EU:n ulkopuolelle, ja näitä ehtoja on noudatettava.

Lisäksi työnantajien on kohtuullisin pyrkimyksin pidettävä huolta siitä, että henkilötietojen käyttöä koskevia henkilöstön valintoja noudatetaan. Tämä merkitsee esimerkiksi sitä, että rajoitetaan tietokannan käyttöä, esitetään tietyt tiedot anonyymeinä tai käytetään nimien sijasta koodeja tai salanimiä, jos oikeiden nimien käyttö ei liikkeenjohdollisista syistä ole välttämätöntä.

Jotta organisaation lailliset edut eivät vaarantuisi esimerkiksi nimityksiä, ylennyksiä ja muita henkilöstöön liittyviä päätöksiä koskevissa asioissa, sen ei tarvitse antaa ilmoitusta tai valintamahdollisuutta siinä määrin ja sinä aikana kuin on tarpeen.

Kysymys 3: *Miten tiedonsaantiperiaatetta sovelletaan?*

Vastaus 3: Tiedonsaantia koskevat FAQ:t antavat tietoja syistä, joiden perusteella voidaan kieltäytyä antamasta pyydettyjä henkilöstöä koskevia tietoja tai rajoittaa niiden saantia. Euroopan unionin työnantajien on luonnollisesti noudatettava paikallisia säädöksiä ja varmistettava, että eurooppalaiset (EU) työntekijät saavat tietoja kotimaansa lainsäädännön mukaisesti huolimatta siitä, missä tietoja käsitellään ja säilytetään. Safe harbor -periaatteet edellyttävät, että tällaista tietoa Yhdysvalloissa käsittelevä organisaatio tekee asiassa yhteistyötä ja antaa tiedot joko suoraan tai eurooppalaisen työnantajan kautta.

Kysymys 4: *Miten safe harbor -järjestelmään kuuluviin henkilöstöä koskeviin tietoihin liittyvät määräykset pannaan täytäntöön?*

Vastaus 4: Jos tietoa käytetään ainoastaan työsuhteen yhteydessä, työntekijän osalta tiedoista on ensisijaisesti vastuussa EU:ssa toimiva yritys. Tästä seuraa se, että jos eurooppalaiset työntekijät valittavat tietosuojaoikeuksiensa rikkomisesta eivätkä ole tyytyväisiä sisäisen tarkastuksen tai valitus- ja muutoksenhakumenettelyn tulokseen (tai jonkin ammattiliiton kanssa tehdyn sopimuksen mukaisesti sovellettavan valitusmenettelyn tulokseen), heidän on käännyttävä valtion tai osavaltion tietosuojaviranomaisen puoleen tai kyseisen alan työvoimaviranomaisen puoleen. Tähän sisältyvät myös tapaukset, joissa työntekijöiden henkilötietojen väärinkäytön väitetään tapahtuneen Yhdysvalloissa, jotka ovat tietoja työnantajalta vastaanottaneen yhdysvaltalaisen organisaation vastuulla eivätkä työnantajan vastuulla ja joissa näin ollen olisi rikottu safe harbor -periaatetta eikä siis direktiivin täytäntöön panemiseksi annettuja kansallisia säädöksiä. Tämä on tehokkain tapa selviytyä työlainsäädännön, työsopimusten ja tietosuojasäädösten usein päällekkäisistä määräyksistä.

Safe harbor -järjestelmään osallistuvan yhdysvaltalaisen organisaation, joka käyttää työsuhteen yhteydessä Euroopan unionista toimitettua, eurooppalaisia (EU) työntekijöitä koskevaa tietoa ja haluaa kyseisten tiedonsiirtojen kuuluvan safe harbor -järjestelyn piiriin, olisi tämän vuoksi sitouduttava yhteistyöhön toimivaltaisten Euroopan unionin viranomaisten toteuttamissa tutkintatapauksissa ja noudatettava näissä asioissa kyseisten viranomaisten antamia ohjeita. Ne tietosuojaviranomaiset, jotka ovat hyväksyneet tällaisen yhteistyön,ilmoittavat tästä Euroopan komissiolle ja Yhdysvaltojen kauppaministeriölle. Jos safe harbor -järjestelmään osallistuva yhdysvaltalainen organisaatio haluaa siirtää henkilöstöä koskevia tietoja sellaisesta jäsenvaltiosta, jonka tietosuojaviranomaiset eivät ole hyväksyneet kyseistä yhteistyötä, sovelletaan FAQ 5:n säännöksiä.

FAQ 10 — 17 artiklan mukaiset sopimukset

Kysymys: *Kun tietoa siirretään EU:sta Yhdysvaltoihin ainoastaan käsittelytarkoituksessa, onko tästä laadittava sopimus riippumatta siitä, kuuluuko tietojen käsittelijä safe harbor -järjestelmään?*

Vastaus: Kyllä. Eurooppalaisen rekisterinpitäjän on tehtävä sopimus aina, kun siirretään tietoja pelkästään käsittelytarkoituksessa riippumatta siitä, käsitelläänkö tiedot EU:ssa vai sen ulkopuolella. Sopimuksen tarkoituksena on turvata rekisterinpitäjän edut; rekisterinpitäjällä tarkoitetaan henkilöä tai elintä, joka päättää tietojen käsittelyn tarkoituksesta ja keinoista ja joka on tiedoista vastuussa kyseisille rekisteröidyille. Sopimuksessa täsmennetään toteutettava tietojen käsittely ja tietojen suojaamiseksi tarvittavat toimet.

▼B

Safe harbor -järjestelmään kuuluvan yhdysvaltalaisen organisaation, joka vastaanottaa EU:sta henkilötietoja pelkästään käsittelytarkoituksessa, ei tarvitse soveltaa näihin tietoihin safe harbor -periaatteita, koska EU:ssa toimiva rekisterinpitäjä on edelleen rekisteröityyn nähden vastuussa tätä koskevien EU-säädösten mukaisesti (jotka saattavat olla tiukempia kuin vastaavat safe harbor -periaatteet).

Koska safe harbor -järjestelmään osallistuvat takaavat riittävän tietosuojan, siihen kuuluvien organisaatioiden kanssa tehtävät, pelkkää tietojen käsittelyä koskevat sopimukset eivät edellytä ennakkolupaa (tai jäsenvaltio myötää tällaisen luvan automaattisesti), toisin kuin sopimukset, joissa tietojen vastaanottajat eivät osallistu safe harbor -järjestelmään tai eivät muutoin takaa riittävää tietosuojaa.

FAQ 11 — Riitojen ratkaisu ja järjestelmän täytäntöönpano

Kysymys 11: *Miten täytäntöönpanoperiaatteeseen kuuluva riitojen ratkaisu toteutetaan ja miten toimitaan, jos organisaatio jatkuvasti rikkoo periaatteita?*

Vastaus 11: Täytäntöönpanoperiaatteessa ilmaistaan safe harbor -järjestelmän täytäntöönpanon edellytykset. Todentamista koskevassa FAQ 7:ssä käsitellään periaatteen b kohdassa esitettyjen edellytysten täyttämistä. Tässä FAQ 11:ssä käsitellään periaatteen a ja c kohtia, joissa edellytetään riippumatonta valitusmenettelyä. Nämä menettelyt voivat olla erilaisia, mutta niiden on oltava täytäntöönpanoperiaatteen edellytysten mukaisia. Organisaatiot täyttävät edellytykset: 1) noudattamalla yksityisen sektorin laatimaa yksityisyydensuojaohjelmaa, jonka sääntöihin sisältyvät safe harbor -periaatteet ja johon kuuluu tehokkaita ja täytäntöönpanoperiaatteessa kuvatun kaltaisia täytäntöönpanovälineitä, 2) noudattamalla yksittäisiä valituksia käsittelevien ja riitoja ratkaisevien valvontaviranomaisten ohjeita tai 3) sitoutumalla yhteistyöhön Euroopan yhteisön alueella toimivien tietosuojaviranomaisten tai niiden valtuutettujen edustajien kanssa. Tämä luettelo on esimerkinomainen eikä se ole kattava. Yksityisellä sektorilla voidaan laatia muita menettelyjä täytäntöönpanon varmistamiseksi, kunhan tällaiset järjestelmät täyttävät täytäntöönpanoperiaatteessa ja tavallisimmissa kysymyksissä (FAQ:issa) esitetyt edellytykset. On huomattava, että täytäntöönpanoperiaatteessa esitetyt edellytykset ovat lisäys niihin edellytyksiin, jotka on esitetty periaatteiden kolmannessa johdantokappaleessa ja joiden mukaan itsesääntelytoimien on oltava kannekelpoisia sopimattomat ja harhaanjohtavat toimet kieltävän Federal Trade Commission Act -lain 5 pykälän tai muun vastaavan säädöksen nojalla.

Valitusmenettely:

Kuluttajia olisi rohkaistava tekemään valitus kyseiselle organisaatiolle ennen turvautumista riippumattomaan valitusmenettelyyn. Valitusmenettelyn riippumattomuus voidaan osoittaa useilla eri tavoilla, esimerkiksi kyseisen elimen avoimen kokoonpanon ja rahoituksen tai aikaisempien päätösten perusteella. Kuten täytäntöönpanoperiaatteessa edellytetään, yksityishenkilöille tarkoitetun valitusmenettelyn on oltava helpostisaatavilla ja kohtuuhintainen. Riitojen ratkaisusta vastaavien elinten on tutkittava kaikki yksityishenkilöiltä tulleet valitukset, elleivät ne ole ilmeisen perusteettomia tai aiheettomia. Tästä huolimatta valitusmenettelystä vastaava organisaatio voi asettaa kelpoisuusvaatimuksia valituksille, mutta tällaisten vaatimusten on oltava avoimia ja perusteltuja (voidaan esim. hylätä valitukset, jotka eivät kuulu ohjelman alaan tai jotka on käsiteltävä toisella foorumilla), eivätkä ne saa vaarantaa sitoutumista aiheellisten valitusten tutkimiseen. Lisäksi valitusmenettelyssä on tarjottava kattavaa ja helposti saatavilla olevaa tietoa riitojenratkaisumenettelyn toiminnasta yksityishenkilöille, jotka jättävät valituksen. Näihin tietoihin pitäisi sisältyä valitusmenettelyyn kuuluva, safe harbor -periaatteiden mukainen yksityisyydensuoja ([1]). Valitusmenettelystä

([1]) Riitojen ratkaisusta vastaavien elinten ei välttämättä tarvitse noudattaa täytäntöönpanoperiaatetta. Ne voivat myös ratkaisuissaan poiketa periaatteesta, jos tapaukseen liittyy ristiriitaisia velvoitteita tai nimenomainen lupa.

▼B

vastaavien organisaatioiden olisi toimittava yhteistyössä kehittääkseen välineitä, joilla helpotetaan valitusten ratkaisumenettelyä. Tällaisia välineitä ovat mm. vakiomuotoiset valituslomakkeet.

Oikeuskeinot ja seuraamukset:

Riitojen ratkaisusta vastaavan elimen päätösten seurauksena pitäisi olla se, että organisaatio mahdollisuuksien mukaan peruuttaa tai korjaa periaatteiden rikkomisen vaikutukset ja että vastaisuudessa tietoja käsitellään periaatteiden mukaisesti tai että soveltuvin osin valituksen tehneen henkilön tietojen käsittely lopetetaan. Seuraamusten on oltava riittävän ankaria, jotta ne selvästi kannustavat periaatteiden noudattamiseen. Kun käytössä on vakavuudeltaan eri asteisia seuraamuksia, voidaan eri asteisiin periaatteiden rikkomistapauksiin reagoida sopivin keinoin. Seuraamuksia ovat mm. rikkomistapausten julkistaminen ja tietyissä tapauksissa tietojen poistovaatimus ([1]). Muita seuraamuksia ovat ohjelman tunnuksen käyttöoikeuden keskeyttäminen ja poistaminen, periaatteiden rikkomisesta kyseisille henkilöille koituneiden menetysten korvaaminen sekä kieltomääräykset. Yksityisellä sektorilla toimivien riitojen ratkaisusta tai itsesääntelystä vastaavien elinten on ilmoitettava tapauksen mukaan tuomioistuimelle tai asiassa toimivaltaiselle valtiolliselle elimelle sellaiset tapaukset, joissa safe harbor -järjestelmään kuuluva organisaatio ei noudata niiden päätöksiä, sekä ilmoitettava niistä kauppaministeriölle (tai sen nimeämälle edustajalle).

FTC:n toiminta:

FTC on sitoutunut asettamaan tarkastelussaan ensisijalle tapaukset, jotka on sille toimittanut yksityisyydensuojan itsesääntelystä vastaava organisaatio, kuten BBBOnline tai TRUSTe tai EU:n jäsenvaltio, joka katsoo, että safe harbor -periaatteita ei ole noudatettu. FTC tutkii tällöin, onko toiminnassa rikottu FTC:tä koskevan säädöksen (FTC Act) 5 pykälää, jossa kielletään sopimattomat ja harhaanjohtavat toimet ja käytännöt kaupan alalla. Jos FTC katsoo, että sillä on syy (syitä) uskoa, että 5 pykälää on rikottu, se voi ratkaista asian hakemalla hallinnollista kieltomääräystä (cease and desist order), jolla estetään kyseiset toimet, tai nostamalla kanteen liittovaltion piirioikeudessa (federal district court). Jos kanne hyväksytään, sillä on vastaava vaikutus kuin kieltomääräyksellä. FTC voi hakea siviilioikeuteen kuuluvaa rangaistusta hallinnollisen kieltomääräyksen rikkomisesta, ja se voi nostaa siviili- tai rikosjutun liittovaltin tuomioistuimen päätöksen noudattamatta jättämisestä. FTC ilmoittaa kauppaministeriölle kaikista toimistaan. Kauppaministeriö rohkaisee muita valtiollisia elimiä ilmoittamaan sille lopullisesta tuloksesta kaikissa oikeusjutuissa tai muissa päätöksissä, jotka koskevat safe harbor - periaatteiden noudattamista.

Jatkuva periaatteiden noudattamatta jättäminen:

Jos organisaatio jatkuvasti rikkoo periaatteita, se menettää oikeutensa safe harbor -järjestelmän etuihin. Kyseessä on jatkuva periaatteiden rikkominen, jos organisaatio, joka on itse ilmoittanut kauppaministeriölle (tai sen nimeämälle edustajalle) osallistuvansa safe harbor -järjestelmään, kieltäytyy noudattamasta itsesääntelyelimen tai viranomaisen lopullista päätöstä, tai jos tällainen elin tai viranomainen on todennut organisaation toistuvasti rikkoneen järjestelmän periaatteita siinä määrin, että sen oma ilmoitus periaatteiden noudattamisesta ei enää ole uskottava. Organisaation on viipymättä ilmoitettava tällaisista tapauksista kauppaministeriölle (tai sen nimeämälle edustajalle). Ilmoitusvelvoitteen laiminlyöminen on kannekelpoinen False Statements Act -lain nojalla.

Ministeriö (tai sen nimeämä edustaja) pitää yllä julkista luetteloa organisaatioista, jotka ovat ilmoittaneet noudattavansa safe harbor

([1]) Riitojen ratkaisusta vastaavat elimet voivat harkita, missä tapauksissa pakotteita käytetään. Kyseisten tietojen arkaluonteisuus on yksi niistä tekijöistä, jotka on otettava huomioon päätettäessä, vaaditaanko tietojen poistamista. Huomioon on otettava myös se, onko organisaatio kerätessään, käyttäessään tai paljastaessaan tietoja rikkonut periaatteita räikeästi.

▼B

-periaatteita. Tässä luettelossa ministeriö ilmoittaa kaikista ilmoituksista, jotka koskevat jatkuvaa periaatteiden noudattamatta jättämistä, riippumatta siitä, onko ilmoitus saatu organisaatioilta itseltään, itsesääntelyelimeltä vaiko viranomaiselta. Ilmoitus julkaistaan luettelossa kuitenkin vasta, kun kyseiselle organisaatiolle on annettu kolmenkymmenen (30) päivän määräaika, jonka kuluessa periaatteita rikkoneella organisaatiolla on mahdollisuus esittää vastineensa. Kauppaministeriön (tai sen nimeämän edustajan) ylläpitämästä luettelosta käyvät siis selvästi ilmi ne organisaatiot, jotka ovat oikeutettuja safe harbor -järjestelmän etuihin, ja ne organisaatiot, jotka eivät enää ole oikeutettuja kyseisiin etuihin.

Jos organisaatio vetoaa itsesääntelyelimeen voidakseen uudestaan saada oikeuden safe harbor -järjestelmän etuihin, sen on toimitettava kyseiselle elimelle täydelliset tiedot aiemmasta osallistumisestaan safe harbor -järjestelmään.

FAQ 12 — Valintaperiaate — Kieltäytymisen ajoitus

Kysymys: *Antaako valintaperiaate rekisteröidylle mahdollisuuden valita vain rekisteröintisuhteen alussa vai milloin hän niin haluaa?*

Vastaus: Yleisesti valintaperiaatteen tarkoituksena on varmistaa, että henkilötietoja käytetään ja julkistetaan tavalla, joka noudattaa rekisteröidyn odotuksia ja valintoja. Sen mukaan rekisteröidyn on voitava kieltää (tai valita) häntä itseään koskevien tietojen käyttäminen suoramarkkinointiin milloin tahansa organisaation asettamissa kohtuullisissa aikarajoissa, jotka antavat organisaatiolle riittävästi aikaa kiellon täytäntöönpanoon. Organisaatio saattaa myös vaatia riittäviä tietoja voidakseen varmistua käsittelyn kieltämistä vaativan rekisteröidyn henkilöllisyydestä. Yhdysvalloissa voi valita tämän vaihtoehdon käyttämällä keskitettyä kielto-ohjelmaa kuten Direct Marketing Association's Mail Preference Service. Kyseistä kielto-ohjelmaa käyttävien organisaatioiden olisi tiedotettava tällaisesta mahdollisuudesta kuluttajille, jotka eivät halua saada mainoksia. Joka tapauksessa rekisteröidylle on tarjottava heti käytettävissä oleva ja kohtuuhintainen menettely, jonka avulla hän voi käyttää tätä oikeuttaan.

Samoin organisaatio saa käyttää tietoa tiettyihin suoramarkkinointitarkoituksiin sellaisissa tapauksissa, joissa on käytännössä mahdotonta antaa rekisteröidylle etukäteen mahdollisuus kieltää tietojen käyttö, jos organisaatio tarjoaa hänelle samanaikaisesti (ja pyynnöstä milloin tahansa) mahdollisuuden kieltäytyä (ilman rekisteröidylle koituvia kuluja) vastaanottamasta muita suoramarkkinointiin liittyviä yhteydenottoja ja jos organisaatio myöntyy rekisteröidyn vaatimukseen.

FAQ 13 — Matkustustiedot

Kysymys: *Milloin lentomatkustajien varaus- ja muita matkustustietoja, kuten kanta-asiakas- ja hotellivaraustietoja, sekä erityistarpeita, esim. uskonnon mukaisia aterioita tai fyysistä apua, koskevia tietoja voi siirtää EU:n ulkopuolella sijaitseville organisaatioille?*

Vastaus: Kyseistä tietoa voidaan siirtää useissa eri tapauksissa. Direktiivin 26 artiklan mukaan henkilötietoja voidaan siirtää "sellaiseen kolmanteen maahan, jossa ei taata 25 artiklan 2 kohdassa tarkoitettua tietosuojan riittävää tasoa", 1) jos se on tarpeen kuluttajan vaatimien palvelujen tarjoamiseksi tai sopimuksen, kuten kanta-asiakassopimuksen, ehtojen täyttämiseksi, tai 2) jos kuluttaja on selkeästi antanut siihen suostumuksensa. Safe harbor -järjestelmässä mukana olevat yhdysvaltalaiset organisaatiot antavat riittävän henkilötietojen suojan, ja ne saavat siten ottaa vastaan EU:sta siirrettyjä tietoja täyttämättä edellä mainittuja ehtoja tai muita ehtoja, joista säädetään direktiivin 26 artiklassa. Koska safe harbor -järjestelmässä on arkaluonteista tietoa koskevia erityissääntöjä, tällaisia tietoja (joita on kerättävä esim. asiakkaan tarvitessa fyysistä apua) saa sisältyä safe harbor -järjestelmään kuuluville organisaatioille siirrettäviin tietoihin. Tietoja siirtävän organisaation on joka tapauksessa kuitenkin noudatettava sen EU:n jäsenvaltion lakia, jossa se toimii, ja kyseisen valtion lainsäädännössä saattaa olla mm. arkaluonteisten tietojen käsittelyä koskevia erityissääntöjä.

