32000D0520

L 215/7 URADNI LIST EVROPSKIH SKUPNOSTI 25.8.2000

ODLOČBA KOMISIJE
z dne 26. julija 2000
po Direktivi Evropskega parlamenta in Sveta 95/46/ES o primernosti zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana in s tem povezana najpogosteje zastavljena vprašanja, ki jih je izdalo Ministrstvo za trgovino ZDA

(notificirano pod dokumentarno številko K(2000)2441)

(Besedilo velja za EGP)

(2000/520/ES)

KOMISIJA EVROPSKIH SKUPNOSTI JE –

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti,

ob upoštevanju Direktive Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ([1]) ter zlasti člena 25(6) Direktive,

ob upoštevanju naslednjega:

(1) Po Direktivi 95/46/ES morajo države članice zagotoviti, da se prenos osebnih podatkov v tretjo državo lahko izvede, samo če zadevna tretja država zagotovi ustrezno raven zaščite in če se pred prenosom upoštevajo predpisi države članice o izvajanju drugih določb Direktive.

(2) Komisija lahko ugotovi, da tretja država zagotavlja ustrezno raven zaščite. V tem primeru se osebni podatki lahko prenesejo iz držav članic, ne da bi bila potrebna dodatna jamstva.

(3) Po Direktivi 95/46/ES je treba raven zaščite podatkov oceniti glede na vse okoliščine, v katerih poteka postopek ali postopki prenosa podatkov, in glede na dane razmere. Delovna skupina o varstvu posameznikov pri obdelavi osebnih podatkov, ki je bila ustanovljena z navedeno direktivo ([2]), je objavila smernice za takšno ocenjevanje ([3]).

(4) Glede na različne pristope do zaščite podatkov v tretjih državah morata biti ocena primernosti zaščite in uveljavitev vseh odločb na podlagi člena 25(6) Direktive 95/46/ES izvedena na način, ki ni niti samovoljno ali neupravičeno diskriminatoren do tretjih držav ali med tretjimi državami, v katerih prevladujejo podobne razmere, niti ne pomeni prikrite ovire za trgovino, pri čemer se upoštevajo sedanje mednarodne obveznosti Skupnosti.

(5) Ustrezna raven zaščite pri prenosu podatkov iz Skupnosti v Združene države, ki jo priznava ta odločba, bi morala biti dosežena, če organizacije ravnajo po načelih zasebnosti varnega pristana za zaščito podatkov, ki se prenašajo iz države članice v Združene države, (v nadaljnjem besedilu „načela“) in po najpogosteje zastavljenih vprašanjih („Frequently Asked Questions“, v nadaljnjem besedilu „FAQ“), ki zagotavljajo smernice za uveljavljanje načel in jih je izdala Vlada Združenih držav 21. julija 2000. Poleg tega morajo organizacije javno razglasiti svojo politiko varovanja zasebnosti in biti v okviru pristojnosti Federal Trade Commission (FTC) po oddelku 5 Federal Trade Commission Act, ki prepoveduje nepoštena ali goljufiva dejanja ali prakse v trgovini ali prakse, ki vplivajo na trgovino, ali v okviru pristojnosti kakega drugega z zakonom določenega organa, ki bo učinkovito zagotovil skladnost z načeli, uveljavljenimi v skladu s FAQ.

(6) Področja in/ali obdelava podatkov, ki niso v okviru pristojnosti nobenega od vladnih organov v Združenih državah, naštetih v Prilogi VII k tej odločbi, ne sodijo na področje uporabe te odločbe.

(7) Za zagotovitev pravilne uporabe te odločbe je potrebno, da zainteresirane stranke, kot so subjekti podatkov, izvozniki podatkov in organi za zaščito podatkov, priznavajo organizacije, ki spoštujejo načela in FAQ. V ta namen se mora Ministrstvo za trgovino ZDA ali od njega imenovani subjekt zavezati, da bo vzdrževalo in javnosti omogočilo

([1]) UL L 281, 23.11.1995, str. 31.
([2]) Spletna stran Delovne skupine je: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.
([3]) WP 12: Prenosi podatkov v tretje države: uporabljata se člena 25 in 26 Direktive o zaščiti podatkov v EU, ki jo je Delovna skupina sprejela 24. julija 1998.

dostop do seznama organizacij, ki so samocertificirale zavezanost k načelom, uveljavljenim v skladu s FAQ, in ki so v okviru pristojnosti vsaj enega od vladnih organov, naštetih v Prilogi VII k tej odločbi.

(8) Zaradi preglednosti in zaščite zmožnosti pristojnih organov v državah članicah, da zagotovijo varstvo posameznika glede obdelave njegovih osebnih podatkov, je treba s to odločbo določiti izjemne okoliščine, ki lahko upravičijo prekinitev prenosa posebnih podatkov, ne glede na ugotovitve o ustrezni zaščiti.

(9) „Varni pristan“, vzpostavljen z načeli in FAQ, bo morda treba preveriti z vidika izkušenj in razvoja v zvezi z varstvom zasebnosti v okoliščinah, ko tehnologija vse bolj lajša prenos in obdelavo osebnih podatkov, ter z vidika poročil o uporabi, ki jih predložijo za uveljavljanje pristojni organi.

(10) Mnenja Delovne skupine za varstvo posameznikov glede obdelave osebnih podatkov, ustanovljene po členu 29 Direktive 95/46/ES, o ravni zaščite, ki jo v Združenih državah zagotavljajo načela „varnega pristana“, so bila upoštevana pri pripravi te odločbe ([1]).

(11) Ukrepi, predvideni s to odločbo, so v skladu z mnenjem odbora, ustanovljenega po členu 31 Direktive 95/46/ES.

(12) Po Direktivi Sveta 1999/468 in zlasti členu 8 Direktive je Evropski parlament 5. julija 2000 sprejel Resolucijo A5-0177/200 o osnutku Odločbe Komisije o primernosti zaščite, ki jo zagotavljajo „načela zasebnosti varnega pristana“ in s tem povezana najpogosteje zastavljena vprašanja, ki jih je izdalo Ministrstvo za trgovino ZDA. ([2])

Komisija je ponovno preučila osnutek odločbe z vidika navedene resolucije in sklenila, da čeprav je Evropski parlament izrazil stališče, da so pri „načelih varnega pristana“ in s tem povezanih FAQ potrebne nekatere izboljšave, še preden se šteje, da je zagotovljena „ustrezna zaščita“, ni ugotovil, da bi Komisija s sprejetjem odločbe presegla svoja pooblastila –

SPREJELA NASLEDNJO ODLOČBO:

Člen 1

1. V členu 25(2) Direktive 95/46/ES se za vse dejavnosti, ki sodijo na področje uporabe navedene direktive, šteje, da „načela zasebnosti varnega pristana“ (v nadaljnjem besedilu „načela“), kakor so navedena v Prilogi I k tej odločbi in uveljavljena v skladu s smernicami iz najpogosteje zastavljenih vprašanj (v nadaljnjem besedilu „FAQ“), ki jih je izdalo Ministrstvo za trgovino ZDA 21. julija 2000 in so navedena v Prilogi II k tej odločbi, zagotavljajo ustrezno raven zaščite osebnih podatkov, ki se prenašajo iz Skupnosti v organizacije s sedežem v Združenih državah, pri čemer se upoštevajo naslednji dokumenti, ki jih je izdalo Ministrstvo za trgovino ZDA:

(a) pregled uveljavljanja varnega pristana iz Priloge III;

(b) memorandum o odškodnini za kršitve zasebnosti in izrecnih pooblastilih v pravu ZDA iz Priloge IV;

(c) pismo Federal Trade Commission iz Priloge V;

(d) pismo Ministrstva za promet iz Priloge VI.

2. Pri vsakem prenosu podatkov morajo biti izpolnjeni naslednji pogoji:

(a) organizacija, ki prejema podatke, je nedvomno in javno razglasila zavezanost k spoštovanju načel, uveljavljenih v skladu s FAQ; in

(b) organizacija je podvržena zakonskim pooblastilom vladnega organa v Združenih državah, naštetega v Prilogi VII k tej odločbi, ki je pooblaščen za preiskave pritožb ter za pridobitev pomoči v primeru nepoštenih ali goljufivih praks, pa tudi odškodnine za posameznike, ne glede na njihovo državo stalnega prebivališča ali državljanstvo, kadar organizacije ne spoštujejo načel, uveljavljenih v skladu s FAQ.

3. Pogoji iz odstavka 2 štejejo za izpolnjene za vsako organizacijo, ki samocertificira zavezanost k načelom, uveljavljenim v skladu s FAQ, od datuma, ko organizacija uradno obvesti Ministrstvo za trgovino ZDA (ali njegovega pooblaščenega predstavnika) o javni razglasitvi zavezanosti iz odstavka 2(a) in o identiteti vladnega organa iz odstavka 2(b).

([1]) WP 15: Mnenje 1/99 o ravni zaščite podatkov v Združenih državah in razpravah, ki potekajo med Evropsko komisijo in Združenimi državami.
WP 19: Mnenje 2/99 o primernosti „mednarodnih načel varnega pristana“, ki jih je izdalo Ministrstvo za trgovino 19. aprila 1999.
WP 21: Mnenje 4/99 o najpogosteje zastavljenih vprašanjih (Frequently Asked Questions) glede primernosti „mednarodnih načel varnega pristana“, ki naj bi jih v zvezi s predlaganimi „načeli varnega pristana“ izdalo Ministrstvo za trgovino.
WP 23: Delovni dokument o trenutnem stanju razprav, ki potekajo med Evropsko komisijo in Vlado Združenih držav glede „mednarodnih načel varnega pristana“.
WP 27: Mnenje 7/99 o ravni zaščite podatkov, zagotovljene z načeli „varnega pristana“, ki jih je skupaj z najpogosteje zastavljenimi vprašanji in drugimi s tem povezanimi dokumenti objavilo Ministrstvo za trgovino 15. in 16. novembra 1999.
WP 31: Mnenje 3/2000 o pogovorih med EU/ZDA glede dogovora „varni pristan“.
WP 32: Mnenje 4/2000 o ravni zaščite, ki jo zagotavljajo „načela varnega pristana“.

([2]) Resolucija še ni objavljena v Uradnem listu.

Člen 2

Ta odločba zadeva samo primernost zaščite, ki jo v Združenih državah zagotavljajo po načelih, uveljavljenih v skladu s FAQ, zaradi izpolnitve zahtev iz člena 25(1) Direktive 95/46/ES, in ne vpliva na uporabo drugih določb navedene direktive, ki zadevajo obdelavo osebnih podatkov v državah članicah, zlasti člena 4 direktive.

Člen 3

1. Brez poseganja v pooblastila pristojnih organov v državah članicah, da ukrepajo zaradi zagotovitve skladnosti z nacionalnimi predpisi, sprejetimi po drugih določbah, kakor so tiste iz člena 25 Direktive 95/46/ES, lahko ti organi izvršijo svoja obstoječa pooblastila za prekinitev prenosa podatkov v organizacijo, ki je samocertificirala zavezanost k načelom, uveljavljenim v skladu s FAQ, da bi zaščitili posameznike glede obdelave njihovih osebnih podatkov v primerih, kadar:

(a) vladni organ v Združenih državah, naveden v Prilogi VII k tej odločbi, ali neodvisni pritožbeni mehanizem v smislu točke (a) načela uveljavljanja iz Priloge I k tej odločbi ugotovita, da organizacija krši načela, uveljavljena v skladu s FAQ; ali

(b) obstaja precejšnja verjetnost, da se načela kršijo; obstaja utemeljena podlaga za prepričanje, da zadevni mehanizem uveljavljanja ne sprejema ali ne bo sprejel ustreznih in pravočasnih ukrepov za rešitev spornega primera; nadaljnji prenos podatkov bi povzročil neposredno nevarnost za nastanek velike škode za subjekte podatkov; in so si pristojni organi v državah članicah v danih okoliščinah razumno prizadevali, da bi organizacijo obvestili in ji dali priložnost za odgovor.

Prekinitev preneha takoj, ko je zagotovljena skladnost z načeli, uveljavljenimi v skladu s FAQ, in so zadevni pristojni organi v Skupnosti o tem uradno obveščeni.

2. Kadar države članice sprejmejo ukrepe na podlagi odstavka 1, o tem nemudoma obvestijo Komisijo.

3. Države članice in Komisija se prav tako medsebojno obvestijo, kadar ukrepanje organov, ki so v Združenih državah odgovorni za zagotavljanje skladnosti z načeli, uveljavljenimi v skladu s FAQ, takšne skladnosti ne zagotovi.

4. Če informacije, zbrane po odstavkih 1, 2 in 3, dokazujejo, da kateri koli organ, ki je v Združenih državah odgovoren za zagotavljanje skladnosti z načeli, uveljavljenimi v skladu s FAQ, njegove naloge ne opravlja učinkovito, Komisija obvesti Ministrstvo za trgovino ZDA ter po potrebi in po postopku iz člena 31 Direktive 95/46/ES predloži osnutek ukrepov za razveljavitev ali odložitev te odločbe ali omejitev področja njene uporabe.

Člen 4

1. Ta odločba se lahko kadar koli prilagodi glede na izkušnje z njeno uporabo in/ali če zakonodaja ZDA prevzame raven zaščite, ki jo zagotavljajo načela in FAQ.

Komisija v vsakem primeru oceni izvajanje sedanje odločbe na podlagi razpoložljivih informacij tri leta po uradnem obvestilu držav članic o odločbi in poroča odboru, ustanovljenemu po členu 31 Direktive 95/46/ES, o vseh ustreznih ugotovitvah, vključno z vsemi dokazi, ki bi lahko vplivali na oceno, da določbe iz člena 1 te odločbe zagotavljajo ustrezno zaščito v smislu člena 25 Direktive 95/46/ES, in s katerim koli dokazom, da se sedanja odločba uporablja diskriminatorno.

2. Komisija po potrebi predloži osnutek ukrepov po postopku iz člena 31 direktive 95/46/ES.

Člen 5

Države članice sprejmejo vse potrebne ukrepe za uskladitev s to odločbo najpozneje v 90 dneh od datuma uradnega obvestila o odločbi državam članicam.

Člen 6

Ta odločba je naslovljena na države članice.

V Bruslju, 26. julija 2000

Za Komisijo

Frederik BOLKESTEIN

Član Komisije

PRILOGA I

NAČELA ZASEBNOSTI VARNEGA PRISTANA

ki jih je izdalo Ministrstvo za trgovino ZDA 21. julija 2000

Izčrpna zakonodaja Evropske unije o varstvu zasebnosti, Direktiva o zaščiti podatkov (Direktiva), je začela veljati 25. oktobra 1998. Direktiva zahteva, da se lahko osebni podatki prenašajo samo v tiste države nečlanice EU, ki zagotavljajo „primerno“ raven varstva zasebnosti. Združene države in Evropska unija so si sicer zadale skupen cilj, da krepita varstvo zasebnosti za svoje državljane, vendar se pristop Združenih držav do zasebnosti razlikuje od pristopa Evropske unije. V Združenih državah se uporablja sektorski pristop, ki temelji na mešanici predpisov, uredb in samourejanja. Glede na te razlike so mnoge organizacije ZDA izrazile negotovost glede vpliva „standarda primernosti“, ki ga zahteva EU, na prenos osebnih podatkov iz Evropske unije v Združene države.

Za zmanjšanje negotovosti in zagotovitev bolj predvidljivega okvira za prenos takih podatkov Ministrstvo za trgovino v okviru svojih zakonskih pooblastil za spodbujanje, pospeševanje in razvijanje mednarodne trgovine izdaja ta dokument in najpogosteje postavljena vprašanja – FAQ („načela“). Razvoj načel je potekal v posvetovanju s predstavniki industrije in širše javnosti zaradi lajšanja trgovskih in gospodarskih stikov med Združenimi državami in Evropsko unijo. Načela so namenjena izključno organizacijam ZDA, ki prejemajo osebne podatke iz Evropske unije, da izpolnijo pogoje varnega pristana in iz njega izhajajoče domneve o „primernosti“. Ker so bila načela oblikovana izključno za ta posebni namen, je lahko njihovo sprejetje v druge namene neustrezno. Načela se ne morejo uporabljati kot nadomestek za nacionalne predpise o izvajanju Direktive, ki se v državah članicah uporabljajo pri obdelavi osebnih podatkov.