▼B

FAQ 14 — Lääkevalmisteet ja lääketieteelliset tuotteet

Kysymys 1: *Kun henkilötietoja kerätään EU:ssa ja niitä siirretään Yhdysvaltoihin lääkeaineiden tutkimusta ja/tai muuta tarkoitusta varten, sovelletaanko siihen jäsenvaltioiden lakeja vai safe harbor -periaatteita?*

Vastaus 1: Jäsenvaltioiden lainsäädäntöä sovelletaan henkilötietojen keruuseen ja kaikkeen tietojen käsittelyyn, joka suoritetaan ennen tietojen siirtämistä Yhdysvaltoihin. Safe harbor -periaatteita sovelletaan heti, kun tiedot on siirretty Yhdysvaltoihin. Lääkeaineiden tutkimukseen ja muihin tarkoituksiin käytettävistä tiedoista tulisi mahdollisuuksien mukaan poistaa viittaukset henkilöihin.

Kysymys 2: *Lääketieteellisissä ja lääkeaineita koskevissa tutkimuksissa saadut henkilötiedot ovat usein hyödyksi tulevissa tutkimuksissa. Kun tieteellisessä tutkimuksessa kerättyjä henkilötietoja siirretään yhdysvaltalaiselle organisaatiolle safe harbor -järjestelmässä, voiko kyseinen organisaatio käyttää saatuja tietoja uudessa tutkimuksessa?*

Vastaus 2: Kyllä, jos tästä on alun perin asianmukaisesti ilmoitettu ja annettu valintamahdollisuus. Ilmoituksessa on kerrottava kaikista tiedon tulevista käyttötarkoituksista, esimerkiksi jaksottaisesta seurannasta, kyseistä tutkimusta sivuavista tutkimuksista ja markkinoinnista. Ymmärrettävästi tiedon kaikkia tulevia käyttötarkoituksia ei pystytä täsmentämään, koska uusi tutkimus voi saada alkunsa uudesta näkökulmasta alkuperäiseen tietoon, lääketieteellisistä löydöistä ja edistysaskeleista tai kehityksestä kansanterveyden tai sääntelyn alalla. Tarvittaessa ilmoituksen olisi siksi sisällettävä maininta siitä, että henkilötietoja saatetaan käyttää lääketieteellisissä ja lääkeaineita koskevissa tutkimuksissa, joista ei tällä hetkellä vielä tiedetä. Jos tällainen käyttötarkoitus ei ole yhteensopiva sen tutkimuksen yleistarkoituksen kanssa, jonka vuoksi tiedot on alun perin kerätty tai johon kyseinen henkilö on antanut suostumuksensa, häneltä on saatava uusi suostumus.

Kysymys 3: *Mitä yksityishenkilön tiedoille tapahtuu, jos kliiniseen kokeeseen osallistuja päättää omasta tahdostaan tai tutkimuksen teettäjän pyynnöstä vetäytyä kokeesta?*

Vastaus 3: Koehenkilö voi milloin tahansa vetäytyä kliinisestä kokeesta, tai häntä voidaan pyytää tekemään näin. Kaikkia tätä ennen kerättyjä tietoja saadaan silti käsitellä muiden kliinisessä kokeessa kerättyjen tietojen ohella, jos tästä on selkeästi ilmoitettu kyseiselle henkilölle, kun hän on suostunut osallistumaan kokeeseen.

Kysymys 4: *Lääkkeitä ja lääkintälaitteita valmistavat yritykset saavat toimittaa EU:ssa tehdyissä kliinisissä kokeissa saatuja henkilötietoja yhdysvaltalaisille valvontaviranomaisille sääntely- ja valvontatarkoituksiin. Sallitaanko tällainen tiedonsiirto muille osapuolille kuin valvontaviranomaisille, esimerkiksi yrityksen muihin toimipaikkoihin ja muille tutkijoille?*

Vastaus 4: Kyllä, ilmoitusta ja valintaa koskevien periaatteiden mukaisesti.

Kysymys 5: *Objektiivisuuden takaamiseksi monissa kliinisissä tutkimuksissa kokeeseen osallistujat ja usein tutkijatkaan eivät saa tietää, mitä hoitoa kullekin henkilölle annetaan. Tällaisen tiedon antaminen vaarantaisi tutkimuksen ja tulosten validiteetin. Saavatko kyseisiin kliinisiin kokeisiin (sokkotutkimuksiin) osallistuvat omaan hoitoonsa liittyviä tietoja tutkimuksen jatkuessa?*

Vastaus 5: Eivät. Tällaisia tietoja ei tarvitse antaa rekisteröidylle, jos rajoituksesta on ilmoitettu siinä vaiheessa, kun kyseinen henkilö on päättänyt osallistua tutkimukseen ja jos tietojen antaminen vaarantaisi tutkimuksen luotettavuuden. Osallistuminen tutkimukseen näillä edellytyksillä on riittävä osoitus siitä, että kyseinen henkilö luopuu oikeudestaan tiedonsaantiin. Kun tutkimus on saatettu päätökseen ja tulokset on analysoitu, siihen osallistuneilla on oltava oikeus halutessaan saada itseään koskevat tiedot. Tietoja voi pyytää ensisijaisesti lääkäriltä tai muulta terveydenhoitohenkilökuntaan kuuluvalta, joka on hoitanut kyseistä henkilöä tutkimuksen aikana, taikka tutkimuksen teettäneeltä yritykseltä.

Kysymys 6: *Onko lääkkeitä ja lääkintälaitteita valmistavan yrityksen sovellettava ilmoitusta, valintaa, edelleen siirtoa ja tiedonsaantia koskevia safe harbor -periaatteita toteuttaessaan tuoteturvallisuuteen ja tehokkuuden valvontaan liittyviä toimia, mukaan luettuina vaaratilanneilmoitukset ja tiettyjä lääkkeitä tai lääkinnällisiä*

▼B

laitteita (esim. sydämentahdistinta) käyttävien potilaiden/henkilöiden jäljittäminen?

Vastaus 6: Ei, siltä osin kuin safe harbor -järjestelmän periaatteiden noudattaminen vaikeuttaa lakisääteisten vaatimusten noudattamista. Tämä koskee raportteja, joita esimerkiksi terveydenhoitopalvelujen tarjoajat antavat lääkkeitä ja lääkintälaitteita valmistaville yrityksille, samoin kuin raportteja, joita lääkkeitä ja lääkintälaitteita valmistavat yritykset antavat viranomaisille, kuten FDA:lle (Food and Drug Administration).

Kysymys 7: *Tutkimuksen johtaja salaa poikkeuksetta henkilötiedot tutkimuksen alussa antamalla niille ainutkertaiset koodit, jottei rekisteröityjen henkilöllisyys paljastuisi. Tutkimuksia teettävät lääkealan yritykset eivät saa tietää koodien avaimia. Avaimet ovat tiedossa vain tutkijalla, jotta hän voi erityistapauksessa (esimerkiksi tarvittaessa lääketieteellistä jatkohoitoa) tunnistaa, kenestä on kyse. Katsotaanko tällä tavoin koodatun tiedon siirto EU:sta Yhdysvaltoihin henkilötietojen siirroksi, johon sovelletaan safe harbor -periaatteita?*

Vastaus 7: Ei. Tässä ei ole kyse henkilötietojen siirrosta, johon sovellettaisiin kyseisiä periaatteita.

FAQ 15 — Julkisista rekistereistä saatu tieto ja yleisesti saatavilla oleva tieto

Kysymys: *Onko tarpeen soveltaa ilmoitusta, valintaa ja edelleen siirtoa koskevia periaatteita julkisista rekistereistä saatuun tietoon tai yleisesti saatavilla olevaan tietoon?*

Vastaus: Ilmoitusta, valintaa ja edelleen siirtoa koskevia periaatteita ei ole tarpeen soveltaa julkisista rekistereistä saatuun tietoon, jos sitä ei ole yhdistetty ei-julkiseen rekisteritietoon ja jos toimivaltaisen viranomaisen vahvistamia rekisterin käytön edellytyksiä noudatetaan.

Ilmoitusta, valintaa ja edelleen siirtoa koskevia periaatteita ei myöskään ole yleensä tarpeen soveltaa yleisesti saatavilla olevaan tietoon, ellei eurooppalainen siirtäjä ilmoita, että kyseistä tietoa koskevat rajoitukset, joiden vuoksi organisaation on sovellettava kyseisiä periaatteita aikomaansa käyttötarkoitukseen. Organisaatio ei ole vastuussa siitä, miten julkaistusta materiaalista saatua tietoa käytetään.

Jos todetaan, että organisaatio on tarkoituksellisesti julkaissut henkilötietoja safe harbor -periaatteiden vastaisesti, jotta se tai muut voisivat hyötyä mainituista poikkeuksista, organisaatio menettää safe harbor -järjestelmän mukaiset edut.

▼B

LIITE III

Yleiskatsaus safe harbor -järjestelmän täytäntöönpanoon

Sopimattomia ja harhaanjohtavia käytäntöjä (Unfair and Deceptive Practices) koskeva liittovaltion ja osavaltioiden toimivalta ja yksityisyyden suoja

Tässä muistiossa kuvaillaan Federal Trade Commissionin (FTC) Federal Trade Commission Act -lain (15 U.S.C. §§ 41—58, sellaisena kuin se on muutettuna) 5 pykälän mukaista toimivaltaa ryhtyä toimenpiteisiin sellaisia tahoja vastaan, jotka eivät ole suojanneet henkilötietoja ilmoituksistaan ja/tai sitoumuksistaan huolimatta. Muistiossa käsitellään myös kyseiseen toimivaltaan liittyviä poikkeuksia ja muiden liittovaltion ja osavaltioiden viranomaisten mahdollisuutta ryhtyä toimenpiteisiin tapauksissa, joissa FTC:llä ei ole toimivaltaa ([1]).

FTC:n toimivalta sopimattomien tai harhaanjohtavien käytäntöjen suhteen

Federal Trade Commission Act -lain 5 pykälän mukaan kauppaa koskevat tai kauppaan vaikuttavat sopimattomat tai harhaanjohtavat toimet tai käytännöt ovat laittomia (unfair or deceptive acts or practices in or affecting commerce), 15 U.S.C. § 45(a)(1). Samassa pykälässä annetaan FTC:lle täydet valtuudet kyseisten käytäntöjen estämiseksi, 15 U.S.C. § 45(a)(2). Siten FTC voi muodollisen käsittelyn jälkeen antaa kieltomääräyksen (cease and desist order) oikeudenvastaisen toiminnan lopettamiseksi, 15 U.S.C. § 45(b). Jos se on yleisen edun mukaista, FTC voi myös hakea tilapäistä rajoitusmääräystä (restraining order) tai tilapäistä tai pysyvää kieltotuomiota (injunction) yhdysvaltalaisessa piirioikeudessa, 15 U.S.C. § 53(b). Jos kyseessä ovat moninaiset sopimattomat tai harhaanjohtavat toimet tai käytännöt tai jos FTC on jo antanut asiassa kieltomääräyksen, FTC voi saattaa voimaan hallinnollisen määräyksen, jossa määrätään kyseisistä toimista tai käytännöistä, 15 U.S.C. § 57a.

Ne, jotka eivät noudata FTC:n määräystä, voivat saada siviilioikeudellista sakkoa enintään 11 000 Yhdysvaltain dollaria, siten että jokainen rikkomuspäivä muodostaa erillisen rikkomuksen ([2]), 15 U.S.C. § 45(1). Samoin FTC:n sääntöä tietoisesti rikkovat voivat saada 11 000 Yhdysvaltain dollarin sakon kustakin rikkomuksesta, 15 U.S.C. § 45(m). Täytäntöönpanotoimet toteuttaa joko oikeusministeriö tai sen kieltäytyessä FTC, 15 U.S.C. § 56.

FTC:n toimivalta ja yksityisyyden suoja

Käyttäessään 5 pykälän mukaista toimivaltaa FTC katsoo, että väärien tietojen antaminen siitä, miksi tietoja kerätään kuluttajilta tai miten tietoja käytetään,

([1]) Tässä ei käydä läpi kaikkia liittovaltion lakeja, joissa käsitellään yksityisyyden suojaa eri yhteyksissä, tai mahdollisesti sovellettavia osavaltioiden lakeja ja common law -oikeutta. Henkilötietojen kaupallista keruuta ja käyttöä säänteleviä liittovaltion lakeja ovat mm. Cable Communications Policy Act (18 U.S.C. § 551), Driver's Privacy Protection Act (18 U.S.C. § 2721), Electronic Communications Privacy Act (18 U.S.C. § 2701 et seq.), Electronic Funds Transfer Act (15 U.S.C. §§ 1693, 1693m), Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.), Right to Financial Privacy Act (12 U.S.C. § 3401 et seq.), Telephone Consumer Protection Act (47 U.S.C. § 227) ja Video Privacy Protection Act (18 U.S.C. § 2710). Monilla osavaltioilla on vastaavaa lainsäädäntöä näillä aloilla. Ks. esim. Mass. Gen. Laws ch. 167B, § 16 (kieltää rahoituslaitoksia luovuttamasta asiakkaiden tilitietoja kolmansille ilman asiakkaan suostumusta tai oikeudenkäyntimenettelyä), N.Y. Pub. Health Law § 17 (rajoittaa fyysiseen tai henkiseen terveydentilaan liittyvien tietojen käyttöä ja luovuttamista ja antaa potilaille oikeuden tutustua tietoihin).

([2]) Sellaisessa tapauksessa yhdysvaltalainen piirioikeus voi myös antaa FTC:n määräystä tukevan kieltotuomion (injunctive and equitable relief), 15 U.S.C. § 45(1).

▼B

muodostaa harhaanjohtavan käytännön ([1]). Esimerkiksi vuonna 1998 FTC nosti kanteen GeoCities-sivustoa vastaan, koska se oli antanut Internet-sivustollaan keräämiään tietoja kolmansille osapuolille kaupallisia tarkoituksia varten ja ilman lupaa päinvastaisista ilmoituksista huolimatta ([2]). FTC:n henkilöstö on myös vakuuttanut, että henkilötietojen kerääminen lapsilta ja kyseisten tietojen myynti ja paljastaminen ilman vanhempien suostumusta on todennäköisesti sopimaton käytäntö ([3]).

Kirjeessään Euroopan komission pääjohtajalle John Moggille FTC:n johtaja Pitofsky huomautti FTC:n toimivallan rajoista yksityisyyden suojaamisessa tapauksissa, joissa ei ole annettu väärää tietoa (tai ollenkaan tietoa) siitä, miten kerättyjä tietoja käytetään. FTC:n johtaja Pitofskyn kirje John Moggille (23. syyskuuta 1998). Kuitenkin yritysten, jotka haluavat käyttää hyväkseen ehdotettua safe harbor -järjestelmää, on vakuutettava, että ne suojelevat keräämiään tietoja määrättyjen toimintalinjojen mukaisesti. Jos yritys on vakuuttanut turvaavansa tietosuojan mutta ei teekään sitä, sellainen toiminta olisi siten väärän tiedon antamista ja harhaanjohtava käytäntö (deceptive practice) 5 pykälän tarkoittamassa merkityksessä.

Koska FTC:n toimivalta koskee sellaisia sopimattomia tai harhaanjohtavia toimia tai käytäntöjä, jotka koskevat kauppaa tai vaikuttavat siihen (in or affecting commerce), FTC:llä ei ole toimivaltaa muihin kuin kaupallisiin tarkoituksiin kerättyjen tai käytettyjen henkilötietojen osalta, esimerkiksi hyväntekeväisyyteen tarkoitetun rahankeruun suhteen, ks. Pitofskyn kirje, s. 3. Henkilötietojen käyttö missä tahansa kaupallisissa liiketoimissa kuitenkin täyttää tämän toimivaltamääritelmän. Siten esimerkiksi jos työnantaja myy työntekijöidensä henkilötietoja suoramarkkinoijalle, liiketoimi kuuluu 5 pykälän soveltamisalaan.

Lain 5 pykälän poikkeukset

Lain 5 pykälässä säädetään poikkeuksista FTC:n sopimattomia tai harhaanjohtavia toimia tai menettelyjä koskevaan toimivaltaan seuraavien asioiden suhteen:

— rahoituslaitokset, mukaan lukien pankit, asuntolainarahastot ja luotto-osuuskunnat,

— televiestintäoperaattorit ja osavaltioiden välillä toimivat kuljetusliikkeet,

— lentoyhtiöt,

— lihanpakkausliikkeet ja karjanvälittäjät.

Ks. 15 U.S.C. § 45(a)(2). Kutakin poikkeusta ja FTC:n sijasta toimivaa sääntelyviranomaista käsitellään jäljempänä.

Rahoituslaitokset ([4])

Ensimmäinen poikkeus koskee pykälässä 18(f)(3) [15 U.S.C. § 57a(f)(3)] määriteltyjä pankkeja ja asuntolainarahastoja (banks, savings and loan institutions described in section 18(f)(3) [15 U.S.C. § 57a(f)(3)]) ja pykälässä 18(f)(4) [15

([1]) Harhaanjohtava käytäntö (deceptive practice) määritellään ilmoitukseksi, tekemättä jättämiseksi tai menettelyksi, joka todennäköisesti johtaa järkeviä kuluttajia harhaan oleellisella tavalla.

([2]) Ks. www.ftc.gov/opa/1998/9808/geocitie.htm.

([3]) Ks. henkilöstökirje Center for Media Educationille, www.ftc.gov/os/1997/9707/cenmed.htm. Lisäksi vuoden 1998 Children's Online Privacy Protection Act -laissa annetaan FTC:lle erityinen oikeudellinen toimivalta säännellä henkilötietojen keräämistä lapsilta Internet-sivustoissa ja verkko-operaattoreiden toimesta, ks. 15 U.S.C. §§ 6501—6506. Laissa säädetään erityisesti verkko-operaattorien velvoitteesta ilmoittaa vanhemmille ja saada todistettavissa oleva vanhempien suostumus ennen henkilötietojen keräämistä lapsilta tai lapsia koskevien tietojen käyttämistä tai luovuttamista, id., § 6502(b). Laissa myös annetaan vanhemmille oikeus saada tietoonsa ja kieltää tiedon käyttö, id.

([4]) Presidentti Clinton allekirjoitti 12. marraskuuta 1999 Gramm-Leach-Bliley Act -lain (Pub. L. 106—102, kodifioitu 15 U.S.C. § 6801 et seq.). Laissa rajoitetaan rahoituslaitosten oikeutta luovuttaa asiakkaidensa henkilötietoja. Laissa vaaditaan rahoituslaitoksia mm. antamaan kaikille asiakkaille tiedoksi niiden noudattamat yksityisyyden suojaa koskevat ohjelmat ja käytännöt henkilötietojen luovuttamisessa tytärpankeille ja muille. Laissa annetaan FTC:lle, liittovaltion pankkiviranomaisille ja muille viranomaisille valtuudet antaa säädöksiä laissa edellytetyn yksityisyyden suojan täytäntöönpanemiseksi. Virastot ovat tehneet säädösehdotuksia tätä varten.