Odločitve organizacij, da izpolnijo pogoje varnega pristana, je povsem prostovoljna, organizacije pa lahko izpolnijo pogoje varnega pristana na različne načine. Organizacije, ki se odločijo za zavezanost k načelom, morajo spoštovati načela, da bi pridobile in obdržale ugodnosti varnega pristana, in to javno razglasiti. Na primer, če organizacija pristopi k samourejevalnemu programu varstva zasebnosti, ki vsebujejo načela, izpolnjuje pogoje varnega pristana. Organizacije jih lahko izpolnjujejo tudi, če oblikujejo svoje samourejevalne politike varstva zasebnosti, če so v skladu z načeli. Kadar se organizacija glede skladnosti z načeli v celoti ali deloma opira na samourejanje, vendar tega samourejanja ne spoštuje, mora biti tako ravnanje kršitev po oddelku 5 Federal Trade Commission Act, ki prepoveduje nepoštena in goljufiva dejanja, ali po drugem zakonu ali predpisu, ki prepoveduje taka dejanja. (Glej v Prilogi seznam z zakonom določenih organov v ZDA, ki jih priznava EU.) Poleg tega lahko pogoje za ugodnosti varnega pristana izpolnjuje tudi organizacija, ki je podvržena zakonom in drugim predpisom (ali pravilom), ki učinkovito varujejo zasebnost posameznikov. V vseh primerih so ugodnosti varnega pristana zagotovljene od tistega datuma, ko organizacija, ki želi izpolniti pogoje varnega pristana, samocertificira pri Ministrstvu za trgovino (ali njegovemu pooblaščenemu predstavniku) zavezanost k načelom, v skladu s smernicami, ki jih glede samocertificiranja določajo najpogosteje zastavljena vprašanja.

Zavezanost k načelom je lahko omejena: (a) če je to potrebno za izpolnjevanje zahtev nacionalne varnosti, javnega interesa ali odkrivanja in pregona; (b) z zakonom, vladnim podzakonskim aktom ali sodno prakso, ki ustvarijo nezdružljivost obveznosti ali izrecnih pooblastil, pod pogojem, da lahko organizacija pri izvajanju takih pooblastil dokaže, da je njeno neizpolnjevanje načel toliko omejeno, kolikor je potrebno za izpolnitev prednostnih zakonitih interesov na podlagi takšnih pooblastil; ali (c) če direktiva ali pravo države članice dovoljuje izjeme in odstopanja, če da se te izjeme in odstopanja uporabljajo v primerljivih okoliščinah. V skladu s ciljem krepitve varstva zasebnosti si morajo organizacije prizadevati, da načela uveljavijo v celoti in pregledno, vključno z navedbo v svoji politiki varstva zasebnosti, kdaj se bodo izjeme, dovoljene z (b) zgoraj, redno uporabljale. Iz istega razloga se od organizacij pričakuje, da se, kadar načela in/ali pravo ZDA dopuščajo izbiro, po možnosti odločijo za možnost večjega varstva.

Organizacije bodo morda iz praktičnih ali kakih drugih razlogov želele uporabiti načela pri vseh postopkih obdelave podatkov, vendar so jih dolžne uporabiti samo pri podatkih, prenesenih po pristopu organizacij k varnemu pristanu. Organizacije niso dolžne uporabiti načel pri podatkih iz sistemov ročne obdelave, da bi izpolnile pogoj varnega pristana. Organizacije, ki želijo izkoristiti ugodnost varnega pristana pri informacijah, ki jih prejemajo iz EU iz

sistemov ročne obdelave, morajo načela uporabiti pri vsaki taki informaciji po pristopu k varnemu pristanu. Organizacija, ki želi razširiti ugodnosti varnega pristana na osebne podatke o človeških virih, ki jih prejme iz EU, za uporabo v okviru zaposlitvenih razmerij, mora to navesti ob samocertificiranju pri Ministrstvu za trgovino (ali njegovemu pooblaščenemu predstavniku) in izpolniti zahteve, ki so glede samocertificiranja določena v najpogosteje zastavljenih vprašanjih. Organizacije bodo lahko zagotovile tudi po členu 26 Direktive potrebna jamstva za bistvene predpise o varnosti zasebnosti, če vključujejo načela v pisne sporazume s strankami, ki prenašajo podatke iz EU, kakor hitro Komisija in države članice odobrijo druge predpise za take vzorčne pogodbe.

Pri vprašanjih razlage in skladnosti z načeli varnega pristana (vključno z najpogosteje zastavljenimi vprašanji) ter ustreznih politik varstva zasebnosti v organizacijah varnega pristana se uporablja pravo ZDA, razen kadar se organizacije zavežejo, da bodo sodelovale z evropskimi organi za zaščito podatkov. Če ni določeno drugače, se vse določbe načel varnega pristana in najpogosteje zastavljenih vprašanj uporabljajo v primerih, v katerih ustrezajo.

„Osebni podatki" in „osebne informacije" so podatki o znanem ali prepoznavnem posamezniku, ki so zapisani v kateri koli obliki in sodijo na področje uporabe Direktive ter jih organizacije ZDA prejmejo iz Evropske unije.

OBVESTILO

Organizacija mora posameznike obvestiti o namenih zbiranja in uporabe njihovih osebnih podatkov, kako se s kakršnimi koli vprašanji in pritožbami obrnejo na organizacijo, kategorije strank, katerim razkrije informacije, ter kakšne možnosti in sredstva za omejevanje uporabe ali razkritja organizacija ponuja posameznikom. To obvestilo organizacije mora biti jasno in nedvoumno, ko posameznika prvič prosi za zagotovitev osebnih podatkov ali kakor hitro je izvedljivo za tem, v vsakem primeru pa pred uporabo teh podatkov za namene, ki niso tisti, za katere jih je prvotno zbrala in obdelala pošiljajoča organizacija, ali pred prvim razkrijem tretji stranki ([1]).

MOŽNOST IZBIRE

Organizacija mora posameznikom ponuditi možnost izbire (zavrnitve) o tem, ali se bodo njihovi osebni podatki (a) razkrili tretji stranki ([1]) ali (b) se bodo uporabili za namen, ki ni nezdružljiv z namenom(-i), za katerega so bili prvotno zbrani ali ga(jih) je posameznik pozneje odobril. Posameznikom se morajo zagotoviti postopki izvršitve možnosti izbire, ki so jasni in razumljivi, dostopni in stroškovno ugodni.

Pri občutljivih podatkih (tj. osebnih podatkih, ki določajo zdravniško in zdravstveno stanje, rasno in etnično pripadnost, politična, verska in filozofska prepričanja, sindikalno članstvo, in podatkih o spolnem življenju posameznika) morajo imeti posamezniki možnost izrecne pozitivne izbire (privolitve), kadar je te podatke treba razkriti tretji stranki ali jih uporabiti za namen, ki ni tisti, za katerega so bili prvotno zbrani ali ga je posameznik pozneje odobril s svojo izbiro privolitve. V vsakem primeru mora organizacija obravnavati kot občutljive vse podatke, ki jih je prejela od tretje stranke, kadar jih kot občutljive identificira in obravnava tretja stranka.

PRENOS TRETJEMU

Pri razkrivanju podatkov tretji stranki morajo organizacije uporabiti načeli obvestila in možnosti izbire. Kadar organizacija želi razkriti podatke tretji stranki, ki v vlogi posrednika izvaja nalogo(-e) v imenu in po navodilih organizacije, kakor je opisano v sprotni opombi, lahko to stori, če je bodisi tretja stranka pristopila k načelom ali je podvržena Direktivi ali je zajeta z drugo primerno zaščito podatkov bodisi da s to tretjo stranjo sklene pisni sporazum, po katerem mora tretja stranka zagotoviti vsaj takšno raven varstva zasebnosti, kakor jo zahtevajo ustrezna načela. Če organizacija ravna v skladu s temi zahtevami, ne bo odgovorna (razen če se organizacija drugače dogovori), kadar tretja stranka, kateri prenese take podatke, te podatke obdela v nasprotju z vsemi omejitvami in dogovori, razen če je organizacija vedela ali bi morala vedeti, da jih bo tretja stranka obdelala na ta način, in ni ustrezno ukrepala, da bi tako obdelavo preprečila ali ustavila.