▼B

U.S.C. § 57a(f)(4)] määriteltyjä liittovaltion luotto-osuuskuntia (Federal credit unions described in section 18(f)(4) [15 U.S.C. § 57a(f)(4)]) ([1]). Nämä rahoituslaitokset kuuluvat Federal Reserve Boardin, Office of Thrift Supervisionin ([2]) ja National Credit Union Administration Boardin alaisen sääntelyn piiriin, ks. 15 U.S.C. § 57a(f). Näiden sääntelyviranomaisten tehtävänä on antaa tarvittavat säädökset, joilla estetään kyseisten rahoituslaitosten sopimattomat tai harhaanjohtavat käytännöt ([3]), ja perustaa erillinen osasto käsittelemään kuluttajien valituksia, ks. 15 U.S.C. § 57a(f)(1). Täytäntöönpanoa koskeva toimivalta johtuu pankkien ja asuntolainarahastojen osalta Federal Deposit Insurance Act -lain (12 U.S.C. § 1818) 8 pykälästä ja liittovaltion luotto-osuuskuntien osalta Federal Credit Union Act -lain 120 ja 206 pykälästä, 15 U.S.C. §§ 57a(f)(2)—(4).

Vaikka vakuutusala ei nimenomaisesti kuulukaan 5 pykälän poikkeusten luetteloon, McCarran-Ferguson Act -laissa (15 U.S.C. § 1011 et seq.) yleisesti ottaen jätetään vakuutustoiminnan sääntely osavaltioille ([4]). Lisäksi McCarran-Ferguson Act -lain 2 b pykälän mukaan mikään liittovaltion laki ei mitätöi, heikennä tai korvaa osavaltion lakeja ellei sellainen laki nimenomaisesti koske vakuutustoimintaa (unless such Act specifically relates to the business of insurance), 15 U.S.C. § 1012(b). FTC Act -lain säännöksiä kuitenkin sovelletaan vakuutusalaan siltä osin kun kyseiseen alaan ei sovelleta osavaltion lakeja (to the extent that such business is not regulated by State law), id. On myös huomattava, että McCarran-Ferguson viittaa osavaltioihin ainoastaan vakuutustoiminnan (the business of insurance) osalta. Siten FTC säilyttää toimivallan vakuutusyhtiöiden sopimattomissa tai harhaanjohtavissa käytännöissä, jos ne eivät liity vakuutustoimintaan. Tämä voi tarkoittaa esimerkiksi tapauksia, joissa vakuutuksen antajat myyvät vakuutuksen ottajien henkilötietoja muiden kuin vakuutustuotteiden suoramarkkinoijille ([5]).

Kuljetusliikkeet

Lain 5 pykälän toinen poikkeus koskee sellaisia kuljetusliikkeitä, jotka kuuluvat kauppaa sääntelevien säädösten soveltamisalaan (subject to the Acts to regulate commerce), 15 U.S.C. § 45(a)(2). Tässä tapauksessa kauppaa sääntelevillä säädöksillä (Acts to regulate commerce) viitataan United States Code -lain osaston 49 osaan IV ja vuoden 1934 Communications Act -lakiin (47 U.S.C. § 151 et seq.) (the Communications Act), ks. 15 U.S.C. § 44.

49 U.S.C.:n osa IV (osavaltioiden välinen kuljetus) kattaa rautateillä, maanteillä ja vesiteillä toimivat kuljetusliikkeet, kaupanvälittäjät, huolintaliikkeet ja putkijohtokuljettajat, 49 U.S.C. § 10101 et seq. Nämä kuljetusliikkeet kuuluvat Surface Transportation Boardin, liikenneministeriön alaisen itsenäisen viraston, sääntelyn piiriin, 49 U.S.C. §§ 10501, 13501 ja 15301. Kussakin tapauksessa kuljetusliikkeen on kiellettyä luovuttaa tietoja rahdin luonteesta, määränpäästä ja muista sellaisista seikoista, joita voidaan käyttää tavaran lähettäjän vahingoksi, ks. 49 U.S.C. §§ 11904, 14908 ja 16103. On huomattava, että nämä säännökset viittaavat tietoihin, jotka koskevat tavaran lähettäjän lastia, eivätkä siten ilmeisesti koske tavaran lähettäjän henkilötietoja, jotka eivät liity kyseessä olevaan kuljetukseen.

([1]) Sanamuodon mukaan tätä poikkeusta ei sovelleta arvopaperialaan. Meklarit, välittäjät ja muut arvopaperialan toimijat ovat sen vuoksi Securities and Exchange Commissionin ja FTC:n rinnakkaisen toimivallan alaisia sopimattomien tai harhaanjohtavien toimien tai käytäntöjen osalta.

([2]) Lain 5 pykälän poikkeuksessa viitattiin alun perin Federal Home Loan Bank Boardiin, joka lakkautettiin elokuussa 1989 vuoden 1989 Financial Institutions Reform, Recovery and Enforcement Act -lailla. Sen tehtävät siirrettiin Office of Thrift Supervisionille ja Resolution Trust Corporationille, Federal Deposit Insurance Corporationille ja Housing Finance Boardille.

([3]) Samassa yhteydessä kun 5 pykälässä siirretään rahoituslaitokset pois FTC:n toimivallan piiristä, siinä säädetään, että aina FTC:n antaessa säädöksen sopimattomista tai harhaanjohtavista toimista tai käytännöistä, rahoitustoiminnan sääntelyviranomaisten olisi annettava vastaavat säädökset 60 päivän kuluessa, ks. 15 U.S.C. § 57a(f)(1).

([4]) Vakuutustoimintaan ja kaikkiin sitä harjoittaviin sovelletaan usean osavaltion lakeja, jotka koskevat kyseisen toiminnan sääntelyä tai verotusta (The business of insurance, and every person engaged therein, shall be subject of the laws of the several States which relate to the regulation or taxation of such business), 15 U.S.C. § 1012(a).

([5]) FTC on käyttänyt toimivaltaansa vakuutusyhtiöihin useissa eri yhteyksissä. Eräässä tapauksessa FTC nosti yritystä vastaan kanteen harhaanjohtavasta mainonnasta osavaltiossa, jossa sillä ei ollut toimilupaa. FTC:n toimivalta vahvistettiin sillä perusteella, että tapauksessa ei ollut tosiasiallista osavaltion säädöstä, koska yritys oli tosiasiallisesti osavaltion oikeuden ulottumattomissa. Ks. FTC v. Travelers Health Association, 362 U.S. 293 (1960).
Osavaltioista 17 on omaksunut Insurance Information and Privacy Protection Act -mallilain, jonka National Association of Insurance Commissioners (NAIC) on laatinut. Laissa on säännökset ilmoittamisesta, käytöstä ja luovuttamisesta sekä tiedonsaantioikeudesta. Melkein kaikki osavaltiot ovat myös ottaneet käyttöön NAIC:n Unfair Insurance Practices Act -mallin, jossa käsitellään erityisesti vakuutusalan sopimattomia käytäntöjä.

▼B

Communications Act -laissa säädetään Federal Communications Commissionin (FCC) harjoittamasta sääntelystä, joka koskee osavaltioiden välistä ja ulkomaan kauppaa kaapeli- ja radiolähetystoiminnassa (interstate and foreign commerce in communication by wire and radio), ks. 47 U.S.C. §§ 151 ja 152. Televiestintäyhtiöiden lisäksi Communications Act -lakia sovelletaan myös sellaisiin yhtiöihin, kuten televisio- ja radioyhtiöihin ja kaapelipalvelujen tarjoajiin, jotka eivät ole televiestiliikenteen harjoittajia. Viimeksi mainitut eivät siten kuulu FTC Act -lain 5 pykälän poikkeuksen soveltamisalaan. FTC:llä on siten toimivalta tutkia kyseisten yhtiöiden mahdollisia sopimattomia tai harhaanjohtavia käytäntöjä, kun taas FCC:llä on rinnakkainen toimivalta käyttää itsenäisiä valtuuksiaan tällä alalla jäljempänä esitellyllä tavalla.

Communications Act -lain mukaan kaikilla televiestintätoiminnan harjoittajilla (every telecommunications carrier), mukaan lukien paikalliskeskusten operaattorit, on velvollisuus suojella asiakastietoja [1], 47 U.S.C. § 222(a). Tämän yleisen yksityisyyden suojaa koskevan toimivallan lisäksi Communications Act -lakia muutettiin vuoden 1984 Cable Communications Policy Act -lailla (the Cable Act), 47 U.S.C. § 521 et seq., siten, että kaapelioperaattoreille annettiin erityinen velvollisuus suojella kaapelipalvelujen tilaajien tunnistettavissa olevia henkilötietoja (personally identifiable information), 47 U.S.C. § 551 [2]. Cable Act -lailla rajoitetaan henkilötietoja, joita kaapelioperaattorit voivat kerätä, ja asetetaan kaapelioperaattoreille velvollisuus ilmoittaa tilaajalle kerättyjen tietojen laatu ja tietojen käyttötapa. Cable Act -laissa annetaan tilaajille oikeus saada tietoonsa heitä koskevat tiedot ja määrätään kaapelioperaattorit tuhoamaan tarpeettomiksi käyneet tiedot.

Communications Act -laissa FCC:lle annetaan valtuudet panna täytäntöön nämä kaksi yksityisyyden suojaa koskevaa säännöstä, joko omasta aloitteestaan tai vastauksena ulkopuolelta tulleeseen valitukseen [3], 47 U.S.C. §§ 205, 403; id. § 208. Jos FCC katsoo, että televiestintätoiminnan harjoittaja (myös kaapelioperaattori) on rikkonut 222 tai 551 pykälänmukaisia yksityisyyden suojaa koskevia säännöksiä, se voi ryhtyä kolmenlaisiin toimenpiteisiin. Kuulemisen ja rikkomuksen toteamisen jälkeen FCC voi ensinnäkin määrätä viestintätoiminnan harjoittajan maksamaan vahingonkorvausta (monetary damages) [4], 47 U.S.C. § 209. Vaihtoehtoisesti FCC voi antaa viestintätoiminnan harjoittajalle kieltomääräyksen (cease and desist) ja määrätä sen lopettamaan oikeudenvastaisen käytännön, 47 U.S.C. § 205(a). Kolmanneksi FCC voi määrätä viestintätoiminnan harjoittajan mukautumaan ja noudattamaan FCC:n mahdollisesti määräämiä sääntöjä tai käytäntöjä (conform to and observe [any] regulation or practice), id.

Yksityishenkilöt, jotka katsovat, että televiestintätoiminnan harjoittaja tai kaapelioperaattori on rikkonut Communications Act -lain tai Cable Act -lain asiaankuuluvia säännöksiä, voivat joko tehdä valituksen FCC:lle tai nostaa kanteen liittovaltion piirioikeudessa, 47 U.S.C. § 207. Kantajalle, joka voittaa asiakastietojen suojaamatta jättämisestä Communications Act -lain laajan 222 pykälän nojalla liittovaltion piirioikeudessa televiestintätoiminnan harjoittajaa vastaan nostetun kanteen, voidaan myöntää todellisia vahinkoja vastaavia vahingonkorvauksia ja korvata asianajokulut, 47 U.S.C. § 206. Kantajalle, joka nostaa kanteen yksityisyyden loukkaamisesta Cable Act -lain kaapelitoimintaa koskevan 551 pykälän nojalla, voidaan todellisia vahinkoja vastaavien vahingonkorvausten ja asianajokulujen lisäksi myöntää rangaistuksen luonteisia korvauksia ja kohtuulliset oikeudenkäyntikulut, 47 U.S.C. § 551(f).

FCC on antanut 222 pykälän soveltamisesta yksityiskohtaiset säännöt, ks. 47 CFR 64.2001—2009. Säännöt sisältävät erityiset suojatoimet asiakkaiden verkkotieto-

---

(1) Ilmaisulla asiakkaiden verkkotiedot (customer proprietary network information) tarkoitetaan tietoja, jotka liittyvät asiakkaan televiestintäpalvelujen lukumäärään, tekniseen konfiguraatioon, tyyppiin, vastaanottajiin ja käyttömäärään (the quantity, technical configuration, type, destination, and amount of use of a telecommunications service) sekä puhelujen laskutustietoihin, 47 U.S.C. § 222(f)(1). Ilmaisulla ei kuitenkaan tarkoiteta puhelinluettelotietoja, id.

(2) Lainsäädännössä ei ole nimenomaisesti määritelty tunnistettavissa olevia henkilötietoja (personally identifiable information).

(3) Tähän toimivaltaan kuuluu oikeus korjata yksityisyyden loukkaukset sekä Communications Act -lain 222 pykälän että kaapelipalvelujen tilaajien osalta lakia muuttavan Cable Act -lain 551 pykälän nojalla. Ks. myös 47 U.S.C. § 551(f)(3) (siviilikanne liittovaltion piirioikeudessa ei ole poissulkeva oikeuskeino, vaan sitä voidaan käyttää jonkin muun kaapelipalvelun tilaajan käytettävissä olevan laillisen oikeuskeinon lisänä (in addition to any other lawful remedy available to a cable subscriber).).

(4) Kantajalle koituneiden välittömien vahinkojen puuttuminen ei kuitenkaan ole peruste valituksen hylkäämiselle, 47 U.S.C. § 208(a).

▼B

jen luvattoman käytön estämiseksi. Säännöissä edellytetään, että televiestintätoiminnan harjoittajat:

— kehittävät ja käyttävät ohjelmistoja, jotka ilmoittavat (flag) asiakkaan ilmoituksen tai hyväksymisen tilan, kun asiakkaan tiedot tulevat näyttöruudulle ensimmäisen kerran,

— ylläpitävät sähköistä seurantajärjestelmää (audit trail), jolla seurataan asiakkaan tietojen käyttöä, myös milloin asiakasta koskevia tiedostoja on avattu, kenen toimesta ja mitä tarkoitusta varten,

— antavat henkilökunnalle koulutusta asiakkaan verkkotietojen luvallisesta käytöstä ja perustavat asianmukaiset kurinpitomenettelyt,

— laativat valvontamenettelyn, jolla varmistetaan sääntöjen noudattaminen ulospäin suuntautuvan markkinoinnin yhteydessä, ja

— ilmoittavat FCC:lle vuosittain, miten ne noudattavat näitä sääntöjä.

Lentoyhtiöt

Yhdysvaltalaiset ja ulkomaiset lentoyhtiöt, jotka kuuluvat vuoden 1958 Federal Aviation Act -lain soveltamisalaan, ovat myös poikkeus FTC Act -lain 5 pykälään, ks. 15 U.S.C. § 45(a)(2). Tähän kuuluvat kaikki tavaroiden, matkustajien tai postin kuljetusta osavaltioiden välisessä tai ulkomaan lentoliikenteessä tarjoavat, ks. 49 U.S.C. § 40102. Lentoyhtiöt kuuluvat liikenneministeriön toimivallan alaisuuteen. Tässä yhteydessä liikenneministeriöllä on toimivalta ryhtyä toimiin sopimattomien, harhaanjohtavien, riistävien tai kilpailun vastaisten käytäntöjen estämiseksi lentoliikenteessä (preventing unfair, deceptive, predatory, or anticompetitive practices in air transportation), 49 U.S.C. § 40101(a)(9). Liikenneministeriö voi tutkia, onko yhdysvaltalainen tai ulkomainen lentoyhtiö tai lipunmyyjä noudattanut sopimattomia tai harhaanjohtavia käytäntöjä, jos se on yleisen edun mukaista, 49 U.S.C. § 41712. Kuulemisen jälkeen liikenneministeriö voi antaa määräyksen laittoman käytännön lopettamiseksi, id. Tiedossa ei ole, että liikenneministeriö olisi käyttänyt tätä toimivaltuuttaan lentoyhtiöiden asiakkaiden henkilötietojen suojaan liittyvissä kysymyksissä ([1]).

Lentoyhtiöihin sovelletaan tietyissä olosuhteissa kahta säännöstä, jotka koskevat henkilötietojen suojaa. Ensinnäkin Federal Aviation Act -lailla suojellaan lentäjäksi hakevien yksityisyyttä, ks. 49 U.S.C. § 44936(f). Lentoyhtiöillä on mahdollisuus saada hakijan aikaisempia työsuhteita koskevia tietoja, mutta lain mukaan hakijoille on ilmoitettava tietojen pyytämisestä, hakijalla on oikeus antaa suostumuksensa ja korjata virheet ja vaatia, että tiedot luovutetaan vain työhön ottamisesta päättäville. Toiseksi, DOT-säädökset edellyttävät, että lento-onnettomuuksien varalta valtion käyttöön kerätyt matkustajatiedot on pidettävä luottamuksellisina ja annettava ainoastaan sisäministeriön, National Transportation Boardin (NTSB:n pyynnöstä) ja liikenneministeriön käyttöön (be kept confidential and released only to the U.S. Department of State, the National Transportation Board (upon the NTSB's request), and the U.S. Department of Transportation), 14 CFR osa 243, § 243.9(c) (lisättynä 63 FR 8258:lla).

Lihanpakkausliikkeet ja karjanvälittäjät

Vuoden 1921 Packers and Stockyards Act -lain (7 U.S.C. § 181 et seq.) mukaan on laitonta, jos lihanpakkausliike karjan, lihan, lihatuotteiden tai valmistamattomien eläintuotteiden osalta tai siipikarjanvälittäjä elävän siipikarjan osalta ryhtyy sopimattomiin, epäoikeudenmukaisiin tai harhaanjohtaviin käytäntöihin tai keinoihin tai toimii tällä tavoin (any packer with respect to livestock, meats, meat food products, or livestock products in unmanufactured form, or for any live poultry dealer with respect to live poultry, to engage in or use any unfair, unjustly discriminatory, or deceptive practice or device), 7 U.S.C. § 192(a); ks. myös 7 U.S.C. § 213(a) (sopimattomien, epäoikeudenmukaisten tai harhaanjohtavien käytäntöjen tai keinojen (any unfair, unjustly discriminatory, or deceptive practice or device) kieltämisestä karjan yhteydessä). Maatalousministeriöllä on ensisijainen vastuu näiden säännösten täytäntöönpanosta, kun taas FTC:llä on toimivalta vähittäiskaupan alalla ja siipikarjan yhteydessä, 7 U.S.C. § 227(b)(2).

Ei ole selvää, tulkitseeko maatalousministeriö, että lihanpakkausliikkeen tai siipikarjanvälittäjän ilmoitetun toimintalinjan mukaisen yksityisyyden suojan puuttuminen on Packers and Stockyards Act -lain mukaista harhaanjohtavaa

([1]) Alan piirissä on ilmeisesti pyrkimyksiä käsitellä yksityisyyden suojaan liittyviä kysymyksiä. Alan edustajat ovat keskustelleet ehdotetuista safe harbor -periaatteista ja niiden mahdollisesta soveltamisesta lentoyhtiöihin. Keskusteluissa on myös käsitelty ehdotusta alan omasta yksityisyyden suojaa koskevasta toimintalinjasta, jossa osallistuvat yritykset nimenomaisesti alistaisivat itsensä DOT:n toimivallan alaisuuteen.

▼B

(deceptive) käytäntöä. Lain 5 pykälän poikkeuksia kuitenkin sovelletaan henkilöihin tai yhtiöihin vain siinä määrin kuin ne kuuluvat Packers and Stockyards Act -lain soveltamisalaan (insofar as they are subject to the Packers and Stockyards Act). Siten, jos yksityisyyden suoja ei sisälly Packers and Stockyards Act -lain säännöksiin, 5 pykälän poikkeusta ei ehkä sovelleta ja lihanpakkausliikkeet ja karjanvälittäjät kuuluvat FTC:n toimivaltaan kyseisessä asiassa.