([1]) Obvestilo in možnost izbire nista potrebna, kadar se podatki razkrivajo tretji stranki, ki v vlogi posrednika izvaja nalogo(-e) v imenu in po navodilih organizacije. Po drugi strani pa se pri teh razkritjih uporablja načelo prenosa tretjemu.

VARNOST

Organizacije, ki pripravljajo, vzdržujejo, uporabljajo ali razširijo osebne podatke, morajo sprejeti ustrezne preventivne ukrepe, da jih zavarujejo pred izgubo, zlorabo in nepooblaščenim dostopom, razkritjem, spreminjanjem ali uničenjem.

NEOKRNJENOST PODATKOV

V skladu z načeli morajo osebni podatki ustrezati namenu, za katerega se bodo uporabili. Organizacija ne sme obdelovati osebnih podatkov na način, ki je nezdružljiv z nameni, za katere so bili podatki zbrani ali jih je posameznik pozneje odobril. V obsegu, potrebnem za ta namen, mora organizacija z ustreznimi ukrepi zagotoviti, da so podatki zanesljivi za nameravano uporabo, točni, popolni in trenutni.

DOSTOP

Posamezniki morajo imeti dostop do svojih osebnih podatkov, ki jih hrani organizacija, in možnost, da te podatke popravijo, spremenijo ali izbrišejo, kadar niso točni, razen kadar bi bili stroški ali izdatki za zagotovitev dostopa nesorazmerni s tveganjem za zasebnost zadevnega posameznika ali kadar bi bile kršene pravice drugih oseb.

IZVAJANJE

Učinkovito varstvo zasebnosti mora vključevati mehanizme, ki zagotavljajo skladnost z načeli, pritožbene mehanizme za posameznike, na katere se podatki nanašajo in jih neizpolnjevanje načel prizadene, in posledice za organizacije, kadar ne spoštujejo načel. Ti mehanizmi morajo vključevati vsaj (a) lahko dostopne in stroškovno ugodne neodvisne pritožbene mehanizme, ki omogočajo, da se pritožbe in spori vsakega posameznika preiščejo in rešijo s sklicevanjem na načela ter prisodi odškodnina, kadar veljavno pravo ali pobude zasebnega sektorja tako predvidevajo; (b) postopke za preverjanje resničnosti izjav in zatrjevanj podjetij glede njihove prakse varovanja zasebnosti ter preverjanje izvajanja praks varstva zasebnosti na naveden način; in (c) obveznosti odpravljanja težav, ki nastanejo, ker organizacije, ki so javno razglasile svojo zavezanost k načelom, teh ne spoštujejo, in posledice za te organizacije. Sankcije morajo biti dovolj stroge, da zagotovijo spoštovanje načel.

Priloga

Seznam z zakonom določenih organov v ZDA, ki jih priznava Evropska unija

Evropska unija priznava naslednjim ameriškim vladnim organom pooblastila za preiskavo pritožb ter za pridobitev pomoči v primeru nepoštenih in goljufivih praks, pa tudi odškodnine za posameznike v primerih neizpolnjevanja načel, uveljavljenih v skladu s FAQ:

— Federal Trade Commission na podlagi njenih pooblastil iz oddelka 5 Federal Trade Commission Act,

— Ministrstvo za promet na podlagi njegovih pooblastil iz naslova 49 oddelka 41712 United States Code.

PRILOGA II

NAJPOGOSTEJE ZASTAVLJENA VPRAŠANJA (FAQ)

FAQ 1 – Občutljivi podatki

V: *Ali mora organizacija vedno zagotoviti možnost izrecne izbire (privolitve) pri občutljivih podatkih?*

O: Ne, ta možnost se ne zahteva, kadar je obdelava podatkov: (1) v življenjskem interesu subjekta podatkov ali druge osebe; (2) potrebna za uveljavitev pravnih zahtevkov ali obrambe; (3) nujna za zagotovitev zdravstvene nege ali diagnoze; (4) izvedena med potekom zakonitih dejavnosti politično, filozofsko, versko ali sindikalno usmerjenega sklada, združenja ali kake druge nepridobitne organizacije in pod pogojem, da obdelava zadeva izključno člane te organizacije ali osebe, ki so v zvezi z njenimi dejavnostmi z organizacijo v rednih stikih, ter da se podatki ne razkrijejo tretji stranki brez privolitve subjektov podatkov; (5) potrebna za izvajanje obveznosti organizacije na področju delovnega prava; ali (6) povezana s podatki, ki jih je posameznik očitno dal v javnost sam.

FAQ 2 – Izjeme za novinarsko področje

V: *Ali se glede na ustavna varstva svobode tiska in izjemo Direktive za novinarsko gradivo načela varnega pristana uporabljajo za osebne podatke, ki se zbirajo, hranijo in razširjajo za novinarske namene?*

O: Kadar so pravice svobodnega tiska iz prvega amandmaja Ustave ZDA v koliziji z interesom varstva zasebnosti, mora prvi amandma uravnotežiti te interese glede na dejavnosti fizičnih in pravnih oseb v ZDA. Za osebne podatke, ki se zbirajo za objavo v časopisu ali po radiu in televiziji ali za drugo obliko javnega sporočanja novinarskega gradiva, ne glede na to, ali so bili dejansko uporabljeni, pa tudi za podatke, najdene v predhodno objavljenem gradivu, razširjenem iz medijskih arhivov, ne veljajo zahteve načel varnega pristana.

FAQ 3 – Sekundarna odgovornost

V: *Ali so ponudniki internetnih storitev (Internet Service Providers, ISP) in telekomunikacijska podjetja ter druge organizacije odgovorni po načelih varnega pristana, kadar v imenu druge organizacije zgolj prenašajo, usmerjajo, zamenjujejo ali pridobivajo podatke, ki lahko kršijo njihove določbe?*

O: Ne. Kakor utemeljuje sama Direktiva, varni pristana ne ustvarja sekundarne odgovornosti. Kolikor je organizacija zgolj posrednik podatkov, ki jih prenaša tretja stranka ter pri tem ne določa namenov in načinov obdelave teh osebnih podatkov, ni odgovorna.

FAQ 4 – Investicijske banke in revizorske hiše

V: *Dejavnosti revizorjev in investicijskih bank bodo lahko vključujejo obdelavo osebnih podatkov brez privolitve ali vednosti posameznika. V kakšnih okoliščinah je to združljivo z načeli obvestila, možnosti izbire in dostopa?*

O: Investicijske banke in revizorji lahko obdelujejo podatke brez vednosti posameznika samo v takšnem obsegu in tako dolgo, kolikor je potrebno, da se zadosti zakonskim ali javnim interesom, ter v drugih okoliščinah, v katerih bi uporaba teh načel škodovala zakonitim interesom organizacije. Ti zakoniti interesi vključujejo spremljanje izpolnjevanja zakonitih obveznosti in zakonitih računovodskih dejavnosti podjetij ter potrebo po zaupnosti v zvezi z morebitnimi nakupi, združitvami, skupnimi vlaganji ali drugo podobno transakcijo, ki jo opravijo investicijske banke in revizorji.

FAQ 5 [1] **– Vloga organov za zaščito podatkov**

V: *Kako bodo podjetja, ki se zavežejo, da bodo sodelovale z organi za zaščito podatkov Evropske unije, prevzele navedene obveznosti in kako se bodo te obveznosti izvajale?*

O: V okviru varnega pristana se morajo organizacije ZDA, ki prejemajo osebne podatke iz EU, zavezati, da bodo uporabile učinkovite mehanizme za zagotavljanje skladnosti z načeli varnega pristana. Kakor je natančneje določeno v načelu uveljavljanja, morajo zagotoviti (a) pritožbeni mehanizem za posameznike, na katere podatki nanašajo, (b) postopke za preverjanje resničnosti izjav in zatrjevanj, ki jih dajejo glede svoje prakse varstva zasebnosti in (c) obveznost reševanja težav, ki nastanejo zaradi neizpolnjevanja načel, in posledice za take organizacije. Organizacija lahko izpolni točki (a) in (c) načela uveljavljanja, če se zaveže k zahtevam tega FAQ glede sodelovanja z organi za zaščito podatkov.