Osavaltioiden toimivalta sopimattomien tai harhaanjohtavien käytäntöjen (Unfair and Deceptive Practices) suhteen

FTC:n laatiman tutkimuksen mukaan kaikki 50 osavaltiota sekä District of Columbia, Guam, Puerto Rico ja Yhdysvaltain Neitsytsaaret ovat säätäneet Federal Trade Commission Act -lakia vastaavia lakeja sopimattomien tai harhaanjohtavien kauppakäytäntöjen estämiseksi (All fifty states plus the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted laws more or less like the Federal Trade Commission Act ("FTCA") to prevent unfair or deceptive trade practices), FTC:n tietosivu, painos Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation, 59 Tul. L. Rev. 427 (1984). Kaikissa tapauksissa täytäntöönpanoviranomaisella on toimivaltuus suorittaa tutkimuksia käyttämällä haasteita tai siviilitutkintapyyntöjä sekä hankkimalla vakuutuksia vapaaehtoisesta sääntöjen noudattamisesta, antaa kieltomääräyksiä tai saada tuomioistuimelta kieltotuomio sopimattomien, kohtuuttomien tai harhaanjohtavien kaupankäyntikäytäntöjen estämiseksi (to conduct investigacions through the use of subpoenas or civil investigative demands, obtain assurances of voluntary compliance, to issue cease and desist orders or obtain court injunctions preventing the use of unfair, unconscionable or deceptive trade practices), id. Lisäksi 46 lainkäyttöalueella laissa sallitaan yksityiset vahingonkorvauskanteet todellisten, kaksinkertaisten, kolminkertaisten tai rangaistuksen luonteisten korvausten saamiseksi ja joissakin tapauksissa oikeudenkäyntikulut ja asianajokulut korvataan, id.

Esimerkiksi Floridan Deceptive and Unfair Trade Practices Act -laissa osavaltion attorney generalille annetaan toimivaltuudet tutkia ja nostaa siviilikanne sopimattomia kilpailumenetelmiä sekä sopimattomia, kohtuuttomia tai harhaanjohtavia kaupankäyntikäytäntöjä vastaan (unfair methods of competition, unfair, unconscionable or deceptive trade practices), mukaan lukien väärä tai harhaanjohtava mainonta, harhaanjohtava edustussopimus tai liiketoimintatilaisuus, vilpillinen telemarkkinointi ja pyramidijärjestelmät, ks. myös N.Y. General Business Law § 349 sopimattomien toimien ja harhaanjohtavien käytäntöjen kieltämisestä liiketoiminnassa (prohibiting unfair acts and deceptive practices carried out in the course of business).

National Association of Attorneys General -järjestön (NAAG) tänä vuonna suorittama tutkimus vahvistaa nämä tulokset. Kaikilla tutkimukseen vastanneilla 43 osavaltiolla on omat pienois-FTC:n (mini-FTC) säädökset tai muut säännöt, jotka antavat samankaltaisen suojan. Lisäksi NAAG:n tutkimuksen mukaan 39 osavaltiota ilmoitti, että niillä on toimivalta käsitellä muiden kuin osavaltion omien asukkaiden tekemiä valituksia. Kuluttajien yksityisyyteen liittyen 37 osavaltiota 41 vastanneesta ilmoitti, että ne reagoisivat valituksiin, joissa väitetään, että niiden lainkäyttöalueella sijaitseva yhtiö ei noudata ilmoittamiaan yksityisyyden suojaa koskevia toimintalinjoja.

▼B

LIITE IV

Yksityisyyden suoja ja vahingonkorvaukset, lakisääteiset luvat sekä yritysfuusiot ja yritysostot Yhdysvaltojen oikeusjärjestelmässä

Tämä selvitys on laadittu vastauksena Euroopan komission esittämään selvityspyyntöön, joka koskee seuraaviin osa-alueisiin sovellettavaa Yhdysvaltojen lainsäädäntöä: a) yksityisyyden loukkauksien perusteella vaadittavat vahingonkorvaukset, b)Yhdysvaltojen lakien mukaiset ”nimenomaiset luvat”, jotka koskevat henkilötietojen käyttöä safe harbor -periaatteista poikkeavalla tavalla ja c) yritysfuusioiden ja yritysostojen vaikutukset velvollisuuksiin, joiden noudattamiseen on sitouduttu safe harbor -periaatteiden mukaisesti.

A **Yksityisyyden loukkauksiin perustuvat vahingonkorvaukset**

Safe harbor -periaatteiden noudattamatta jättämisestä voi seurata useita yksityisoikeudellisia korvausvaatimuksia kuhunkin tapaukseen liittyvien olosuhteiden mukaan. Safe harbor -järjestelmään kuuluvien organisaatioiden voidaan katsoa syyllistyneen etenkin harhaanjohtamiseen, jos ne eivät noudata ilmoittamaansa käytäntöä yksityisyyden suojaamisessa. Yksityisyyden loukkaukseen perustuvia yksityisoikeudellisia vahingonkorvauskanteita voidaan nostaa myös common law -oikeuden mukaisten kanneperusteiden nojalla. Monissa yksityisyyttä koskevissa liittovaltion ja osavaltioiden laeissa säädetään lisäksi yksityishenkilöiden oikeudesta vahingonkorvauksiin rikkomustapauksissa.

Oikeus saada vahingonkorvausta yksityisyyden loukkauksen johdosta on vakiintunut Yhdysvaltojen common law -oikeuteen.

Jos henkilötietoja käytetään safe harbor -periaatteiden vastaisella tavalla, seurauksena voi olla oikeudellisen vastuun syntyminen useamman kuin yhden oikeusteorian perusteella. Esimerkiksi sekä tietoja siirtävä rekisterinpitäjä että kohteena olevat yksityishenkilöt voivat nostaa harhaanjohtamista (misrepresentation) koskevan kanteen sellaista safe harbor -järjestelmään kuuluvaa organisaatiota vastaan, joka ei noudata safe harbor -järjestelmän mukaisia sitoumuksiaan. Oikeuskirjallisuuden mukaan (Restatement of the Law, Second, Torts [1]):

> Se, joka tahallisesti esittää seikan, mielipiteen, aikomuksen tai lain säännöksen harhaanjohtavalla tavalla tarkoituksenaan saada esittämänsä perusteella toinen osapuoli toimimaan tai olemaan toimimatta tietyllä tavalla, on erehdyttämisen nojalla vastuussa toiselle osapuolelle aiheutuneesta rahallisesta vahingosta, joka johtuu siitä, että kyseinen osapuoli perustellusti luotti harhaanjohtavaan tietoon.

Restatement § 525. Harhaanjohtaminen on ”tahallista” (fraudulent), jos tekijä tietää tai uskoo antaneensa väärää tietoa, id., § 526. Harhaanjohtavaa tietoa tahallisesti antanut on yleissäännön mukaan mahdollisesti vastuussa kaikille niille, joiden hän haluaa tai odottaa luottavan näihin tietoihin kaikista niistä rahallisista menetyksistä, joita näille saataa koitua harhaanjohtamisen seurauksena, id. § 531. Toista osapuolta tahallisesti harhaanjohtanut osapuoli voi joutua vastuuseen myös kolmatta osapuolta kohtaan, jos hän haluaa tai odottaa, että harhaanjohtava tieto välitetään kolmannelle osapuolelle ja että tämä toimii kyseisen tiedon perusteella, id. § 533.

Kun tarkastellaan safe harbor -järjestelmää, annettu tieto on organisaation julkinen ilmoitus siitä, että se noudattaa safe harbor -periaatteita. Koska organisaatio on tehnyt tämän sitoumuksen, tietoinen periaatteiden noudattamatta jättäminen voi muodostaa kanneperusteen, jonka nojalla harhaanjohtavaan tietoon luottaneet voivat nostaa harhaanjohtamista koskevan kanteen. Koska sitoumus periaatteiden noudattamisesta annetaan yleisölle, niillä yksityishenkilöillä, joita koskevista tiedoista on kysymys, ja Eurooppaan sijoittautuneilla rekisterinpitäjillä, jotka siirtävät henkilötietoja yhdysvaltalaiselle organisaatiolle, voi kaikilla olla peruste harhaanjohtamista koskevan kanteen nostamiseen yhdysvaltalaista organisaatiota vastaan [2]. Lisäksi yhdysvaltalainen organisaatio on vastuussa ”jatketusta harhaanjohtamisesta” (continuing misrepresentation) niin pitkään kuin edellä mainitut tahot luottavat harhaanjohtavaan tietoon omaksi haitakseen. Restatement, § 535.

(1) Second Restatement of the Law — Torts; American Law Institute (1997).

(2) Tapausesimerkki tästä olisi tilanne, jossa rekisteröidyt luottavat yhdysvaltalaisen organisaation tekemiin safe harbor -sitoumuksiin antaessaan rekisterinpitäjälle luvan siirtää henkilötietojaan Yhdysvaltoihin.

▼B

Tahallisesti annettuun harhaanjohtavaan tietoon luottaneilla on oikeus vahingonkorvaukseen. Oikeuskirjallisuuden (Restatement) mukaan:

> Tahallisesti annettun harhaanjohtavan tiedon vastaanottajalla on oikeus saada tiedon antajaa vastaan erehdyttämisen nojalla nostetulla kanteella korvaus rahallisista vahingoista, joiden lainmukaisena syynä on harhaanjohtaminen.

Restatement, § 549. Mahdolliset vahingonkorvaukset kattavat sekä varsinaiset rahalliset tappiot että ”benefit of the bargain” -säännön perusteella määritettävän kauppaan liittyvän edun menetyksen kaupallisen toiminnan yhteydessä, id.; ks. esim. Boling v. Tennessee State Bank, 890 S.W.2d 32 (1994) (pankki velvoitettiin maksamaan 14 825 Yhdysvaltain dollarin arvosta vahingonkorvauksia, koska se oli antanut lainansaajien henkilötietoja ja tietoja näiden liiketoimintasuunnitelmista pankinjohtajalle, jolla oli eturistiriita).

Tahallinen harhaanjohtaminen edellyttää joko varsinaista tietoa siitä tai vähintään uskoa siihen, että tieto on harhaanjohtava, mutta vastuu voi syntyä myös tuottamuksellisen (negligent) harhaanjohtamisen perusteella. Oikeuskirjallisuuden (Restatement) mukaan jokainen, joka antaa vääriä tietoja liiketoimintansa, ammanttitoimintansa, työnsä tai minkä tahansa liiketoimen yhteydessä, voidaan asettaa vastuuseen, ”jos hän ei tietoja hankkiessaan tai antaessaan noudata kohtuullista huolellisuutta tai täytä kohtuullisia ammattipätevyysvaatimuksia”. Restatement, § 552(1). Toisin kuin tahallisen harhaanjohtamisen yhteydessä tuottamuksellisen harhaanjohtamisen perusteella voidaan myöntää vahingonkorvauksia vain rahallisista menetyksistä, id., § 552B(1).

Connecticutin osavaltion ylioikeus (Superior Court of Connecticut) katsoi jokin aika sitten ratkaisemassaan asiassa, että harhaanjohtamista koskevan kanteen nostamiselle oli peruste, koska sähköyhtiö oli ilmoittamatta antanut asiakkaittensa maksutietoja valtakunnallisille luottotietokeskuksille (national credit reporting agencies), ks. Brouillard v. United Illuminating Co., 1999 Conn. Super. LEXIS 1754. Tässä tapauksessa kantaja ei saanut luottoa, koska vastaaja oli ilmoittanut myöhästyneiksi suoritukset, joita ei ollut saatu kolmenkymmenen päivän kuluessa laskutuspäivämäärästä. Kantaja väitti, ettei vastaaja ollut ilmoittanut hänelle tästä käytännöstä kotitaloussähkön laskutussopimuksen teon yhteydessä. Oikeus katsoi erityisesti, että ”tuottamuksellista harhaanjohtamista koskevan kanteen perustana voi olla se seikka, että vastaaja laiminlyö tiedonantovelvollisuutensa”. Tämä tapaus osoittaa myös sen, ettei tuottamuksellisesta harhaanjohtamisesta nostetun kanteen perusteena välttämättä tarvita ”tietoisuutta” tai tahallista aikomusta. Näin yhdysvaltalainen organisaatio, joka tuottamuksellisesti laiminlyö velvollisuutensa ilmoittaa kaikki tiedot siitä, miten se käyttää safe harbor -järjestelmän mukaisesti saamiaan tietoja, voidaan asettaa vastuuseen harhaanjohtamisesta.

Jos safe harbor -periaatteiden rikkomiseen liittyy henkilötietojen väärinkäyttö, rekisteröity voi nostaa kanteen myös yksityisyyden loukkauksen perusteella, joka on common law -oikeuden mukainen vahingonteko. Yhdysvaltojen oikeusjärjestyksessä on jo pitkään tunnustettu yksityisyyden loukkauksiin pohjautuvat kanneperusteet. Vuonna 1905 Georgian osavaltion korkein oikeus (Supreme Court) katsoi ratkaistessaan asian yksityisen kansalaisen hyväksi tapauksessa ([1]), jossa henkivakuutusyhtiö oli käyttänyt mainoksessaan kantajan valokuvaa tämän tietämättä ja ilman tämän antamaa suostumusta, että oikeus yksityisyyteen on yksi keskeisistä luonnonoikeuden ja common law -oikeuden säännöistä. Tuomioistuin viittasi yksityisyyttä koskevassa Yhdysvaltojen oikeusopissa nykyisin hyvin tunnettuihin teemoihin katsoessaan, että valokuvaa oli käytetty ”pahaa tarkoittaen” (malicious) ja että sen käyttö oli ”harhaanjohtavaa” (false) ja teki kantajan julkisesti naurunalaiseksi ([2]). Pavesichin asiassa tehdyn päätöksen perusteita on sen jälkeen sovellettu pienin muutoksin, ja niistä on tullut Yhdysvalloissa voimassa olevan tätä osa-aluetta koskevan oikeuden perusta. Osavaltioiden tuomioistuimet ovat johdonmukaisesti hyväksyneet yksityisyyden loukkauksiin liittyviä kanneperusteita, ja vähintään 48 osavaltiossa tunnustetaan oikeudellisesti ainakin jokin yksityisyyden loukkaukseen liittyvä peruste ([3]). Lisäksi ainakin 12 osavaltion perustuslakiin sisältyy säännöksiä, joilla taataan kansalaisten oikeus suojaan oikeudenloukkauksia vastaan ([4]) ja jotka voidaan joissakin tapauksissa ulottaa koskemaan myös muita kuin viranomaisten aiheuttamia oikeudenloukkauksia, ks. esim. Hill vs. NCAA, 865 P.2d 633 (Ca. 1994); ks. esim. S. Ginder, Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet, 34 S.D. L. Rev. 1153 (1997) (”Seuraavien osavaltioiden perustuslakeihin sisältyy

([1]) Pavesich vs. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).

([2]) Id., kohta 69.

([3]) Westlaw-tietokannasta tehty sähköinen haku antoi tulokseksi 2 703 osavaltioiden tuomioistuimissa vuodesta 1995 nostettua siviilikannetta, jotka liittyivät hakusanaan ”privacy” (yksityisyys). Tämän haun tulokset on annettu tiedoksi komissiolle jo aikaisemmin.

([4]) Ks. esim. Alaska Constitution, Art. 1, Sec. 22; Arizona, Art. 2, Sec. 8; California, Art. 1, Sec. 1; Florida, Art. 1, Sec. 23; Hawaii, Art. 1, Sec. 5; Illinois, Art. 1, Sec. 6; Louisiana, Art. 1, Sec. 5; Montana, Art. 2, Sec. 10; New York, Art. 1, Sec. 12; Pennsylvania, Art. 1, Sec. 1; South Carolina, Art. 1, Sec. 10 ja Washington, Art. 1, Sec. 7.

▼B

tiukempia yksityisyyden suojaa koskevia säännöksiä kuin Yhdysvaltain perustuslakiin: Alaska, Arizona, Kalifornia, Florida, Havaiji, Illinois, Louisiana, Montana, Etelä-Carolina ja Washington.")

The Second Restatement of Torts -teos on laajalti tunnustettu selvitys tämän osa-alueen oikeudesta. Siinä selvitetään yleisen oikeuskäytännön mukaisesti, että "oikeus yksityisyyteen" kattaa neljä erillistä perustetta siviilioikeudellisesta rikkomuksesta nostettavalle kanteelle, ks. Restatement, § 652A. Ensinnäkin kanne voidaan nostaa yksityiselämän loukkauksen(intrusion upon seclusion) perusteella sellaista vastaajaa vastaan, joka tarkoituksella fyysisesti tai muutoin loukkaa toisen henkilön oikeutta yksityiselämään, omaan rauhaan tai yksityisasioihin ([1]). Toiseksi kanne voidaan nostaa anastuksen (appropriation) perusteella silloin, kun henkilö ottaa itselleen toisen henkilön nimen tai persoonan omiin tarkoituksiinsa tai omaksi hyödykseen ([2]). Kolmanneksi kanne voidaan nostaa yksityiselämää koskevien tietojen julkistamisen (publication of private facts) perusteella silloin, kun julkistetut tiedot ovat luonteeltaan sellaisia, että ne olisivat järkevästi toimivan henkilön näkökulmasta arvioituna hyvin loukkaavia, eikä niiden julkistaminen yleisölle ole perusteltua ([3]). Neljänneksi kanne voidaan nostaa kielteisen julkisuuden (false light publicity) perusteella silloin, kun vastaaja tietoisesti tai vastuuttomasti esittää julkisuudessa toisen henkilön väärässä valossa ja kun tämä olisi järkevästi toimivan henkilön näkökulmasta arvioituna hyvin loukkaavaa ([4]).

Safe harbor -järjestelmän yhteydessä yksityiselämän loukkauksena (intrusion upon seclusion) voitaisiin pitää esimerkiksi henkilötietojen luvatonta keräämistä. Sen sijaan henkilötietojen luvattoman käytön kaupallisiin tarkoituksiin katsottaisiin muodostavan mahdollisen perusteen anastamista koskevan kanteen nostamiselle. Virheellisten henkilötietojen antamista pidettäisiin puolestaan kielteisen julkisuuden (false light publicity) aiheuttamisesta johtuvana siviilioikeudellisena rikkomuksena, jos annettuja tietoja voitaisiin pitää järkevästi toimivan henkilön näkökulmasta arvioituna erittäin loukkaavina. Arkaluontoisten henkilötietojen julkistamisesta tai paljastamisesta johtuva yksityisyyden loukkaus olisi puolestaan mahdollisesti peruste yksityiselämää koskevien tietojen julkistamista (publication of private facts) koskevan kanteen nostamiselle (ks. jäljempänä esiteltävät oikeustapausesimerkit).

Yksityisyyden loukkauksen johdosta vahinkoa kärsineen osapuolen on oikeus saada korvausta seuraavista vahingoista:

a) loukkauksen yksityisyydelle aiheuttama vahinko;

b) todistein osoitetut henkiset kärsimykset, jos ne ovat kyseisestä loukkauksesta yleensä aiheutuvien kärsimysten kaltaisia; ja

c) erityinen vahinko, jonka lainmukaisena syynä oikeudenloukkaus on.

Restatement, § 652H. Kun otetaan huomioon siviilioikeudellisia rikkomuksia koskevan oikeuden (tort law) yleissoveltuvuus ja yksityisyyden eri osatekijöihin liittyvien kanneperusteiden runsaus, on todennäköistä, että safe harbor -periaatteiden noudattamatta jättämisestä johtuvista yksityisyyden loukkauksista kärsineet saavat vahingoista rahallista korvausta.