Organizacija se lahko zaveže, da bo sodelovala z organi za zaščito podatkov, tako da pri certificiranju zavezanosti k načelom varnega pristana pri Ministrstvu za trgovino (glej FAQ 6 o samocertificiranju) izjavi naslednje:

1. da se je organizacija odločila izpolniti zahteve iz točk (a) in (c) načela uveljavljanja varnega pristana z zavezo o sodelovanju z organi za zaščito podatkov;

2. da bo sodelovala z organi za zaščito podatkov pri preiskavah in reševanju pritožb, s sklicevanjem na načela varnega pristana; in

3. da bo upoštevala vsak nasvet organov za zaščito podatkov, kadar ti organi menijo, da mora organizacija s posebnim ukrepom poskrbeti za uskladitev z načeli varnega pristana, vključno z reševanjem pritožb in izplačilom odškodnin v korist posameznikov, ki so bili prizadeti zaradi kakršnega koli neizpolnjevanja načel, ter da bo organom za zaščito podatkov pisno potrdila, da je take ukrepe sprejela.

Sodelovanje z organi za zaščito podatkov EU bo potekalo prek informacij in nasvetov na naslednji način:

— Nasvete organov za zaščito podatkov EU bo posredoval neuradni forum, ustanovljen na ravni Evropske unije, ki bo med drugim pomagal zagotoviti usklajen in skladen pristop.

— Forum bo zadevnim organizacijam ZDA svetoval glede nerešenih pritožb posameznikov v zvezi z ravnanjem z osebnimi podatki, ki so bili preneseni iz Evropske unije v okviru varnega pristana. Nasvet bo oblikovan za zagotovitev pravilne uporabo načel varnega pristana in bo vključeval vsa pravna sredstva za zadevnega posameznika(-e), ki ga(jih) bodo organi za zaščito podatkov šteli za ustreznega.

— Forum bo takšne nasvete zagotavljal v odgovor na posredovana stališča iz zadevnih organizacij in/ali na neposredne pritožbe posameznikov zoper organizacije, ki so se zavezale, da bodo sodelovale z organi za zaščito podatkov za namene varnega pristana, pri čemer bo spodbujal in po potrebi pomagal takim posameznikom, da na začetku uporabijo morebitni notranji mehanizem reševanja pritožb, ki ga lahko ima organizacija.

— Nasvet bo izdan šele, ko bosta oba udeleženca v sporu imela ustrezno priložnost za predložitev pripomb in kakršnih koli dokazov. Forum bo poskušal dati nasvet tako hitro, kakor to dopušča zahteva po pravilnem postopku. Praviloma si bo forum prizadeval zagotoviti nasvet v 60 dneh po prejetju pritožbe ali posredovanega stališča in po možnosti še prej.

— Forum bo javno objavil rezultate svojih preučevanj pritožb, če se mu bo to zdelo primerno.

— Nasvet foruma ne povzroči odgovornosti za forum ali za posamezne organe za zaščito podatkov.

[1] Vključitev tega FAQ v paket je odvisna od dogovora z organi za zaščito podatkov. Ti so obravnavali sedanje besedilo v členu 29 Delovne skupine in večina meni, da je sprejemljivo, vendar so končno stališče pripravljeni sprejeti le v okviru celotnega mnenja, ki ga bo Delovna skupina izdala o sklepnem paketu.

Kakor je navedeno zgoraj, se morajo organizacije, ki se odločijo za tak način reševanja sporov, zavezati, da bodo ravnale po nasvetu organov za zaščito podatkov. Če organizacija tudi po 25 dneh po prejemu nasveta ne ravna v skladu z njim in če ne ponudi zadovoljive razlage za zamudo, forum sporoči svojo namero, da bo predložil zadevo Federal Trade Commission ali drugemu zveznemu ali državnemu organu ZDA, ki ima zakonska pooblastila za pregon v primeru goljufije ali zavajanja, ali da bo sklenil, da gre za resno kršitev sporazuma o sodelovanju, ki ga je zato treba šteti za ničnega in neveljavnega. V slednjem primeru bo forum obvestil Ministrstvo za trgovino (ali njegovega pooblaščenega predstavnika), da ustrezno spremeni seznam organizacij v okviru varnega pristana. Vsako neizpolnjevanje zaveze o sodelovanju z organi za zaščito podatkov, pa tudi neizpolnjevanje načel varnega pristana pomeni goljufivo prakso in kršitev po oddelku 5 Federal Trade Commission Act ali drugega podobnega zakona.

Organizacije, ki se bodo odločile za sodelovanje, bodo morale plačati letno pristojbino za pokrivanje stroškov delovanja foruma, dodatno pa so lahko zaprošene za kritje vseh potrebnih stroškov za prevajanje, ki izhajajo iz obravnave forumu predloženih stališč ali pritožb posameznikov zoper organizacije. Letna pristojbina ne bo presegla 500 USD in bo nižja za manjša podjetja.

Možnost sodelovanja z organi za zaščito podatkov bo na voljo organizacijam, ki pristopijo k varnemu pristanu v treh letih. Organi za zaščito podatkov bodo pred iztekom tega obdobja ponovno preučili ta dogovor, če se bo za to možnost odločilo preveliko število organizacij ZDA.

FAQ 6 – Samocertificiranje

V: *Kako organizacija samocertificira svojo zavezanost k načelom varnega pristana?*

O: Ugodnosti varnega pristana se zagotavljajo od datuma, ko organizacija v skladu s spodnjimi smernicami pri Ministrstvu za trgovino (ali njegovem pooblaščenem predstavniku) samocertificira svojo zavezanost k načelom.

Če se želi organizacija samocertificirati glede varnega pristana, lahko Ministrstvu za trgovino (ali njegovemu pooblaščenemu predstavniku) pošlje pismo, ki ga podpiše vodstveni delavec v imenu organizacije, ki pristopa k varnemu pristanu, in mora vsebovati vsaj naslednje podatke:

1. ime organizacije, poštni naslov, elektronski naslov, telefonsko številko in število faksa;

2. opis dejavnosti organizacije v zvezi z osebnimi podatki, ki jih prejema iz EU; in

3. opis politike organizacije glede varstva zasebnosti, vključno s podatki: (a) kje je ta politika na voljo za javnost, (b) datum dejanske uveljavitve te politike, (c) kontaktno službo, ki se ukvarja s pritožbami, zahtevami po dostopu in drugimi vprašanji, ki izhajajo iz načel varnega pristana, (d) posebno zakonsko telo, ki je pristojno za obravnavo morebitnih zahtevkov zoper organizacije zaradi morebitnih nepoštenih in goljufivih praks in kršitev zakonov ali predpisov o zasebnosti (in ki je navedeno v prilogi k načelom), (e) ime katerega koli programa za varstvo zasebnosti, katerega član je organizacija, (f) metodo preverjanja (znotraj organizacije, tretja stran) ([1]), in (g) neodvisni pritožbeni mehanizem, ki je na voljo za preiskave nerešenih pritožb.

Kadar organizacija želi, da bi ugodnosti varnega pristana zajele tudi podatke o človeških virih, ki so iz Evropske unije preneseni za uporabo na področju zaposlitvenih razmerij, lahko to stori, kadar obstaja zakonsko telo, pristojno za obravnavo pritožb v zvezi s podatki o človeških virih, ki je navedeno v prilogi k načelom. Organizacija mora to navesti tudi v svojem pismu ter se zavezati, da bo sodelovala z zadevnim organom ali organi EU v skladu s FAQ 9 in FAQ 5 ter da bo upoštevala nasvet, ki ga bo dobila od teh organov.

Ministrstvo za trgovino (ali od njega imenovan predstavnik) bo vodilo seznam vseh organizacij, ki predložijo taka pisma, pri čemer bo zagotavljalo razpoložljivost ugodnosti varnega pristana, ter bo letno ažuriralo podatke na tem seznamu na podlagi letnih pisem in uradnih obvestil, ki jih prejme v skladu s FAQ 11. Taka samocertifikacijska pisma se zagotavljajo najmanj vsako leto. Drugače se organizacija zbriše s seznama in ji ugodnosti varnega pristana ne bodo več zagotovljene. Seznam insamocertifikacijska

([1]) Glej FAQ 7 o preverjanju.

pisma organizacij bodo na voljo javnosti. Vse organizacije, ki samocertificirajo načela varnega pristana, morajo tudi v ustreznih objavljenih izjavah o svoji politiki zasebnosti navesti, da spoštujejo načela varnega pristana.

Pri podatkih, ki jih organizacija prejme v času, ko uživa ugodnosti varnega pristana, zavezanost k načelom varnega pristana ni časovno omejena. Ta zaveza pomeni, da bo organizacija uporabljala načela, dokler take podatke hrani, uporablja ali razkriva, četudi pozneje iz kakršnega koli razloga izstopi iz varnega pristana.

Organizacija, ki zaradi združitve ali prevzema preneha obstajati kot ločena pravna oseba, mora o tem vnaprej uradno obvestiti Ministrstvo za trgovino (ali njegovega pooblaščenega predstavnika). V uradnem obvestilu mora tudi navesti, ali bo prevzemna ali združena organizacija (1) še naprej zavezana k načelom varnega pristana po zakonu o prevzemu ali združitvi ali (2) se bo odločila, da samocertificira zavezanost k načelom varnega pristana ali uvede druge varovalke, kot je pisni sporazum, ki bo zagotovil zavezanost k načelom. Kadar se ne uporabljata ne (1) ne (2), se morajo takoj zbrisati vsi podatki, ki so bili pridobljeni v okviru varnega pristana.

Ni potrebno, da organizacija spoštuje načela varnega pristana pri vseh osebnih podatkih, mora pa spoštovati načela varnega pristana pri vseh osebnih podatkih, ki jih je prejela iz EU po pristopu k varnemu pristanu.

Za vsako zavajanje širše javnosti v zvezi zavezanostjo k načelom varnega pristana lahko Federal Trade Commission ali drug pristojni državni organ ukrepa proti kršitvi. Zavajanje Ministrstva za trgovino (ali njegovega pooblaščenega predstavnika) se lahko kazensko preganja po False Statements Acts (18 U.S.C. § 1001).

FAQ 7 – Preverjanje

V: *Kako organizacije zagotovijo postopke za preverjanje resničnosti izjav in zatrjevanj, ki jih dajo organizacije glede svojih praks zasebnosti varnega pristana, ter izvajanja teh praks na naveden način in v skladu z načeli varnega pristana?*

O: Da organizacija izpolni zahteve preverjanja iz načela uveljavljanja, lahko takšne izjave in zatrjevanja preveri s samoocenjevanjem ali zunanjim pregledom skladnosti z načeli.

Pri samoocenjevanju mora tako preverjanje pokazati, da je objavljena politika organizacije glede zasebnosti osebnih podatkov, prejetih iz EU, točna, celovita, prikazana na vidnem mestu, v celoti izvedena in dostopna. Pokazati mora tudi, da je njena politika zasebnosti v skladu z načeli varnega pristana; da so posamezniki obveščeni o kakršnem koli notranjem mehanizmu organizacije za obravnavo pritožb in o neodvisnih mehanizmih, prek katerih se lahko pritožijo; da je vzpostavila postopke za izobraževanje zaposlenih o izvajanju politike ter za disciplinske ukrepe v primeru kršitve te politike; ter da je vzpostavila notranje postopke za redno objektivno pregledovanje usklajenosti z zgoraj navedenim. Izjavo o samooceni mora podpisati vodstveni delavec ali drug pooblaščeni predstavnik organizacije vsaj enkrat na leto in mora biti na voljo posameznikom na njihovo zahtevo ali v okviru preiskave ali pritožbe zaradi neskladnosti z načeli.

Organizacije morajo voditi evidenco o svojem izvajanju prakse zasebnosti varnega pristana in jo v primeru preiskave ali pritožbe zaradi neskladnosti izročiti neodvisnemu organu, ki je pristojen za preiskavo pritožb, ali agenciji, ki je pristojna za obravnavo nepoštenih in goljufivih praks.

Kadar se organizacija odloči za zunanji pregled skladnosti z načeli, mora tak pregled pokazati, da je njena politika zasebnosti v zvezi z osebnimi podatki, prejetimi iz EU, v skladu z načeli varnega pristana, da organizacija ravna v skladu z njo ter da so posamezniki obveščeni o mehanizmih za pritožbe. Metode pregledovanja so neomejene in lahko obsegajo revizijo, naključne preglede, uporabo „vab“ ali tehnoloških orodij. Izjavo o uspešno končanem zunanjem pregledu mora podpisati bodisi izvajalec pregleda bodisi vodstveni delavec ali drug pooblaščeni

predstavnik organizacije vsaj enkrat na leto in mora biti na voljo posameznikom na njihovo zahtevo ali organom za preiskavo ali pritožbe zaradi skladnosti z načeli.

FAQ 8 – Dostop

Načelo dostopa

Posamezniki morajo imeti dostop do svojih osebnih podatkov, ki jih hrani organizacija, in možnost, da te podatke popravijo, spremenijo ali izbrišejo, kadar niso točni, razen kadar bi bili stroški in izdatki za zagotovitev dostopa nesorazmerni s tveganjem za zasebnost zadevnega posameznika ali kadar bi bile kršene zakonite pravice drugih oseb.

1. V: *Ali je pravica do dostopa absolutna?*

1.O: Ne. Po načelih varnega pristana je pravica do dostopa temeljna za varstvo zasebnosti. Posameznikom zlasti omogoča, da preverijo točnost svojih podatkov, ki jih hrani organizacija. Kljub temu pa za obveznost organizacije, da zagotovi dostop do osebnih podatkov, ki jih hrani o posamezniku, velja načelo sorazmernosti ali razumnosti in jo je v nekaterih primerih treba ublažiti. Že iz Obrazložitvenega memoranduma k Smernicam o zasebnosti, ki jih je leta 1980 izdala OECD, jasno razvidno, da obveznost organizacije glede dostopnosti podatkov ni absolutna. V memorandumu ni niti zahteve za pretirano temeljito iskanje, kakor je na primer s sodnim pozivom, niti ni zahtevan dostop do vseh različnih oblik zapisa podatkov, ki jih hrani organizacija.

Izkušnje so pravzaprav pokazale, da naj organizacije pri odzivu na posameznikovo zahtevo po dostopu najprej pogledajo težavo(-e), ki je(so) vodila(-e) do zahteve. Če je na primer zahteva po dostopu nejasna in se nanaša na več področij, lahko organizacija v pogovoru s posameznikom poskuša bolje razumeti motiv za njegovo zahtevo ter poišče ustrezne podatke. Organizacija lahko poizve, na kateri(-e) del(-e) organizacije se je posameznik obrnil in/ali na katere vrste podatkov (ali njihovo uporabo) se nanaša zahteva po dostopu. Vendar pa posameznikom ni treba upravičevati zahtev po dostopu do njihovih lastnih podatkov.

Stroški in izdatki so pomemben dejavnik, ki ga je treba upoštevati, vendar ne prevladajo pri ugotavljanju, ali je zagotovitev dostopa razumna ali ne. Na primer, če se bodo informacije uporabile za odločitve, ki bodo pomembno vplivale na posameznika (npr. zavrnitev ali dodelitev pomembnih ugodnosti, kot so zavarovanje, hipoteka in zaposlitev), potem mora organizacija v skladu z drugimi določbami teh FAQ razkriti navedene podatke, četudi je zagotovitev njihovega dostopa razmeroma težka ali draga.