Osavaltioiden tuomioistuimissa on käsitelty runsaasti tapauksia, jotka ovat koskeneet yksityisyyden loukkauksia samankaltaisissa tilanteissa. Esimerkiksi tapauksessa Ex Parte AmSouth Bancorporation et al., 717 So. 2d 357, oli kysymys ryhmäkanteesta, jonka mukaan vastaaja "käytti hyväkseen pankissa toimivia notariaattitallettajia antamalla luottamuksellista tietoa pankin asiakkaista ja näiden tileistä", jotta pankin tytärpankki voisi myydä rahasto-osuuksia ja muita sijoitusinstrumentteja. Tämänkaltaisissa tapauksissa määrätään usein maksettavaksi vahingonkorvauksia. Tapauksessa Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580 (D.C.App. 1985), muutoksenhakutuomioistuin kumosi alemman oikeusasteen tuomioistuimen tuomion ja katsoi, että ennen kauneusleikkausta ja sen jälkeen otettujen kantajan valokuvien käyttäminen tavaratalossa järjestetyn esityksen yhteydessä muodosti yksityisyyden loukkauksen yksityiselämää koskevien tietojen julkistamisen muodossa. Tapauksessa Candebat v. Flanagan, 487 So.2d 207 (Miss. 1986), vastaajana ollut vakuutusyhtiö oli käyttänyt mainoskampanjassa hyväkseen onnettomuutta, jossa kantajan vaimo oli loukkaantunut vakavasti. Kantaja nosti kanteen yksityisyyden loukkaamisesta. Tuomioistuin katsoi, että kantaja oli oikeutettu saamaan vahingonkorvausta henkisestä kärsimyksestä sekä identiteetin anastamisesta. Anastamista koskeva kanne voidaan nostaa, vaikka kantajana ei olisikaan tunnettu henkilö, ks. esim. Staruski v. Continental Telephone Co., 154 Vt. 568 (1990) (vastaaja sai taloudellista hyötyä käyttäessään työntekijän nimeä ja valokuvaa lehtimainoksessa). Tapauksessa Pulla v. Amoco Oil Co., 882 F.Supp. 836 (S.D Iowa 1995), työnantaja loukkasi

([1]) Id., Chapter 28, Section 652B.
([2]) Id., Chapter 28, Section 652C.
([3]) Id., Chapter 28, Section 652D.
([4]) Id., Chapter 28, Section 652E.

▼B

kantajana olevan työntekijän oikeutta yksityiselämään antamalla toiselle työntekijälle tehtäväksi kantajan luottokorttitietojen tutkimisen tarkistaakseen sairauspoissaolojen paikkansapitävyyden. Tuomioistuin piti voimassa valamiehistön määräämän 2 Yhdysvaltain dollarin varsinaisen vahingonkorvauksen sekä sanktiona määrätyn 500 000 Yhdysvaltain dollarin vahingonkorvauksen. Erään toisen työnantajan katsottiin olevan vastuussa yhtiön omassa lehdessä julkaistusta artikkelista, joka koski työntekijää, joka oli irtisanottu, koska hänen epäiltiin väärentäneen työuraansa koskevia tietoja, ks. Zinda v. Louisiana-Pacific Corp., 140 Wis.2d 277 (Wis.App. 1987). Artikkeli loukkasi kantajan yksityisyyttä, koska siinä julkistettiin kantajan yksityiselämää koskevia tietoja ja koska lehti oli yleisessä jakelussa yhteisössä. Myös oppilaitoksen, joka teki opiskelijoille HIV-testin mutta ilmoitti, että verikoe otettiin vain vihurirokkoa varten, katsottiin syyllistyneen yksityiselämän loukkaukseen, ks. Doe v. High-Tech Institute, Inc., 972 P.2d 1060 (Colo.App. 1998). (Muiden selostettujen tapausten osalta ks. Restatement, § 652H, Liite.)

Yhdysvaltoja arvostellaan usein siitä, että asiat viedään maassa hyvin helposti oikeuteen. Tämä tarkoittaa kuitenkin myös sitä, että yksityishenkilöt todella voivat hakea ja käytännössä myös hakevat ratkaisua oikeusteitse silloin, kun he katsovatoikeuksiaan loukatun. Monet piirteet Yhdysvaltojen oikeusjärjestelmässä helpottavat kanteen nostamista sekä yksityishenkilönä että ryhmänä. Asianajajakunta, joka on suhteessa suurempi kuin monissa muissa maissa, varmistaa, että oikeudellinen edustus on helposti toteutettavissa. Yksityistä kantajaa siviilikanteessa edustava asianajaja työskentelee yleensä osuuspalkkiolla, jolloin myös vähävaraiset voivat viedä asiansa oikeuteen. Tämä tuo esille tärkeän seikan — Yhdysvalloissa kumpikin osapuoli vastaa oman lakimiehensä palkkioista ja muista oikeudenkäyntikuluista. Tämä käytäntö poikkeaa Euroopassa yleisestä säännöstä, jonka mukaan hävinnyt osapuoli korvaa myös toisen osapuolen kustannukset. Puuttumatta siihen, kumpi edellä mainituista käytännöistä on parempi, voidaan todeta, että Yhdysvalloissa noudatettava sääntö mahdollistaa perusteltujen kanteiden nostamisen yleensä myös tapauksissa, joissa yksityishenkilö ei hävitessään pystyisi maksamaan molempien osapuolten kustannuksia.

Yksityishenkilöt voivat nostaa korvauskanteen, vaikka korvausvaatimus olisi melko pieni. Suurimmassa osassa Yhdysvaltojen tuomiopiirejä (joskaan ei kaikissa) on pienten korvausvaatimusten käsittelyyn erikoistuneita tuomioistuimia, joissa lakisääteisten kynnysarvojen alle jäävien riita-asioiden käsittelyssä sovelletaan tavanomaista yksinkertaisempaa ja edullisempaa tuomioistuinkäsittelyä ([1]). Mahdollisuus määrätä vahingonkorvauksia sanktiotarkoituksessa tarjoaa lisäksi muutoin vain hyvin vähän suoraa vahinkoa kärsineille yksityishenkilöille rahallisen kannustimen kanteen nostamiseksi asiassa, jossa vastapuolen toiminta on ollut moitittavaa. Lisäksi samankaltaista vahinkoa kärsineet yksityishenkilöt voivat yhdistää voimavaransa ja korvausvaatimuksensa nostamalla ryhmäkanteen.

Hyvä esimerkki yksityishenkilöiden mahdollisuuksista nostaa korvauskanne on Amazon.com-yhtiötä vastaan nostettu yksityisyyden loukkausta koskeva kanne, jonka käsittely on vielä kesken. Verkkokaupan alalla toimivaa suurta vähittäismyyjää Amazon.com-yhtiötä vastaan on nostettu ryhmäkanne, jossa kantajat väittävät, ettei heille ilmoitettu, että heidän henkilötietojaan kerättiin heidän käyttäessään Amazonin omistamaa Alexa-ohjelmaa, eivätkä he antaneet tähän suostumustaan. Kantajat ovat katsoneet yhtiön syyllistyneen tietokonepetoksista ja -väärinkäytöksistä annetun lain (Computer Fraud and Abuse Act) nojalla rikkomukseen, koska yhtiö on laittomasti hankkinut käyttöönsä kantajien tallentamia viestejä, sekä rikkoneen sähköiseen viestintään liittyvästä tietosuojasta annettua lakia (Electronic Communications Privacy Act), koska yhtiö on laittomasti siepannut kantajien sähköisesti ja langallisen verkon välityksellä välittämiä viestejä. Kantajat katsovat lisäksi, että yhtiö on common law -oikeuden nojalla syyllistynyt yksityisyyden loukkaukseen. Tämä perustuu Internetin turvallisuuteen erikoistuneen asiantuntijan joulukuussa tekemään valitukseen. Kanteella haetaan vahingonkorvauksia siten, että jokaiselle ryhmäkanteeseen osallistuvalle maksettaisiin 1 000 Yhdysvaltain dollaria, sekä asianajopalkkioiden korvaamista ja lainvastaisilla toimilla hankitun tuoton palauttamista. Koska ryhmäkanteeseen voi osallistua miljoonia henkilöitä, vahingonkorvausten kokonaismäärä voi olla miljardeja dollareita. Myös FTC (Federal Trade Commission) tutkii asiaa.

Yksityisyyttä koskevat liittovaltion ja osavaltioiden lait sisältävät useita yksityisoikeudellisia kanneperusteita rahamääräisen vahingonkorvauksen hakemiseksi.

Safe harbor -periaatteiden noudattamatta jättämisestä voi siis olla seurauksena siviilioikeudellisia vahingontekoja sääntelevän oikeuden (tort law) mukainen siviilioikeudellinen vastuu. Sillä voidaan kuitenkin myös rikkoa joitakin niistä lukuisista liittovaltion ja osavaltioiden laeista, joissa säädetään yksityisyyden suojasta. Monet näistä laeista, joissa säädetään sekä julkisella että yksityisellä

([1]) Komissiolle on jo toimitettu pienten korvauskanteiden käsittelyä koskevat tiedot.

▼B

sektorilla tapahtuvasta henkilötietojen käsittelystä, antavat yksityishenkilöille mahdollisuuden korvauskanteen nostamiseen oikeudenloukkaustapauksissa. Esimerkiksi:

Electronic Communications Privacy Act, 1986 (Laki sähköisen viestinnän tietosuojasta). ECPA-laissa keilletään matkapuhelujen ja tietokoneiden välisten tiedonsiirtojen luvaton sieppaaminen. Rikkomuksista voi olla seurauksena vähintään 100 dollarin siviilioikeudellinen korvausvastuu kultakin päivältä, jona lakia rikotaan. ECPA-lain tarjoama suoja koskee myös tallennettujen sähköisten viestien luvatonta käyttöä tai julkistamista. Rikkomuksista on seurauksena velvollisuus korvata syntyneet vahingot tai rikkomuksella hankitun tuoton menettäminen.

Telecommunications Act, 1996 (televiestintälaki). Asiakkaiden hallinnassa olevia verkkotietoja (customer proprietary network information) ei lain 702 kohdan mukaan saa käyttää mihinkään muuhun tarkoitukseen kuin televiestintäpalvelujen tarjoamiseen. Palvelujen tilaajat voivat joko tehdä valituksen Federal Communications Commissionille tai nostaa kanteen liittovaltion alioikeudessa vahingonkorvausten saamiseksi sekä asianajajan palkkioiden korvaamiseksi.

Consumer Credit Reporting Reform Act, 1996 (laki kuluttajien luottotietoselvityksistä). Tällä vuonna 1996 annetulla lailla muutettiin vuonna 1970 annettua Fair Credit Reporting Act (FCRA)-lakia. Lainmuutoksella parannettiin luottotietoselvitysten kohteina olevien henkilöiden oikeutta tietojen ja ilmoitusten saantiin. Uudessa laissa asetetaan lisäksi uusia rajoituksia kuluttajien luottotietojen jälleenmyyjille. Kuluttajat voivat rikkomistapauksissa saada vahingonkorvausta sekä korvauksen asianajajapalkkioista.

Myös osavaltioiden lait suojaavat yksityisyyttä monilla osa-alueilla. Näihin kuuluvat mm. pankkien asiakastiedot, kaapelitelevisioliittymät, luottotietoselvitykset, työuraa koskevat tiedot, hallinnolliset tiedot, geneettinen, tieto ja potilastiedot, vakuutusyhtiöiden asiakastiedot, koulujen hallussa olevat oppilastiedot, sähköinen viestintä ja videoiden vuokraus ([1]).

B **Nimenomainen lakisääteinen lupa**

Safe harbor -periaatteisiin sisältyy poikkeus silloin, kuin lainsäädännöstä, hallituksen asetuksista tai oikeuskäytännöstä johtuu ”ristiriitaisia velvoitteita tai niissä selkeästi annetaan lupa tiettyyn toimintaan sillä edellytyksellä, että tällaista lupaa käyttäessään organisaatio voi osoittaa, että periaatteiden noudattamatta jättäminen rajoittuu siihen, mikä on tarpeen tällaisen lupaan liittyvän oikeutetun ja ensisijaisen tavoitteen täyttämiseksi”. On selvää, että jos Yhdysvaltojen lainsäädäntö asettaa yhdysvaltalaiselle organisaatiolle safe harbor -periaatteiden kanssa ristiriitaisen velvoitteen, organisaation on noudatettava lakia riippumatta siitä, kuuluko se safe harbor -järjestelmään vai ei. Nimenomaisten lupien osalta voidaan todeta, että vaikka safe harbor -periaatteiden tarkoituksena on tasoittaa yksityisyyden suojassa Yhdysvaltojen ja Euroopan välillä esiintyviä eroja. Yhdysvaltojen on kunnioitettava vaaleilla valittujen lainsäätäjien valtaoikeuksia. Safe harbor -periaatteiden ehdottomasta noudattamisesta tehtävällä rajatulla poikkeuksella pyritään ottamaan huomioon molempien osapuolten perustellut edut.

Poikkeus rajoittuu tapauksiin, joissa on olemassa nimenomainen lupa. Tämän vuoksi vähimmäisvaatimuksena on, että kyseisessä laissa, asetuksessa tai tuomioistuimen päätöksessä safe harbor -organisaatioiden nimenomaisesti sallitaan toimia tietyllä tavalla ([2]). Poikkeusta ei siis sovelleta, jos laissa ei ole kyseistä mainintaa. Lisäksi poikkeusta sovellettaisiin vain silloin, kun nimenomainen lupa on ristiriidassa safe harbor -periaatteiden noudattamisen kanssa. Tässäkin tapauksessa poikkeus ”rajoittuu siihen, mikä on tarpeen tällaisen lupaan liittyvän oikeutetun ja ensisijaisen tavoitteen täyttämiseksi”. Esimerkiksi tapauksessa, jossa laki sallii yrityksen antaa henkilötietoja valtion viranomaisille, poikkeusta ei sovellettaisi. Sen sijaan tapauksessa, jossa laki antaa yritykselle erityisluvan henkilötietojen antamiseen valtion viranomaisille ilman rekisteröidyn suostumusta, on kysymyksessä ”nimenomainen lupa” toimia safe harbor -periaatteiden vastaisella tavalla. Poikkeuksen piiriin kuuluisivat myös sellaiset tapaukset, joissa erikseen myönnetään poikkeus ilmoitusvelvollisuudesta ja velvollisuudesta hankkia rekisteröidyn suostumus (koska tämä vastaa tapausta, jossa annetaan erityislupa tietojen antamiseen ilman ilmoitusta ja rekisteröidyltä hankittua suostumusta). Esimerkiksi laki, joka antaa lääkäreille luvan ilmoittaa potilaidensa potilastiedot terveysviranomaisille ilman potilailta etukäteen hankittua suostumusta, saattaisi muodostaa poikkeuksen ilmoitus- ja valintaperiaatteista. Lupa ei kuitenkaan antaisi lääkärille oikeutta ilmoittaa samoja potilastietoja terveys-

([1]) Westlaw-tietokannasta jokin aika sitten tehdyn haun tuloksena saatiin 994 osavaltioiden tuomioistuimissa käsiteltyä oikeustapausta, jotka liittyivät vahingonkorvauksiin ja yksityisyyden loukkauksiin.

([2]) Selvennyksenä mainittakoon, että kyseisessä oikeuslähteessä ei tarvitse olla nimenomaista viittausta safe harbor -periaatteisiin.

▼B

palveluja tuottaville organisaatioille tai kaupallisille lääketutkimuslaboratorioille, jotka eivät lain mukaan kuulu luvan käyttötarkoituksiin eivätkä näin myöskään poikkeuksen soveltamisalaan ([1]). Lakisääteiset valtuudet voivat olla yksittäisiä lupia, jotka oikeuttavat käsittelemään henkilötietoja tietyllä tavalla, mutta kuten jäljempänä esitetyistä esimerkeistä käy ilmi, kyseessä on yleensä poikkeus soveltamisalaltaan laajempaan lakiin, jossa säädetään henkilötietojen keruusta, käytöstä ja julkistamisesta.

Vuonna 1996 annettu Telecommunications Act -laki

Sallitut käyttötarkoitukset ovat useimmissa tapauksissa joko direktiivin vaatimusten ja safe harbor -periaatteiden tai jonkin muun sallitun poikkeuksen mukaisia. Telecommunications Act -lain (lakikokoelma 47 U.S.C. § 222) kohdassa 702 televiestintätoiminnan harjoittajille asetetaan ensimerkiksi velvollisuus pitää salassa henkilötiedot, jotka ne saavat tarjotessaan palveluja asiakkailleen. Tämän säännöksen mukaan televiestintätoiminnan harjoittajat voivat

1) käyttää asiakastietoja televiestintäpalvelujen tuottamiseen, puhelinluettelojen julkaiseminen mukaan luettuna;

2) antaa asiakkaan tietoja kolmansille asiakkaan kirjallisesta pyynnöstä; ja

3) antaa asiakastietoja koostetussa muodossa.

Ks. 47 U.S.C. § 222(c)(1)-(3). Laissa säädetään lisäksi poikkeuksesta, jonka mukaan televiestintätoiminnan harjoittajat voivat käyttää asiakastietoja:

1) palvelutarjonnan aloittamiseen, palvelujen tuottamiseen, niistä veloittamiseen ja maksujen perintään;

2) suojautuakseen vilpilliseltä tai laittomalta toiminnalta tai väärinkäytöksiltä;

3) tarjotakseen etämyyntiin, asiakasneuvontaan tai hallintoon liittyviä palveluja asiakkaan aloittaman puhelun aikana ([2]).

Id., § 222(d)(1)-(3). Televiestintätoiminnan harjoittajien on lisäksi toimitettava puhelinluettelojen kustantajille tilaajatiedot, jotka saavat sisältää ainoastaan asiakkaiden nimet, osoitteet ja puhelinnumerot sekä yritysasiakkaiden osalta tiedot näiden toimialasta, id., § 222(e).

”Nimenomaiseen lupaan” perustuva poikkeus saattaisi tulla sovellettavaksi tilanteessa, jossa televiestintätoiminnan harjoittajat käyttävät asiakkaidensa hallinnassa olevia verkkotietoja estääkseen petoksia tai muuta laitonta toimintaa. Tässäkin tilanteessa näiden tietojen käyttöä voitaisiin pitää ”yleisen edun” ja näin myös safe harbor -periaatteiden mukaisena.

Yhdysvaltojen terveys- ja sosiaalipalveluministeriön (Department of Health and Human Services) ehdottamat säännöt

Yhdysvaltojen terveys- ja sosiaalipalveluministeriö (The Department of Health and Human Services, HHS) on tehnyt ehdotuksen terveyttä koskevien tunnistettavissa olevien tietojen suojaamisessa noudatettavista säännöistä, ks. 64 Fed. Reg. 59,918 (Nov. 3, 1999) (lakikokoelman tuleva kohta 45 C.F.R., kohdat 160—164). Säännöillä pantaisiin täytäntöön vuonna 1996 annettuun Health Insurance Portability and Accountability Act -lakiin (Pub. L. 104—191) sisältyvät yksityisyyttä koskevat vaatimukset. Ehdotetuissa säännöissä kielletään niiden soveltamisalaan kuuluvia yksiköitä (kuten sairasvakuutusten tarjoajia, terveydenhuollon selvityskeskuksia sekä terveyspalvelujen tuottajia, jotka siirtävät potilastietoja sähköisesti) käyttämästä tai julkistamasta suojattuja potilastietoja ilman potilaan antamaa lupaa, ks. ehdotus 45 C.F.R. § 164.506. Ehdotetuissa säännöissä sallitaan suojattujen potilastietojen julkistaminen ainoastaan kahta tarkoitusta varten: 1) jotta henkilö voisi tutkia ja kopioida itseään koskevat tiedot, ks. id., kohta § 164.512, ja 2) jotta säännöt voitaisiin panna täytäntöön ks. id., kohta § 164.522.

([1]) Lääkäri ei tässä esimerkissä voisi myöskään vedota lakisääteiseen lupaan tavalla, joka syrjäyttäisi rekisteröidyn oikeuden kieltää tietojensa käyttöö suoramarkkinointiin FAQ 12:n mukaisesti. Kunkin ”nimenomaiseen lupaan” perustuvan poikkeuksen soveltamisala rajoittuu aina laissa annetun luvan soveltamisalaan.

([2]) Tämän poikkeuksen soveltamisala on hyvin rajallinen. Poikkeuksen mukaan televiestintätoiminnan harjoittaja voi käyttää asiakkaan hallinnassa olevia verkkotietoja ainoastaan asiakkaan soittaman puhelun aikana. Lisäksi FCC on ilmoittanut, ettei televiestintätoiminnan harjoittaja saa käyttää näitä tietoja markkinoidakseen palveluja, jotka eivät kuulu asiakkaan tiedustelun piiriin. Koska asiakkaan on lisäksi hyväksyttävä tietojensa käyttö tätä tarkoitusta varten, säännös ei ole varsinainen ”poikkeus”.

▼B

Säännöissä sallitaan suojattujen potilastietojen käyttö tai julkistaminen ilman rekisteröidyn lupaa tietyissä tarkkaan rajatuissa olosuhteissa. Näihin kuuluvat esimerkiksi terveydenhuoltojärjestelmän valvonta, lainvalvonta ja hätätilanteet, ks. id. kohta § 164.510. Ehdotetuissa säännöissä rajataan tarkkaan tämäntyyppinen käyttö ja julkistaminen. Lisäksi suojattujen potilastietojen käyttäminen tai julkistaminen rajataan tarvittaviin vähimmäistietoihin, ks. id. kohta § 164.506.

Ehdotetuissa säännöissä nimenomaisesti sallitut käyttötarkoitukset ovat yleisesti ottaen safe harbor -periaatteiden mukaisia, tai ne voidaan sallia jonkin muun poikkeuksen nojalla. Esimerkiksi lainvalvonta, oikeushallinto ja lääketieteellinen tutkimus ovat sallittuja käyttötarkoituksia. Muut käyttötarkoitukset, kuten terveydenhuoltojärjestelmän valvonta, kansanterveys ja julkiset terveysalan tietojärjestelmät, ovat yleisen edun mukaisia käyttötarkoituksia. Terveydenhuollon maksujen ja vakuutusmaksujen käsittelyä varten annettuja tietoja tarvitaan terveydenhuoltopalvelujen tuottamista varten. Kun tietoja käytetään hätätilanteissa tai lähiomaisen kuulemisessa hoitopäätöksen osalta silloin, kun politaan suostumusta ”ei voida käytännössä tai kohtuudella saada”, tai henkilöllisyyden tai kuolemansyyn selvittämisessä kuolemantapauksissa, suojataan rekisteröityjen ja muiden osapuolten ratkaisevan tärkeitä etuja. Tietojen käyttäminen puolustusvoimien henkilöstön ja muiden erityisryhmien toiminnan hallinnassa tukee puolustusvoimien operaatioiden tai muun kriisinhallinnan asianmukaista toteuttamista. Lisäksi näillä käyttötarkoituksilla on hyvin vähän, jos lainkaan, vaikutusta tavalliseen kuluttajaan.

Käsiteltäväksi jää näin vain tapaus, jossa terveydenhoitopalvelujen tuottajat käyttävät henkilötietoja potilasluetteloiden laatimiseen. Vaikka tällä käyttötarkoituksella ei välttämättä ole ”ratkaisevaa” merkitystä, luetteloista on hyötyä potilaille ja heidän läheisilleen. Tämä käyttötarkoitus on lisäksi luonteensa vuoksi aina tarkkaan rajattu. Tässä yhteydessä vetoaminensafe harbor -periaatteiden mukaiseen poikkeukseen, joka koskee lakisääteisen ”nimenomaisen luvan” kattamia käyttötarkoituksia, ei sanottavasti vaaranna potilaiden yksityisyyttä.

Fair Credit Reporting Act -laki

Euroopan komissio on ilmaissut huolensa siitä, että ”nimenomaiseen lupaan” perustava poikkeus ”tosiasiassa vastaisi tietosuojan riittävyyttä koskevaa päätöstä” Fair Credit Reporting Act (FCRA) -lain osalta. Näin ei kuitenkaan ole. Jos riittävyyttä koskevaa päätöstä ei ole FCRA:n osalta tehty, niiden yhdysvaltalaisten organisaatioiden, jotka olisivat muutoin vedonneet kyseiseen päätökseen, olisi sitouduttava noudattamaan safe harbor -periaatteita kaikilta osin. Käytännössä tämä tarkoittaa, että silloin, kun FCRA:n asettamat vaatimukset ovat safe harbor -vaatimuksia tiukemmat, yhdysvaltalaisten organisaatioiden tarvitsee noudattaa ainoastaan FCRA:n säännöksiä. Vastaavasti jos FCRA:n vaatimukset ovat periaatteissa asetettuja vaatimuksia lievemmät, organisaation on muutettava tietojärjestelmänsä periaatteiden vaatimusten mukaiseksi. Poikkeuksen soveltaminen ei muuttaisi tätä perusasetelmaa. Poikkeusta sovelletaan periaatteiden mukaan ainoastaan silloin, kun tietyssä laissa nimenomaisesti sallitaan toimintatapa, joka on ristiriidassa safe harbor -periaatteiden kanssa. Poikkeusta ei siis sovellettaisi tilanteissa, joissa FCRA:n vaatimukset eivät ole safe harbor -järjestelmän vaatimusten mukaisia ([1]).

Tarkoituksena ei siis ole katsoa poikkeuksen tarkoittavan, että se, mitä ei ole vaadittu, on ”nimenomaisesti sallittua”. Lisäksi poikkeusta sovelletaan vain silloin, kun Yhdysvaltojen laissa nimenomaisesti sallittu seikka on ristiriidassa safe harbor -periaatteiden vaatimusten kanssa. Kyseeseen tulevan lainkohdan on siis täytettävä molemmat näistä vaatimuksista, ennen kuin periaatteiden noudattamatta jättäminen voidaan sallia.

Esimerkiksi FCRA:n kohdassa 604 annetaan kuluttajien luottotietoja myyville yrityksille nimenomainen lupa antaa kuluttajien tietoja koskevia selvityksiä kohdassa luetelluissa erilaisissa tilanteissa, ks. FCRA, § 604. Jos luottotietoja myyville yrityksille annetaan kohdassa 604 lupa toimia tavalla, joka on ristiriidassa safe harbor -periaatteiden kanssa, luottotietoyritysten on vedottava poikkeukseen (ellei sovellettavaksi tule jokin muu poikkeus). Luottotietoyritysten on noudatettava oikeuden määräyksiä ja haasteita, joilla ne velvoitetaan todistamaan suuren valamiehistön eteen. Lisäksi luottotietoselvitysten käyttäminen lupia myöntävien tai sosiaali- ja elatusavun täytäntöönpanosta vastaavien viranomaisten tarpeisiin on yleisen edun mukaista, id., § 604(a)(1), (3)(D) ja (4). Luottotietoyrityksen ei siis näissä tilanteissa tarvitsisi vedota ”nimenomaiseen lupaan” perustuvaan poikkeukseen. Kun luottotietoyritys toimii kuluttajan antamien kirjallisten ohjeiden mukaisesti, tämä on täysin safe harbor -peri-

([1]) Tässä esitettyjä näkökohtia ei pitäisi tulkita osoitukseksi siitä, ettei FCRA ei tarjoa ”riittävää” tietosuojaa. FCRA:n tarjoamaa suojaa arvioitaessa on tarkasteltava koko säädöksen tarjoamaa suojaa eikä ainoastaan poikkeuksia, kuten tässä on tehty.

▼B

aatteiden mukaista, id., § 604(a)(2). Luottotietoselvityksiä voidaan hankkia työpaikkaan liittyviin tarkoituksiin vain kuluttajan kirjallisella suostumuksella (id., §§ 604(a)(3)(B) ja (b)(2)(A)(ii)) ja sellaisia luotto- tai vakuutusliiketoimia varten, joita ei toteuteta kuluttajan aloitteesta, vain jos kuluttaja ei ole kieltäytynyt tämänkaltaisista tarjouksista (id., § 604(c)(1)(B)). FCRA:ssa kielletään lisäksi luottotietoyrityksiä antamasta lääketieteellistä tietoa työpaikkaan liittyviin tarkoituksiin ilman kuluttajan suostumusta, id., § 604(g). Nämä käyttötarkoitukset ovat ilmoitus- ja valintaperiaatteiden mukaisia. Muita kohdan 604 sallimia käyttötarkoituksia ovat liiketoimet, joihin kuluttaja itse osallistuu, joten tämä käyttötarkoitus olisi myös periaatteiden mukainen, ks. id., § 604(a)(3)(A) ja (F).

Kohdassa 604 annetaan ”lupa” vielä yhteen käyttötarkoitukseen, joka liittyy luottojen johdannaismarkkinoihin, id., § 604(a)(3)(E). Kuluttajien luottotietoselvitysten käyttäminen tähän tarkoitukseen ei sinänsä ole ristiriidassa safe harbor -periaatteiden kanssa. On totta, ettei FCRA:ssa esimerkiksi vaadita luottotietoyrityksiä ilmoittamaan kuluttajille tätä tarkoitusta varten julkaistuista selvityksistä ja hankkimaan kuluttajien suostumusta. On kuitenkin jälleen huomattava, ettei vaatimuksen puuttuminen muodosta ”nimenomaista lupaa” toimia muulla kuin vaaditulla tavalla. Vastaavasti kohdassa 608 luottotietoyrityksille annetaan lupa toimittaa tiettyjä henkilötietoja valtion viranomaisille. Luottotietoyritys ei voisi tämän ”luvan” nojalla laiminlyödä safe harbor -periaatteiden noudattamisesta antamaansa sitoumusta. Tämä on erilainen tilanne kuin muissa esimerkeissä, joissa ilmoitusta ja valintaa koskeviin positiivisiin vaatimuksiin tehtävillä poikkeuksilla on sama vaikutus kuin nimenomaisella luvalla henkilötietojen käyttöön ilman ilmoitusta ja valintaa.

Päätelmät

Edellä esitetyn suppeankin tarkastelun perusteella voidaan erottaa seuraavat selkeät perustekijät:

— Lakiin sisältyvä ”nimenomainen lupa” sallii yleensä henkilötietojen käytön tai julkistamisen ilman rekisteröidyn etukäteen antamaa suostumusta; tämän perusteella poikkeukset koskisivat vain ilmoitus- ja valintaperiaatteita.

— Laissa sallitut poikkeukset ovat useimmissa tapauksissa tarkkaan rajattuja siten, että niitä sovelletaan tietyissä tilanteissa tiettyihin tarkoituksiin. Laissa kielletään aina henkilötietojen luvaton käyttö ja julkistaminen tapauksissa, jotka eivät kuulu poikkeusten soveltamisalaan.

— Nimenomaisen luvan sallima käyttö tai julkistaminen on useimmissa tapauksissa lainsäädännön luonteen mukaisesti yleisen edun mukaista.

— Nimenomaisen luvan sallimat käyttötarkoitukset ovat lähes kaikissa tapauksissa joko täysin safe harbor -periaatteiden mukaisia, tai ne kuuluvat jonkin muun poikkeuksen soveltamisalaan.

Johtopäätöksenä voidaan todeta, että lakisääteisen ”nimenomaisen luvan” perusteella myönnettävän poikkeuksen soveltamisala tulee todennäköisesti olemaan melko rajallinen.

C **Yritysfuusiot ja yritysostot**

29 artiklan mukainen työryhmä on ilmaissut huolensa tilanteista, joissa safe harbor -järjestelmän ulkopuolinen yritys fuusioi itseensä tai ostaa safe harbor -järjestelmään kuuluvan organisaation. Työryhmä näyttää olettaneen, ettei näin syntyvä yritys ole velvollinen noudattamaan safe harbor -periaatteiden hankkimansa yrityksen hallussa olevien henkilötietojen osalta, mutta tämä ei välttämättä ole tilanne Yhdysvaltojen lakien mukaan. Yhdysvalloissa sovellettavan yritysfuusioita ja yritysostoja koskevan yleissäännön mukaan yritys, joka hankkii toisesta yrityksestä osake-enemmistön , ottaa samalla vastuulleen hankkimansa yrityksen velvoitteet ja vastuut, ks. 15 Fletcher Cyclopedia of the Law of Private Corporations § 7117 (1990); ks. myös Model Bus. Corp. Act § 11.06(3) (1979) (”jäljelle jäävällä yrityksellä on kaikkien yritysfuusioon osallistuneiden yritysten kaikki velvoitteet”). Toisin sanoen sellaisen yritysfuusion tai yritysoston tuloksena syntyvä yritys, jossa kohteena on safe harbor -yritys, olisi tässä esitetyn säännön mukaan velvollinen noudattamaan kohdeyrityksen safe harbor -sitoumuksia.

Myös silloin, kun yritysfuusio tai yritysosto toteutetaan omaisuuden hankinnan kautta, kohdeyrityksen velvoitteet voivat sitoa hankinnan tehnyttä yritystä tietyissä olosuhteissa, 15 Fletcher, § 7122. Silloinkin kun velvoitteet eivät säily fuusiossa, on syytä huomata, etteivät velvoitteet säilyisi siinäkään tapauksessa, että tietojen siirto Euroopasta perustuu sopimukseen — mikä on ainoa mahdollinen vaihtoehto safe harbor -järjestelmälle, kun kyse on Yhdysvaltoihin siirrettävistä tiedoista. Safe harbor -asiakirjat edellyttävät nykyisessä tarkistetussa muodossaan, että safe harbor -organisaatio ilmoittaa Yhdysvaltain kauppaministeriölle kaikista yritysostoista ja tietojen siirtämistä jatketaan vain, jos uusi organisaatio liittyy safe harbor

▼B

-järjestelmään, ks. FAQ 6. Yhdysvallat on nyt tarkistanut safe harbor -järjestelmää siten, että yhdysvaltalaisia organisaatioita vaaditaan näiss tilanteissa poistamaan safe harbor -järjestelmän mukaisesti saadut tiedot, jos organisaation safe harbor -sitoumuksia ei pidetä voimassa tai muita tarkoitukseen soveltuvia suojakeinoja oteta käyttöön.

▼B

LIITE V

14. heinäkuuta 2000

John Mogg
Pääjohtaja, pääosasto XV
Euroopan komissio
Toimisto C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Bruxelles/Brussel

Arvoisa herra Mogg

Teille osoittamani, 29. maaliskuuta 2000 päivätty kirje on ilmeisesti synnyttänyt monia kysymyksiä. Tällä kirjeellä pyrin nyt selvittämään omaa toimintaamme aloilla, joilla kysymyksiä on syntynyt. Tämä kirje on lisäys aiempaan kirjeenvaihtoomme ja tulevien viittauksien helpottamiseksi samalla osittainen yhteenveto siitä.

Vierailujenne ja kirjeenvaihtonne yhteydessä olette tuonut esiin monia kysymyksiä, jotka koskevat Yhdysvaltojen Federal Trade Commission -elimen (FTC) toimivaltaa online-alan yksityisyyskysymyksissä. Katsoin parhaimmaksi esittää aluksi tiivistelmän aiemmista vastauksistani ja antaa tämän jälkeen lisätietoja virastomme toimivallasta kuluttajien yksityisyyttä koskevissa kysymyksissä, joihin viittasitte viimeisimmässä kirjeessänne. Kysyitte erityisesti seuraavaa: 1) Onko FTC:llä toimivaltaa työsuhdetietojen siirroissa, jos näissä on rikottu Yhdysvaltojen safe harbor -periaatteita? 2) Onko FTC:llä toimivaltaa voittoa tavoittelemattomien, yksityisyyden suojaa koskevia tunnuksia myöntävien ohjelmien osalta? 3) Sovelletaanko Federal Trade Commission Act -lakia samalla tavoin sekä online-toimintaan että muuhun toimintaan? ja 4) Miten toimitaan, jos FTC:n toimivalta on päällekkäistä muiden lainvalvontaviranomaisten toimivallan kanssa?

Federal Trade Commission Act -lain soveltaminen yksityisyyskysymyksiin

Federal Trade Commission -elimen oikeudellinen toimivalta tällä alalla perustuu Federal Trade Commission Act -lain (FTC Act) 5 pykälään, jossa kielletään kauppaa koskevat tai kauppaan vaikuttavat ”sopimattomat tai harhaanjohtavat toimet tai käytännöt” ([1]). Harhaanjohtava käytäntö määritellään sellaiseksi tietojen esittämiseksi tai poisjättämiseksi taikka käytännöksi, joka todennäköisesti johtaa valistuneita kuluttajia olennaisesti harhaan. Käytäntö on sopimaton, jos se aiheuttaa tai todennäköisesti aiheuttaa kuluttajille merkittäviä haittoja, jotka eivät ole kohtuudella vältettävissä ja joiden vastapainoksi kuluttajille tai kilpailutilanteelle ei koidu vastaavia hyötyjä ([2]).

Tietyt tiedon keruuseen liittyvät toimet rikkovat todennäköisesti FTC Act -lakia. Jos esimerkiksi virheellisesti väitetään, että Internet-sivusto vastaa jonkin yleisen yksityisyyden suojaa koskevan ohjelman tai itsesääntelyn suuntaviivojen vaatimuksia, FTC Act -lain 5 pykälä tarjoaa oikeusperustan, jolta tällaista virheellisen tiedon antamista voidaan pitää harhaanjohtavana. FTC onkin menestyksellisesti valvonut lainsäädäntöä tämän periaatteen täytäntöön panemiseksi ([3]). Lisäksi FTC on katsonut, että se voi 5 pykälän perusteella asettaa kyseenalaiseksi tietyt yksityisyyden suojaa koskevat hyvin erikoislaatuiset järjestelyt, jos ne koskevat lapsia tai jos niissä käytetään erittäin arkaluonteisia tietoja, kuten rahoitus- ([4]) tai terveystietoja. FTC on jatkanut ja aikoo vastaisuudessa jatkaa tällaisia toimia

([1]) 15 U.S.C. § 45. Fair Credit Reporting Act -lakia voidaan soveltaa myös Internetissä tapahtuvaan tiedon keruuseen sekä myyntiin, joka täyttää ”consumer report” ja ”consumer reporting agency” -käsitteiden lakisääteiset määritelmät.

([2]) 15 U.S.C. § 45(n).

([3]) Ks. GeoCities, Docket No. C-3849 (lopullinen päätös, 12. helmikuuta 1999) (saatavilla: http://www.ftc.gov/os/1999/9902/9823015d%26o.htm); Liberty Financial Cos., Docket No. C-3891 (lopullinen päätös, 12. elokuuta 1999) (saatavilla http://www.ftc.gov/opa/1999/9905/younginvestor.htm). Ks. myös Children’s Online Privacy Protection Act Rule (COPPA), 16 C.F.R. Part 312 (saatavilla: http://www.ftc.gov/opa/1999/9910/childfinal.htm). COPPA-sääntö tuli voimaan viime kuussa, ja se edellyttää, että sellaisten Internet-sivustojen operaattorit, joiden sivustot on suunnattu alle 13-vuotiaille lapsille tai jotka tietävät keräävänsä henkilötietoja alle 13-vuotiailta lapsilta, toteuttavat säännössä annetut oikeudenmukaista tiedonkäyttöä koskevat standardit.

([4]) Ks. FTC v. Touch Tone, Inc., Civil Action No. 99-WM-783 (D.Co.) (jätetty 21. huhtikuuta 1999), saatavilla: http://www.ftc.gov/opa/1999/9904/touchtone.htm. Staff Opinion Letter, 17. heinäkuuta 1997, annettu vastauksena Center for Media Educationin anomukseen, saatavilla: http://www.ftc.gov/os/1997/9707/cenmed.htm.

▼B

lainsäädännön täytäntöönpanon valvomiseksi tarkkailemalla alaa aktiivisesti toteuttamalla tutkimuksia ja tutkimalla itsesääntelyorganisaatioilta ja muilta, myös Euroopan unionin jäsenvaltioilta saatuja tutkimuspyyntöjä.

Tuki itsesääntelylle

FTC asettaa etusijalle ne itsesääntelyn suuntaviivojen rikkomista koskevat tutkimuspyynnöt, jotka saadaan esim. BBBOnlinen ja TRUSTe:n [1] kaltaisilta organisaatioilta. Tällainen toimintatapa on johdonmukainen myös, kun otetaan huomioon FTC:n pitkäaikainen suhde Better Business Bureau -elimen National Advertising Division Boardiin (NARB), joka toimittaa mainontaa koskevia valituksia FTC:lle. NARB:n National Advertising Division (NAD) ratkaisee sovittelumenettelyllä kansallista mainontaa koskevia valituksia. Jos osapuoli kieltätytyy noudattamasta NAD:n päätöstä, juttu siirretään FTC:n käsiteltäväksi. FTC:n henkilöstö asettaa kiistanalaisen mainonnan käsittelyn etusijalle ja pyrkii selvittämään, rikkooko mainonta FTC Act -lakia. Usein FTC pystyy estämään kiistanalaisen toiminnan tai onnistuu taivuttelemaan osapuolen jatkamaan NARB:n menettelyä.