Če se zahteva po dostopu nanaša na podatke, ki niso občutljivi in se ne uporabljajo za odločitve, ki bodo pomembno vplivali na posameznika (npr. neobčutljivi tržni podatki, na podlagi katerih se ugotavlja, ali se posamezniku pošlje katalog ali ne), ampak so zlahka dostopni in poceni, mora organizacija zagotoviti dostop do dejanskih podatkov, ki jih hrani o posamezniku. Zadevni podatki lahko zajemajo podatke, ki jih je dal posameznik, podatke, ki so bili zbrani med transakcijo, ali podatke, pridobljene od drugih v zvezi z zadevnim posameznikom.

V skladu s temeljno naravo pravice do dostopa bi si organizacije morale vedno dobronamerno prizadevati zagotoviti dostop. Na primer kadar je treba določeno informacijo zavarovati in jo je mogoče zlahka ločiti od drugih podatkov, na katere se nanaša zahteva po dostopu, mora organizacija prekriti zaščiteno informacijo in dati na voljo preostale podatke. Če organizacija ugotovi, da je treba v določenem posebnem primeru zavrniti dostop, mora posamezniku, ki ga zahteva, pojasniti razloge za svojo odločitev in navesti ime službe za dajanje nadaljnjih informacij.

2. V: *Kaj je zaupna tržna informacija in ali organizacija lahko zavrne dostop, da bi jo zavarovala?*

2. O: Zaupna tržna informacija (ta izraz se uporablja v Federal Rules of Civil Procedure on discovery kot confidential commercial information) je informacija, ki jo organizacija z ukrepi zavaruje pred razkritjem, kadar bi razkritje pomagalo konkurentu na trgu. Računalniški program, ki ga uporablja organizacija, kot je program modeliranja, ali podrobnosti o tem programu so lahko zaupna tržna informacija. Kadar je zaupno tržno informacijo mogoče brez težav ločiti od drugih podatkov, na katere se nanaša zahteva po dostopu,

mora organizacija na novo prekriti zaupno tržno informacijo in omogočiti dostop do podatkov, ki niso zaupni. Organizacije lahko zavrnejo ali omejijo dostop, kadar bi z njegovo odobritvijo razkrile svoje zaupne tržne informacije, kakor so opredeljene zgoraj, kot so v organizaciji narejeni tržni koncepti ali klasifikacije, ali zaupne tržne informacije drugega, kadar za tako informacijo velja pogodbena obveznost o zaupnosti v okoliščinah, v katerih bi bila taka obveznost o zaupnosti običajna ali predpisana.

3. V: *Ali lahko organizacija pri zagotavljanju dostopa razkrije posameznikom zgolj njihove osebne podatke, ki izvirajo iz njenih podatkovnih zbirk, ali mora zagotoviti dostop do podatkovne zbirke?*

3. O: Zadostuje, da organizacija posamezniku razkrije zbrane podatke, dostop posameznika do podatkovne zbirke organizacije se ne zahteva.

4. V: *Ali mora organizacija za zagotavljanje dostopa prestrukturirati svoje podatkovne zbirke?*

4. O: Dostop je treba zagotoviti samo do informacij, ki jih hrani organizacija. Načelo dostopa samo po sebi ne obvezuje organizacije, da hrani, vzdržuje, ponovno organizira ali ponovno strukturira datoteke z osebnimi podatki.

5. V: *Iz teh odgovorov je očitno, da se v nekaterih okoliščinah dostop lahko zavrne. V katerih drugih okoliščinah lahko organizacija zavrne dostop posameznika do njegovih osebnih podatkov?*

5. O: Take okoliščine so omejene in razlogi za zavrnitev morajo biti vedno posebni. Organizacija lahko zavrne dostop do podatkov, samo kadar obstaja verjetnost, da bi njihovo razkritje poseglo v zaščito pomembnih nasprotujočih si javnih interesov, kot je nacionalna varnost; obramba; ali javna varnost. Poleg tega se lahko dostop zavrne, kadar se osebni podatki obdelujejo *izključno* za namene raziskav ali statistike. Drugi razlogi za zavrnitev ali omejitev dostopa so:

a. poseg v izvrševanje ali uveljavljanje prava, vključno s preprečevanjem, preiskovanjem ali odkrivanjem kaznivih dejanj in pravico do poštenega sojenja;

b. poseg v civilnopravne postopke, vključno s preprečevanjem, preiskovanjem ali odkrivanjem pravnih zahtevkov in s pravico do pravičnega sojenja;

c. razkritje osebnih podatkov, ki zadevajo drugega posameznika/posameznike, kadar se tako povezanih podatkov ne da na novo prekriti;

d. kršitev zakonskih in drugih poklicnih privilegijev in obveznosti;

e. kršitev potrebne zaupnosti prihodnjih ali tekočih pogajanj, kot so pogajanja o prevzemu borzno notiranih družb;

f. vplivanje na preiskave o varnosti zaposlenih in pritožbene postopke;

g. vplivanje na zaupnost, ki je lahko potrebna za krajša obdobja v zvezi z načrtovanjem zamenjav zaposlenih in z reorganizacijo podjetja; ali

h. vplivanje na zaupnost, ki je lahko potrebna v zvezi s spremljanjem, inšpekcijo in nadzornimi funkcijami, povezanimi s trdnim gospodarskim ali finančnim upravljanjem; ali

i. druge okoliščine, v katerih bi bili stroški ali cena zagotavljanja dostopa nesorazmerni ali bi bile kršene zakonite pravice ali interesi drugih.

Organizacija, ki se sklicuje na izjemo, mora dokazati njeno veljavnost (kakor je to po navadi). Kakor je navedeno zgoraj, je treba posameznikom pojasniti razloge za zavrnitev ali omejitev dostopa in navesti ime službe za dajanje nadaljnjih informacij.

6. V: *Ali lahko organizacija zaračuna pristojbino za stroške zagotovitve dostopa?*

6. O: Da. Smernice OECD dopuščajo, da lahko organizacije zaračunajo pristojbino, pod pogojem, da je ta v razumnih mejah. Tako lahko organizacija zaračuna razumno pristojbino za dostop. Zaračunavanje pristojbine je lahko tudi koristno sredstvo onemogočanja ponavljajočih se in nadležnih zahtev.

Organizacije, ki se ukvarjajo s prodajo javno dostopnih informacij, lahko zaračunajo svojo običajno pristojbino za izpolnitev zahteve po dostopu. Posamezniki pa lahko zahtevajo dostop do svojih podatkov tudi pri organizaciji, ki je prvotno zbrala podatke.

Dostopa se ne sme zavrniti zaradi stroškov, če jih je posameznik pripravljen plačati.

7. V: *Ali mora organizacija zagotoviti dostop do podatkov, ki izhajajo iz javnih evidenc?*

7. O: Najprej je treba pojasniti, da so javne evidence tiste, ki jih hranijo državne agencije ali subjekti na kateri koli ravni in so odprte na vpogled širši javnosti. Dokler takšni podatki niso povezani z drugimi osebnimi podatki, ni treba uporabiti načela dostopa, razen kadar se manjši del podatkov iz evidenc, ki niso javne, uporablja za indeksiranje in organiziranje podatkov javnih evidenc. Vendar se morajo spoštovati vse določbe, ki jih za vpogled določa ustrezni predpis. Kadar pa je podatek iz javnih evidenc povezan z drugimi podatki iz evidenc, ki niso javne, (razen tistih, ki so podrobno navedene zgoraj), mora organizacija zagotoviti dostop do vseh takih podatkov, če zanje ne veljajo druge dovoljene izjeme.

8. V: *Ali se mora načelo dostopa uporabiti pri javno dostopnih osebnih podatkih?*

8. O: Kakor pri podatkih iz javnih evidenc (glej V 7), ni treba zagotoviti dostopa do podatkov, do katerih ima javnost na splošno dostop, razen če so povezani s podatki, ki javnosti niso dostopni.

9. V: *Kako se lahko organizacija zavaruje pred ponavljajočimi se in nadležnimi zahtevami?*

9. O: Organizaciji ni treba odgovoriti na take zahteve za dostop. Prav iz tega razloga lahko organizacije zaračunavajo razumno pristojbino in lahko razumno omejijo število zahtev določenega posameznika za dostop, ki jih bodo v določenem času izpolnili. Pri postavljanju takih omejitev mora organizacija upoštevati dejavnike, kot so pogostost ažuriranja podatkov, namene, za katere se podatki uporabljajo, in vrsto podatkov.