Vastaavasti FTC asettaa etusijalle myös EU:n jäsenvaltioilta saatavat käsittelypyynnöt, jotka koskevat safe harbor -periaatteiden rikkomista. Kuten Yhdysvaltojen itseääntelyorganisaatioiltakin saatavien pyyntöjen yhteydessä, FTC:n henkilöstö tutkii kaikki tiedot, jotka vaikuttavat siihen, katsotaanko toiminnan rikkovan FTC Act -lain 5 pykälää. Tämä sitoumus on ilmaistu myös safe harbor -periaatteiden täytäntöönpanoa koskevassa FAQ 11:ssä.

GeoCities: FTC:n ensimmäinen online-yksityisyyttä koskeva tapaus

Ensimmäinen FTC:n tutkima yksityisyyden suojaa Internetissä koskeva tapaus, GeoCities, perustuu 5 pykälän mukaiseen FTC:n toimivaltaan [2]. Tässä tapauksessa FTC katsoi, että GeoCities antoi sekä aikuisille että lapsille virheellisen käsityksen siitä, miten heidän henkilötietojaan käytettäisiin. FTC:n valituksen mukaan GeoCities antoi käsityksen, jonka mukaan sen Internet-sivustoltaan keräämiä henkilötietoja oli määrä käyttää ainoastaan yrityksen sisäisesti taikka erityisten mainostarjousten ja -tuotteiden tai kuluttajien pyytämien palveluiden tarjoamiseksi kuluttajille ja jonka mukaan tiettyjä ”vapaaehtoisia” lisätietoja ei luovutettaisi ilman kuluttajan antamaa lupaa. Nämä tiedot kuitenkin luovutettiin kolmansille osapuolille, jotka käyttivät niitä kohdentaakseen tarjouksensa GeoCitiesin jäsenille, jotka eivät olleet sopineet tällaisesta toiminnasta. Valituksessa todettiin myös, että GeoCities oli toiminut harhaanjohtavasti kerätessään tietoja lapsilta. FTC:n valituksen mukaan GeoCities oli antanut käsityksen, jonka mukaan sen Internet-sivustolla oli toiminnassa lasten alue, jolta kerätyistä tiedoista GeoCities vastasi. Itse asiassa Internet-sivuston näistä osista vastasivat kolmannet osapuolet, jotka keräsivät ja säilyttivät tietoja.

Ratkaisussa GeoCitiesiä kielletään antamasta virheellistä kuvaa siitä tarkoituksesta, johon se kerää tai käyttää kuluttajilta, myös lapsilta saatavia tai heitä koskevia henkilötietoja. Päätöksessä edellytetään, että yritys antaa Internet-sivustollaan selkeän ja näkyvän yksityisyyttä koskevan ilmoituksen, jossa kuluttajille kerrotaan, mitä tietoja kerätään, mikä on keruun tarkoitus, kenelle tiedot toimitetaan ja miten kuluttajat saavat tiedot käyttöönsä ja voivat poistaa ne. Jotta

(1) FTC on äskettäin jättänyt valituksen TRUSTe-tunnuksen haltijaa Toysmart.comia vastaan liittovaltion piirioikeudessa, jossa se hakee kielto- ja vahvistustuomiota yhtiön Internet-sivustolle sen omaa yksityisyysohjelmaa rikkoen kerättyjen asiakkaita koskevien luottamuksellisten ja henkilökohtaisten tietojen myynnin estämiseksi. FTC sai tietoonsa tämän mahdollisen lainrikkomistapauksen suoraan TRUSTe:ltä. *FTC v. Toysmart.com, LLC,* Civil Action No. 00-11341-RGS (D.Ma.) (jätetty 11. heinäkuuta 2000) (saatavilla: *http://www.ftc.gov/opa/2000/07/toysmart.htm*).

(2) GeoCities, Docket No. C-3849 (lopullinen päätös 12. helmikuuta 1999) (saatavilla: http://www.ftc.gov/os/1999/9902/9823015d%26o.htm).

▼B

vanhemmat voisivat valvoa lapsiaan, ratkaisussa edellytetään, että GeoCities hankkii vanhempien suostumuksen, ennen kuin se kerää 12-vuotiaita tai sitä nuorempia lapsia koskevia henkilötietoja. Päätöksen mukaisesti GeoCitiesin on tarjottava jäsenilleen mahdollisuus heitä koskevien tietojen poistoon sekä GeoCitiesin että kolmansien osapuolten tietokannoista ja ilmoitettava tästä mahdollisuudesta jäsenilleen. Ratkaisussa edellytetään erityisesti, että GeoCities ilmoittaa tästä 12-vuotiaiden ja sitä nuorempien lasten vanhemmille ja poistaa heitä koskevat tiedot, elleivät vanhemmat nimenomaisesti hyväksy tietojen säilyttämistä ja käyttöä. Lisäksi edellytetään, että GeoCities ottaa yhteyden kolmansiin osapuoliin, joille se on aiemmin toimittanut henkilötietoja, ja että se myös pyyttää kyseisiä osapuolia poistamaan nämä tiedot ([1]).

ReverseAuction.com

FTC hyväksyi tammikuussa 2000 valituksen ja sovitteluratkaisun, joka koskee ReverseAuction.com-nimistä verkossa toimivaa huutokauppasivustoa. Sivuston väitettiin hankkineen kuluttajien henkilötietoja kilpailevalta Internet-sivustolta (eBay.com) ja tämän jälkeen lähettäneen kyseisille kuluttajille ei-toivottuja ja harhaanjohtavia sähköpostiviestejä, jolla yritys pyrki saamaan heidät asiakkaikseen ([2]). FTC:n valituksessa katsottiin, että ReverseAuction rikkoi FTC Act -lain 5pykälää hankkiessaan henkilötietoja, joihin sisältyi eBayn käyttäjien sähköpostiosoitteita ja henkilökohtaisia käyttäjien tunnistenimiä (käyttäjätunnuksia) sekä lähettäessään harhaanjohtavia sähköpostiviestejä.

Kuten valituksessa todetaan, ReverseAuction oli ennen tietojen hankkimista rekisteröitynyt eBayn käyttäjäksi ja sopinut noudattavansa eBayn käyttäjäsopimusta ja yksityisyyden suojaa koskevaa ohjelmaa. Kyseinen sopimus ja ohjelma suojaavat kuluttajien yksityisyyttä kieltämällä eBayn käyttäjiltä henkilötietojen keruun ja niiden käytön tarkoituksiin, joihin ei ole myönnetty lupaa. Tämä koskee esim. ei-toivottujen kaupallisten sähköpostiviestien lähettämistä. Valituksessamme todettiin ensinnäkin, että ReverseAuction oli antanut virheellisiä tietoja kertoessaan noudattavansa eBayn käyttäjäsopimusta ja yksityisyyden suojaa koskevaa ohjelmaa. Tämä on 5 pykälässä tarkoitettua harhaanjohtavaa toimintaa. Valituksessa katsottiin lisäksi, että käyttäessään tietoja käyttäjäsopimuksen ja yksityisyyden suojaa koskevan ohjelman vastaisesti ei-toivottujen sähköpostiviestien lähettämiseen ReverseAuction oli syyllistynyt 5 pykälässä tarkoitettuun sopimattomaan kaupalliseen toimintaan.

Toiseksi valituksessa katsottiin, että kuluttajille lähetetyn sähköpostiviestin otsikkorivi, jossa kuluttajille kerrottiin, että heidän käyttäjätunnuksensa eBayssä ”vanhenee pian”, oli harhaanjohtava. Lopuksi valituksessa katsottiin, että sähköpostiviesteissä annettiin virheellinen kuva, jonka mukaan eBay oli suorasti tai epäsuorasti toimittanut ReverseAuctionille käyttäjiensä henkilötietoja tai muutoin osallistunut ei-toivottujen sähköpostiviestien jakeluun.

FTC:n saavuttamassa sovitteluratkaisussa ReverseAuctionia kielletään rikkomasta kyseisiä sääntöjä vastaisuudessa. Siinä myös edellytetään, että ReverseAuction ilmoittaa ratkaisusta kuluttajille, jotka ReverseAuctionin sähköpostiviestin seurauksena rekisteröityivät tai myöhemmin rekisteröityvät ReverseAuctionin käyttäjiksi. Ilmoituksessa on kerrottava kyseisille kuluttajille, että heidän käyttäjätunnuksensa eBayssä eivät olleet vanhentumassa ja että eBay ei tiennyt ReverseAuctionin lähettävän ei-toivottuja sähköpostiviestejä eikä ollut antanut siihen lupaa. Ilmoituksessa myös annetaan kyseisille kuluttajille mahdollisuus peruuttaa rekisteröitymisensä ReverseAuctioniin ja poistaa henkilötietonsa ReverseAuctionin tietokannasta. Lisäksi päätöksessä edellytetään, että ReverseAuction poistaa niiden eBayn jäsenten henkilötiedot, jotka saivat ReverseAuctionin sähköpostiviestin mutta eivät rekisteröityneet ReverseAuctioniin, ja että Rever-

([1]) FTC on tämän jälkeen ratkaissut toisen asian, johon liittyy henkilötietojen kerääminen lapsilta verkossa. Liberty Financial Companies, Inc. vastasi Young Investor -nimisen Internet-sivuston toiminnasta. Sivusto oli tarkoitettu lapsille ja teini-ikäisille, ja se keskittyi rahaan ja sijoituksiin liittyviin kysymyksiin. FTC katsoi, että sivustossa annettiin virheellistä tietoa lapsilta erään tutkimuksen yhteydessä kerätyistä henkilötiedoista. Nämä oli määrä säilyttää nimettöminä, ja osallistujien oli määrä saada sähköpostitse tiedotuslehti sekä palkintoja. Todellisuudessa tietoja lapsen ja perheen raha-asioista säilytettiin tunnistamisen mahdollistavassa muodossa eikä tiedotuslehteä tai palkintoja lähetetty. Sovitteluratkaisussa kielletään tällainen virheellisten tietojen antaminen vastaisuudessa ja edellytetään, että Liberty Financial antaa lapsille tarkoitetulla Internet-sivustollaan yksityisyyden suojaa koskevan ilmoituksen ja hankkii todennettavissa olevan suostumuksen vanhemmilta ennen henkilötietojen keräämistä lapsilta. Liberty Financial Cos., Docket No. C-3891 (lopullinen päätös 12. elokuuta 1999) (saatavilla http://www.ftc.gov/opa/1999/9905/younginvestor.htm).

([2]) Ks. ReverseAuction.com, Inc., Civil Action No. 000032 (D.D.C.) (jätetty 6. tammikuuta 2000) (lehdistötiedote ja asianosaisten lausunnot: http://www.ftc.gov/opa/2000/01/reverse4.htm).

▼B

seAuction ei käytä eikä luovuta näitä tietoja. Kuten aiemmissa FTC:n saavuttamissa yksityisyyden suojaa koskevissa päätöksissä, myös tässä ratkaisussa edellytetään lisäksi, että ReverseAuction ilmoittaa omasta yksityisyyden suojaa koskevasta ohjelmastaan Internet-sivustollaan ja että ReverseAuction pitää kattavaa rekisteriä toiminnastaan, jotta FTC pystyisi valvomaan ratkaisun noudattamista.

ReverseAuctionin tapaus osoittaa, että FTC on sitoutunut lainvalvontaan, jolla tuetaan online-tietosuojaa koskevaa yritysten itsesääntelyä. Kyseisessä tapauksessa asetettiin kyseenalaiseksi toiminta, joka vaaransi kuluttajien yksityisyyttä suojaavan ohjelman ja käyttäjäsopimuksen ja joka olisi voinut jäytää kuluttajien luottamusta online-yritysten toteuttamiin yksityisyyden suojaa koskeviin toimiin. Koska kyseisessä tapauksessa yritys luvattomasti hankki itselleen kuluttajia koskevia tietoja, joiden suojana oli toisen yrityksen yksityisyyttä koskeva ohjelma, se voi olla erityisen merkittävä myös yksityisyydensuojaa koskevissa tapauksissa, joissa tietoja siirretään eri maissa sijaitsevien yritysten välillä.

Vaikka FTC toteutti lainvalvontatoimia GeoCities-, Liberty Financial Cos.-, ja ReverseAuction-tapauksissa, sen toimivalta on rajoitetumpi tietyissä yksityisyyden suojaan online-ympäristössä liittyvissä kysymyksissä. Kuten edellä todettiin, FTC Act -lain piiriin kuuluu luvaton henkilötietojen keruu ja käyttö, joka katsotaan joko harhaanjohtavaksi tai sopimattomaksi kaupalliseksi toiminnaksi. Tämän vuoksi on todennäköistä, että FTC Act -lain piiriin ei kuuluisi Internet-sivustossa tapahtuva henkilötietojen keruu, johon ei liity väärien tietojen antamista henkilötietojen keruun tarkoituksesta tai jossa henkilötietoja ei käytetä tai luovuteta tavalla, joka todennäköisesti aiheuttaisi merkittävää vahinkoa kuluttajille. Tällä hetkellä FTC:n toimivaltaan ei välttämättä myöskään kuulu sen varmistaminen, että tietoa Internetistä keräävät toimijat noudattavat jotakin yksityisyyden suojaa koskevaa ohjelmaa tai tiettyä tällaista ohjelmaa ([1]). Kuten edellä todettiin, olisi kuitenkin todennäköistä, että harhaanjohtavaksi toiminnaksi katsottaisiin se, että yritys ei ole noudattanut ilmoittamaansa yksityisyyden suojaa koskevaa ohjelmaa.

FTC:n toimivaltaan tällä alalla kuuluvat siis sopimattomat ja harhaanjohtavat toimet vain, jos ne ovat ”kauppaa koskevia tai kauppaan vaikuttavia”. Kauppaa koskeva vaatimus täyttyisi oletettavasti, kun tietoja keräävät kaupalliset toimijat, jotka markkinoivat tuotteita ja palveluita, tai kun tietoja kerätään ja käytetään kaupallisiin tarkoituksiin. Toisaalta monet yksityishenkilöt tai organisaatiot voivat kerätä verkosta tietoja ilman minkäänlaista kaupallista käyttötarkoitusta, jolloin ne jäävät FTC:n toimivallan ulkopuolelle. Esimerkki tästä rajoituksesta ovat ”keskusteluryhmät”, jos niiden toiminnasta vastaa ei-kaupallinen toimija, esim. hyväntekeväisyysorganisaatio.

Lisäksi on tiettyjä täydellisiä tai osittaisia lakisääteisiä rajoituksia, jotka koskevat FTC:n perustoimivaltaa kaupallisten käytäntöjen alalla ja jotka rajoittavat FTC:n mahdollisuuksia reagoida kattavasti yksityisyyden suojaa Internetissä koskeviin

([1]) Tämän vuoksi FTC totesi kongressille antamassaan todistajanlausunnossa, että todennäköisesti tarvittaisiin lisälainsäädäntöä, jolla kaikki kuluttajille suunnatut Yhdysvaltojen kaupalliset Internet-sivustot velvoitettaisiin noudattamaan tiettyjä tietoihin liittyviä hyviä toimintatapoja. ”Kuluttajien yksityisyyden suoja World Wide Webissä” (Consumer Privacy on the World Wide Web) on esitetty Yhdysvaltojen edustajainhuoneen kaupallista toimintaa käsittelevän komitean televiestinnän, kaupan ja kuluttajansuojan alakomitealle (Subcommittee on Telecommunications, Trade and Consumer Protection, House Committee on Commerce, United States House of Representatives) 21. heinäkuuta 1998 (todistajanlausunto saatavilla: http://www.ftc.gov/os/9807/privac98.htm). FTC lykkäsi tällaisen lainsäädännön ehdottamista, jotta itsesääntelyn toteuttajille tarjoutuisi mahdollisuus osoittaa, että Internet-sivustoissa on laajalti omaksuttu tietoja koskevat hyvät toimintatavat. Kesäkuussa 1998 annetussa yksityisyyden suojaa online-toiminnassa käsittelevässä FTC:n raportissa kongressille (Privacy Online: A Report to Congress) suositellaan, että lainsäädännössä edellytettäisiin, että kaupalliset Internet-sivustot hankkivat vanhempien suostumuksen ennen tunnistettavien henkilötietojen keräämistä alle 13-vuotiailta lapsilta (raportti saatavilla: http://www.ftc.gov/reports/privacy3/toc.htm), ks. myös alaviite 3 edellä. Heinäkuussa 1999 annetussa itsesääntelyä ja yksityisyyden suojaa online-ympäristössä koskevassa FTC:n raportissa (Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress) todettiin, että itsesääntelyssä oli edistytty riittävästi ja tämän vuoksi päätettiin pidättäytyä lainsäädännön ehdottamisesta toistaiseksi (raportti saatavilla: http://www.ftc.gov/os/1999/9907/index.htm#13). Lähiviikkojen aikana FTC raportoi jälleen kongressille itsesääntelyn edistymisestä.
Toukokuussa 2000 FTC antoi kongressille kolmannan raportin aiheesta ”Privacy Online: Fair Information Practices in the Electronic Marketplace” (raportti saatavilla: *http://www.ftc.gov/os/2000/05/index.htm#22*), jossa käsitellään FTC:n äskettäistä tutkimusta kaupallisista Internet-sivustoista ja siitä, miten ne noudattavat tietoja koskevia asianmukaisia käytäntöjä. Raportissa myös suositeltiin (FTC:n enemmistöllä), että kongressi antaisi lainsäädäntöä, jossa esitettäisiin yksityisyyden suojelun perustaso kuluttajille suunnattujen kaupallisten Internet-sivustojen osalta.

▼B

uhkiin. Tällaiset rajoitukset koskevat monia tietovaltaisia toimialoja, esimerkiksi pankkeja, vakuutusyhtiötä ja lentoyhtiöitä. Kuten tiedätte, muut liittovaltion toimielimet (esim. liittovaltion pankkitoimintaa koskevat virastot tai liikenneministeriö) ovat toimivaltaisia näillä aloilla.

Niissä tapauksissa, joissa FTC ei ole toimivaltainen, se ottaa vastaan ja resurssiensa salliessa myös toteuttaa toimia Consumer Response Center -keskuksiinsa (CRC) postitse ja puhelimitse sekä nyttemmin myös Internet-sivustoonsa ([1]) tulleiden valitusten pohjalta. CRC ottaa vastaan valituksia kaikilta kuluttajilta, myös Euroopan unionin jäsenvaltioissa asuvilta. FTC Act -lain mukaisesti FTC:llä on kohtuusperiaatteeseen perustuvan oikeuden mukaiset valtuudet (equitable power) hankkia kieltotuomio FTC Act -lain myöhempiä rikkomuksia vastaan sekä korvauksia vahinkoja kärsineille kuluttajille. Tarkastelumme kohteena olisi tällöin se, onko yritys toistuvasti menetellyt sopimattomasti, koska FTC ei ratkaise yksittäisiä kuluttajariitoja. FTC on tarjonnut oikeuskeinoja sekä Yhdysvaltojen että muiden maiden kansalaisille ([2]). FTC aikoo soveltuvissa tapauksissa käyttää valtaansa jatkossakin ja tarjota oikeuskeinoja myös sellaisille muiden maiden kansalaisille, jotka ovat kärsineet sopimattomasta tai harhaanjohtavasta toiminnasta FTC:n toimivaltaan kuuluvalla alalla.

Henkilöstöä koskevat tiedot

Viimeisimmässä kirjeessänne pyysitte lisäselvitystä FTC:n toimivaltaan henkilöstöä koskevien tietojen osalta. Kysyitte ensinnäkin, voiko FTC toteuttaa toimia 5 pykälän nojalla sellaista yritystä vastaan, joka väittää toimivansa Yhdysvaltojen safe harbor -periaatteiden mukaisesti mutta siirtää tai käyttää työsuhteeseen liittyviä tietoja näiden periaatteiden vastaisesti. Tutkittuamme huolellisesti FTC:n perustana olevaa lainsäädäntöä, siihen liittyviä asiakirjoja sekä kysymykseen liittyvää oikeuskäytäntöä voimme vakuuttaa, että FTC:llä on henkilöstöä koskevien tietojen osalta sama toimivalta kuin yleisestikin FTC Act -lain 5 pykälän mukaisesti ([3]). Tämä tarkoittaa sitä, että FTC toteuttaisi toimia henkilöstötietoja koskevassa tapauksessa, joka täyttää nykyiset yksityisyyden suojaan liittyvän lainvalvontatoiminnan edellytykset (sopimattomuus tai harhaanjohtavuus).

Haluamme myös hälventää väärinkäsityksiä, joiden mukaan FTC:n mahdollisuudet toteuttaa yksityisyyden suojaan liittyviä lainvalvontatoimia ovat vähäiset tapauksissa, joissa yritys on johtanut harhaan yksittäisiä kuluttajia. FTC:n äskettäinen toiminta ReverseAuction ([4]) -asiassa osoittaakin selvästi, että FTC toteuttaa yksityisyyteen liittyviä lainvalvontatoimia tapauksissa, joihin liittyy yritysten välistä tiedonsiirtoa ja joissa toisen yrityksistä väitetään toimineen lainvastaisesti toista yritystä kohtaan, mikä saattaisi aiheuttaa vahinkoja sekä kuluttajille että yrityksille. Uskomme, että nimenomaan tällaisissa tilanteissa henkilöstöä koskevat tiedot nousevat esiin, kun EU:n kansalaisten henkilöstötietoja siirretään eurooppalaisilta yrityksiltä yhdysvaltalaisille yrityksille, jotka ovat sitoutuneet noudattamaan safe harbor -periaatteita.

On kuitenkin syytä tuoda esiin yksi tapaus, jossa FTC:n toiminta estyisi. Tämä koskee tilanteita, joissa kysymystä käsitellään perinteisen työlainsäädäntöön liittyvän menettelyn yhteydessä, yleensä sovitteluvaatimuksen tai National Labor Relations Board -elimelle esitetyn sopimatonta työvoimakäytäntöä koskevan valituksen kautta. Näin käy esimerkiksi silloin,kun työnantaja on henkilötietojen käytön osalta sitoutunut yleiseen työehtosopimukseen ja työntekijä tai ammattiliitto katsoo, että työnantaja on rikkonut kyseistä sopimusta. Tällöin FTC todennäköisimmin noudattaisi kyseisen menettelyn tulosta ([5]).

([1]) Ks. http://www.ftc.gov/ftc/complaint.htm — FTC:n online-valituslomake.

([2]) Äskettäisessä tapauksessa, joka koski ”pyramidihuijausta” Internetissä, FTC hankki 15 622 kuluttajalle yhteensä 5,5 miljoonan Yhdysvaltain dollarin arvosta korvauksia. Kyseisten kuluttajien asuinmaita olivat Yhdysvallat sekä 70 muuta maata. Ks. http://www.ftc.gov/opa/9807/fortunar.htm; http://www.ftc.gov/opa/9807/ftcrefund01.htm.

([3]) Lukuun ottamatta kohtia, joissa FTC:n toimivaltaa on nimenomaan rajoitettu FTC:n perustana olevalla lainsäädännöllä, FTC Act -lain mukainen FTC:n ”kauppaa koskeviin tai kauppaan vaikuttaviin” toimiin liittyvä toimivalta vastaa perustuslain mukaista kongressin valtaa Commerce Clause -säädöksen mukaisesti, United States v. American Building Maintenance Industries, 422 U.S. 271, 277 n. 6 (1975). FTC:n toimivaltaan kuuluu tämän mukaisesti siis kansainvälisessä kaupassa toimivien yritysten henkilöstöä koskeva toiminta.

([4]) Ks. ”Online Auction Site Settles FTC Privacy Charges”, FTC:n lehdistötiedote (6.1.2000), saatavilla: *http://www.ftc.gov/opa/2000/01/reverse4.htm*.

([5]) Sen määrittely, onko kyseessä ”sopimaton työvoimakäytäntö” tai yleisen työehtosopimuksen rikkomus, on tekninen kysymys, joka yleensä jätetään valituksia käsittelevien, erikoistuneiden työtuomioistuinten päätettäväksi. Tällaisia ovat esim. sovittelijat ja NLRB.

▼B

Toimivalta tunnusohjelmissa

Toiseksi kysyitte, koskisiko FTC:n toimivalta tunnusohjelmia, jotka tarjoavat riitojenratkaisumenettelyjä Yhdysvalloissa ja joissa annetaan vääriä tietoja niiden toiminnasta safe harbor -periaatteiden täytäntöönpanon ja yksittäisten valitusten käsittelyn osalta, vaikka tällaiset ohjelmat olisivatkin teknisesti ”voittoa tavoittelemattomia”. Selvittäessään toimivaltaansa tietyn yksikön osalta, joka katsoo olevansa voittoa tavoittelematon, FTC tutkii tarkoin, edistääkö kyseinen yksikkö jäsentensä voittoa, vaikka se ei tavoittelisikaan omaa voittoa. FTC:n toimivalta tällaisiin yksiköihin on tunnustettu aivan äskettäin (24. toukokuuta 1999), kun Yhdysvaltojen korkein oikeus päätti asiassa California Dental Association v. Federal Trade Commission yksimielisesti, että FTC:n toimivalta koskee paikallisten hammashoitoalan yhdistysten vapaaehtoista ja voittoa tavoittelematonta järjestöä kilpailuoikeusasiassa. Korkein oikeus totesi seuraavaa:

FTC Act -lailla pyritään sisällyttämään toimivaltaan sekä yksiköt, jotka ”toteuttavat liiketoimintaa omaksi voitokseen” (15 U.S.C. § 44), että yksiköt, jotka toimivat ”jäsentensä” voitoksi … Tuskin voidaan olettaa, että kongressin tarkoituksena olisi ollut tällä tavoin rajoittaa toimivaltaa tukiorganisaatioiden osalta, koska tämä olisi tarjonnut mahdollisuuden toimivallan välttämiseen, vaikka FTC Act -lain tarkoituksena on selvästikin sen antaminen.

Voidaankin todeta, että määritettäessä FTC:n toimivaltaa tietyn ”voittoa tavoittelemattoman”, tunnusohjelman hallinnosta vastaavan organisaation osalta on arvioitava, missä määrin kyseinen yksikkö todellisuudessa tuottaa taloudellista etua liiketaloudellisesti toimiville jäsenilleen. Jos kyseinen yksikkö hoitaa tunusohjelmaa siten, että se tuottaa taloudellista etua jäsenilleen, FTC katsoisi todennäköisesti olevansa toimivaltainen. Erillisenä kohtana voidaan lisäksi todeta, että FTC on todennäköisesti toimivaltainen, kun kyseessä on vilpillinen tunnusohjelma, jossa annetaan vääriä tietoja ohjelman asemasta voittoa tavoittelemattomana kokonaisuutena.

Yksityisyys verkon ulkopuolella

Kolmantena kohtana toteatte, että aiempi kirjeenvaihtomme on keskittynyt yksityisyyden suojaan verkossa. Tämä onkin FTC:n tärkeä toimintakohde, koska yksityisyyden suoja verkossa on tärkeä osa sähköisen kaupan kehitystä. FTC Act -laki on kuitenkin peräisin jo vuodelta 1914, ja sitä sovelletaan luonnollisesti myös verkon ulkopuolella. Voimme siis toteuttaa toimia, jotka koskevat verkon ulkopuolella toimivia yrityksiä, joiden kauppaa koskevat sopimattomat tai harhaanjohtavat toimet vaarantavat kuluttajien yksityisyyden [1]. FTC:n viime vuonna vireille panemassa asiassa FTC v. TouchTone Information, Inc. [2] erästä ”tiedonvälittäjää” syytettiin siitä, että se oli laittomasti hankkinut ja myynyt kuluttajien yksityisiä rahoitustietoja. FTC katsoi, että TouchTone oli hankkinut kuluttajien tiedot ”verukkeilla”. Tämä käsite on lähtöisin yksityisetsivien piiristä, jotka kuvaavat sillä henkilötietojen hankkimista väärien perusteiden avulla, yleensä puhelimitse. Tässä asiassa, joka jätettiin 21. huhtikuuta 1999 liittovaltion tuomioistuimelle Coloradossa, haetaan kieltomääräystä ja kaikkien laittomasti hankittujen voittojen palauttamista.

Tämä lainvalvonnasta saatu kokemus sekä äskettäiset huolet offline- ja online-tietokantojen yhdistämisestä, online- ja offline-kauppiaiden välisten erojen hämärtyminen ja se seikka, että valtava määrä henkilötietoja kerätään ja käytetään verkon ulkopuolella, tekevät selväksi sen, että on aihetta kiinnittää runsaasti huomiota verkon ulkopuolisiin yksityisyyskysymyksiin.

Päällekkäinen toimivalta

Viimeinen kysymyksenne koskee FTC:n toimivallan ja muiden lainvalvontaviranomaisten toimivallan vuorovaikutusta, erityisesti tapauksissa, joissa useat eri elimet voivat olla toimivaltaisia. Olemme luoneet vahvat työsuhteet lukuisiin muihinlainvalvontaelimiin, myös liittovaltion pankkitoimintaa käsitteleviin virastoihin ja osavaltioiden lainopillisiin neuvonantajiin (attorneys general). Kun toimivalta on päällekkäistä, varsin usein koordinoimme tutkimuksemme omien resurssiemme säästämiseksi. Usein myös siirrämme asioita liittovaltion tai osavaltioiden soveltuvien virastojen tutkittaviksi.

([1]) Kuten aiempien keskustelujemme pohjalta tiedätte, Fair Credit Reporting Act -laki antaa FTC:lle valtuudet suojella kuluttajien rahoitukseen liittyvää yksityisyyttä kyseisen lain piiriin kuuluvissa kysymyksissä, ja FTC on äskettäin tehnyt päätöksen, joka liittyy tähän kysymykseen, ks. In the Matter of Trans Union, Docket No. 9255 (1. maaliskuuta 2000) (lehdistötiedote ja lausunto saatavilla: http://www.ftc.gov/os/2000/03/index.htm#1).

([2]) Civil Action 99-WM-783 (D.Colo.) (saatavilla: http://www.ftc.gov/opa/1999/9904/touchtone.htm) (alustava sovintoratkaisu vireillä).

▼B

Toivon, että tämä selvitys osoittautuu hyödylliseksi. Ilmoittakaa minulle, jos tarvitsette lisätietoja.

Kunnioittavasti

Robert Pitofsky

▼B

LIITE VI

John Mogg
Pääjohtaja, pääosasto XV
Euroopan komissio
Toimisto C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Bruxelles/Brussel

Arvoisa pääjohtaja

Toimitan Teille tämän kirjeen Yhdysvaltojen kauppaministeriön pyynnöstä. Kirjeen tarkoituksena on selvittää Yhdysvaltojen liikenneministeriön tehtäviä kuluttajien yksityisyyden suojaamisessa näiden lentoyhtiöille toimittamien tietojen osalta.

Liikenneministeriö tukee itsesääntelyä, jota se pitää joustavimpana ja tehokkaimpana keinona, jolla voidaan varmistaa kuluttajien lentoyhtiöille antamien tietojen tietosuoja. Se tukee näin myös safe harbor -järjestelmän käyttöönottoa. Tämän järjestelmän ansiosta lentoyhtiöt voisivat täyttää ne Euroopan unionin tietosuojadirektiivin vaatimukset, jotka koskevat tietojen siirtämistä EU:n ulkopuolelle. Liikenneministeriö myöntää kuitenkin, että toimiva itsesääntelyjärjestelmä edellyttää, että safe harbor -järjestelmän tietosuojaperiaatteita noudattamaan sitoutuneet lentoyhtiöt todella toimivat niiden mukaisesti. Itsesääntelyä olisi tämän vuoksi tuettava lainvalvontajärjestelyin. Tämän vuoksi liikenneministeriö käyttää kuluttajansuojaa koskevia lakisääteisiä valtuuksiaan varmistaakseen, että lentoyhtiöt noudattavat yleisölle antamiaan tietosuojaa koskevia sitoumuksia, ja tutkii sille toimitettuja, mahdollisia rikkomistapauksia koskevia ilmoituksia, joita se saa itsesääntelyorganisaatioilta ja muilta tahoilta, myös Euroopan unionin jäsenvaltioilta.

Liikenneministeriön täytäntöönpanovaltuudet tällä osa-alueella vahvistetaan lain 49 U.S.C kohdassa 41712, jossa lentoliikenteen harjoittajia kielletään käyttämästä lentokuljetusten myynnissä ”sopimatonta tai harhaanjohtavaa menettelyä tai sopimatonta kilpailumenettelyä”, joka aiheuttaa tai todennäköisesti aiheuttaa vahinkoa kuluttajalle. Kohta 41712 vastaa Federal Trade Commission Act -lain (15 U.S.C. 45) kohtaa 5. Lentoliikenteen harjoittajiin ei kuitenkaan lain 15 U.S.C. 45 kohdan a alakohdan 2 alakohdan mukaan sovelleta Federal Trade Commission Act -lain kohdan 5 säännöksiä.

Osastoni tehtävänä on tutkia ja nostaa kanne tapauksissa, jotka kuuluvat lain 49 U.S.C. kohdan 41712 soveltamisalaan. (Ks. esim. seuraavat Yhdysvaltain liikenneministeriön antamat määräykset (DOT Orders): 99-11-5, annettu 9. marraskuuta 1999; 99-8-23, annettu 26. elokuuta 1999; 99-6-1, annettu 1. kesäkuuta 1999; 98-6-24, annettu 22. kesäkuuta 1998; 98-6-21, annettu 19. kesäkuuta 1998; 98-5-31, annettu 22. toukokuuta 1998 ja 97-12-23, annettu 18. joulukuuta 1997.) Asian vireillepano voi olla seurausta osastomme suorittamista tutkimuksista tai yksityishenkilöiden, matkanjärjestäjien, lentoyhtiöiden sekä Yhdysvaltojen ja muiden valtioiden viranomaisten tekemistä osastollemme toimitetuista virallisista ja epävirallisista valituksista.

Olisi kuitenkin huomattava, että jos lentoliikenteen harjoittaja ei pysty varmistamaan matkustajilta saatujen tietojen tietosuojaa, tämä ei itsessään muodosta kohdan 41712 rikkomista. Sitä vastoin kun lentoliikenteen harjoittaja antaa virallisen ja julkisen sitoumuksen safe harbor -periaatteiden noudattamisesta kuluttajilta saamiensa tietojen suojaamisessa, liikenneministeriöllä on valtuudet käyttää kohdan 41712 mukaisia lakisääteisiä valtuuksiaan varmistaakseen periaatteiden noudattamisen. Kun siis matkustaja antaa tietoja safe harbor -periaatteita noudattamaan sitoutuneelle lentoliikenteen harjoittajalle, noudattamatta jättämisestä todennäköisesti aiheutuu kuluttajalle vahinkoa ja se voidaan näin myös katsoa kohdan 41712 rikkomiseksi. Rikkomisväitteiden tutkinta ja rikkomista koskevien kanteiden nostaminen silloin kun rikkomisesta on todisteita, asetettaisiin osastossani ensisijaiseen asemaan. Ilmoitamme myös Yhdysvaltojen kauppaministeriölle näiden tapausten käsittelyn tuloksista.

Kohdan 41712 rikkomisesta voi olla seurauksena kieltomääräyksen (cease and desist order) antaminen ja kieltomääräyksen rikkomisesta puolestaan siviilioikeudellinen seuraamus. Vaikka liikenneministeriöllä ei ole valtuuksia määrätä vahingonkorvauksia tai antaa rahallista korvausta yksittäisille kantajille, sillä on valtuudet hyväksyä sovitteluratkaisuja, jotka ovat seurausta ministeriön suorittamasta tutkinnasta tai sen vireille panemista asioista ja joiden ansiosta kuluttajat saavat rahallista arvoa joko lievennyksen tai muutoin maksettaviksi määrättävien sakkojen sijasta suoritettavaksi tulevan korvauksen muodossa. Olemme toimineet näin aikaisemminkin ja pystymme ja tulemme toimimaan näin myös safe harbor -periaatteiden osalta, kun olosuhteet sitä edellyttävät. Jos yhdysvaltalainen lentoyhtiö toistuvasti rikkoo kohtaa 41712, kyseisen yhtiön halukkuus noudattaa

▼B

sääntöjä voidaan kyseenalaistaa, mikä saattaa vakavassa tilanteessa johtaa sihen, ettei lentoyhtiön enää katsota olevan toimilupakelpoinen, minkä seurauksena se voi menettää toimilupansa. (Ks. liikenneministeriön antamat määräykset (DOT Orders) 93-6-34, annettu 23. kesäkuuta 1993 ja 93-6-11, annettu9. kesäkuuta 1993. Vaikka kyseinen tuomioistuinkäsittely ei liittynyt kohtaan 41712, tuloksena oli lentoliikenteen harjoittajan toimiluvan peruuttaminen sen vuoksi, että lentoliikenteen harjoittaja oli täysin laiminlyönyt liittovaltion ilmailulain (Federal Aviation Act), kahdenvälisen sopimuksen ja liikenneministeriön sääntöjen ja määräysten noudattamisen.)

Toivon, että tässä esitetyistä tiedoista on hyötyä. Annan mielelläni lisätietoja ja vastaan asiaa koskeviin kysymyksiin.

Kunnioittavasti

Samuel Podberesky

Assistant General Counsel for Aviation
Enforcement and Proceeding

▼B

LIITE VII

Tämän päätöksen 1 artiklan 2 kohdan b alakohdassa tarkoitetut Yhdysvaltojen valtiolliset elimet, joilla on valtuudet tutkia valituksia ja määrätä korvauksia sopimattomista tai harhaanjohtavista toimintatavoista sekä tarjota oikeuskeinoja yksityishenkilöille heidän asuinmaastaan tai kansallisuudestaan riippumatta, jos FAQ:iden mukaisesti sovellettavia periaatteita ei noudateta, ovat seuraavat:

1) Federal Trade Commission; ja

2) Yhdysvaltojen liikenneministeriö.

Federal Trade Commission toimii Federal Trade Commission Act -lain 5 pykälässä annetun valtuuden perusteella. Federal Trade Commissionin toimivaltaan eivät 5 pykälän mukaan kuulu pankit, säästäminen ja lainat sekä luotto-osuuskunnat, televiestintä, valtioiden välisiä kuljetuksia hoitavat kuljetusliikkeet, lentoyhtiöt, pakkausliikkeet eivätkä karjanvälittäjät. Vaikka vakuutusalaa ei ole erikseen mainittu 5 pykälän poikkeuksia koskevassa luettelossa, McCarran-Ferguson Act -lain [1] mukaisesti vakuutusalan sääntely kuuluu yksittäisten osavaltioiden toimivaltaan. Federal Trade Commissionin määräyksiä sovelletaan kuitenkin vakuutusalaan siltä osin kuin siitä ei säädetä osavaltioiden laeissa. Federal Trade Commissionin toimivaltaan kuuluvat vakuutusyhtiöiden sopimattomat ja harhaanjohtavat käytännöt, kun kyseessä on muu kuin varsinainen vakuutustoiminta.

Lentoyhtiöiden osalta periaatteiden ja FAQ:iden noudattamista valvoo Yhdysvaltojen liikenneministeriö, jolla on United States Coden 49 osaston 41712 pykälän mukaisesti toimivalta tapauksissa, joissa se voi panna asian vireille omien tutkimustensa sekä yksityishenkilöiltä, matkatoimistoilta, lentoyhtiöiltä ja Yhdysvaltojen ja muiden maiden hallintoelimiltä saamiensa virallisten ja epävirallisten valitusten perusteella.

[1] 15 U.S.C. § 1011 et seq.