10. V: *Kako se lahko organizacija zavaruje pred goljufivimi zahtevami za dostop?*

10. O: Organizaciji ni treba zagotoviti dostopa, dokler nima v rokah dovolj podatkov, da lahko potrdi istovetnost osebe, ki zahteva dostop.

11. V: *Ali je treba na zahteve za dostop odgovoriti v roku?*

11. O: Da, organizacije bi morale odgovoriti brez pretiranega zavlačevanja in v razumnem roku. Tej zahtevi lahko različno zadostijo, kakor navaja obrazložitveni memorandum k Smernicam OECD glede zasebnosti iz leta 1980. Na primer kontrolor podatkov, ki subjektom podatkov redno daje informacije, je lahko izvzet iz obveznosti, da mora nemudoma odgovoriti na posamezne zahteve.

FAQ 9 – Človeški viri

1. V: *Ali varni pristan zajema tudi prenos osebnih podatkov iz EU v Združene države, ki so bili zbrani v okviru zaposlitvenega razmerja?*

1. O: Da, kadar podjetje v EU prenese osebne podatke o svojih zaposlenih (nekdanjih ali sedanjih), zbranih v okviru zaposlitvenega razmerja, matičnemu, odvisnemu ali neodvisnemu izvajalcu storitev v Združenih državah,

ki sodeluje v okviru varnega pristana, veljajo za prenos ugodnosti varnega pristana. V takih primerih velja za zbiranje in obdelavo podatkov pred prenosom nacionalno pravo države EU, v kateri so bili zbrani, pri prenosu pa je treba spoštovati vse pogoje in omejitve po navedenem pravu.

Načela varnega pristana se uporabljajo samo za prenos ali dostop do podatkov, ki omogočajo identifikacijo posameznika. Pri statističnem poročanju, ki temelji na zbirnih podatkih o zaposlenosti, in/ali uporabi anonimnih podatkov ali podatkov pod psevdonimi, se vprašanje varstva zasebnosti ne pojavlja.

2. V: *Kako se pri takih podatkih uporabljata načeli obvestila in možnosti izbire?*

2. O: Organizacija ZDA, ki je dobila podatke o zaposlenih iz EU v okviru varnega pristana, jih lahko razkrije tretji stranki in/ali jih uporabi za drugačne namene samo v skladu z načeloma obvestila in možnosti izbire. Na primer, kadar organizacija namerava uporabiti podatke, zbrane v zaposlitvenem razmerju, za namene, ki niso povezani z zaposlitvenim razmerjem, kot so tržne komunikacije, mora organizacija ZDA pred tem prizadetim posameznikom zagotoviti možnost izbire, razen če so že odobrili uporabo podatkov v take namene. Poleg tega se take možnosti izbire ne smejo izkoristiti za omejevanje zaposlitvenih možnosti ali za sankcioniranje takih zaposlenih.

Treba je navesti, da nekateri splošno uporabni pogoji za prenos iz nekaterih držav članic, lahko izključijo drugačno uporabo takih podatkov tudi po prenosu v državah zunaj EU, in take pogoje bo treba spoštovati.

Poleg tega bi si morali delodajalci razumno prizadevati ustreči prednostnim pravicam zaposlenih po zasebnosti. Sem sodi na primer omejitev dostopa do podatkov, anonimnost nekaterih podatkov ali uporaba šifer in psevdonimov, kadar se za namene upravljanja ne zahtevajo dejanska imena.

Organizaciji ni treba spoštovati načela obvestila in možnosti izbire v obsegu in obdobju, potrebnem za preprečitev oškodovanja zakonitih interesov organizacije pri odločitvah o napredovanju delavcev, imenovanjih in drugih podobnih zaposlitvenih odločitvah.

3. V: *Kako se uporablja načelo dostopa?*

3. O: FAQ o dostopu določajo smernice o razlogih, ki lahko v okviru človeških virov upravičijo zavrnitev ali omejitev dostopa na zahtevo posameznika. Delodajalci v Evropski uniji morajo seveda ravnati v skladu z lokalnimi predpisi in poskrbeti, da imajo zaposleni v Evropski uniji dostop do takih podatkov, kakor zahteva pravo v njihovih državah, ne glede na lokacijo obdelave in hrambe podatkov. Režim varnega pristana zahteva, da organizacija, ki v Združenih državah Amerike obdeluje take podatke, sodeluje pri zagotavljanju takšnega dostopa bodisi neposredno bodisi prek delodajalca v EU.

4. V: *Kako je z uveljavljanjem pri podatkih o zaposlenih v okviru načel varnega pristana?*

4. O: Dokler se podatki uporabljajo samo v okviru zaposlitvenega razmerja, je zaposlenemu za podatke v prvi vrsti odgovorno podjetje v EU. Iz tega sledi, da je treba, kadar se zaposleni iz EU pritožijo zaradi kršenja njihovih pravic do zaščite podatkov ter niso zadovoljni z rezultati postopkov notranjega pregleda in pritožbenih postopkov (ali drugih predvidenih pritožbenih postopkov v okviru kolektivne pogodbe), te zaposlene napotiti na državni ali nacionalni organ za zaščito podatkov ali delovnopravni organ, ki je pristojen tam, kjer zaposleni dela. Sem sodijo tudi primeri, ko se domnevna zloraba osebnih podatkov zgodi v Združenih državah in nosi odgovornost organizacija ZDA, ki je prejela podatke od delodajalca, in ne delodajalec, tako da gre za domnevno kršitev načel varnega pristana in ne nacionalnih predpisov, ki izvajajo Direktivo. To bo najbolj učinkovit način za uskladitev pogosto prekrivajočih se pravic in obveznosti, ki jih določajo lokalno delovno pravo in kolektivne pogodbe ter pravo o zaščiti podatkov.

Organizacija ZDA, ki je pristopila k varnemu pristanu in uporablja podatke o človeških virih, prenesenih iz EU v okviru zaposlitvenih razmerij, ter želi, da za ta prenos veljajo načela varnega pristana, se mora zato zavezati, da bo v takih primerih sodelovala v preiskavah pristojnih organov EU in upoštevala njihov nasvet. Organi za zaščito podatkov, ki so privolili v tako sodelovanje, bodo o tem uradno obvestili Evropsko

komisijo in Ministrstvo za trgovino. Če organizacija ZDA, ki je pristopilak varnemu pristanu, želi prenesti podatke o človeških virih iz države članice, v kateri organ za zaščito podatkov ni privolil v sodelovanje, se uporabijo določbe FAQ 5.

FAQ 10 – Pogodbe iz člena 17

V: *Ali je pri prenosu podatkov iz EU v Združene države zgolj zaradi njihove obdelave potrebna pogodba, ne glede na to, ali je izvajalec obdelave pristopil k režimu varnega pristana?*

O: Da. Od kontrolorjev podatkov v EU se vedno zahteva podpis pogodbe, kadar se podatki prenašajo zgolj zaradi obdelave, bodisi da se obdelujejo znotraj bodisi zunaj EU. Namen pogodbe je zavarovati interese kontrolorja podatkov, tj. fizične ali pravne osebe, ki določi namene in načine obdelave in je zadevnemu(-im) posamezniku(-om) v celoti odgovorna za podatke. Pogodba opredeli nameravano obdelavo podatkov in vse potrebne ukrepe za zagotovitev zaščite hranjenih podatkov.

Organizaciji ZDA, ki je pristopila k varnemu pristanu in prejema osebne podatke iz EU zgolj v obdelavo, zato ni treba uporabiti načel pri teh podatkih, ker je za podatke posamezniku odgovoren kontrolor podatkov v skladu z ustreznimi predpisi EU (ki so lahko strožji od enakovrednih načel varnega pristana).

Ker pristopnice varnega pristana zagotavljajo ustrezno zaščito podatkov, se za pogodbe, ki so jih sklenjene s pristopnicami varnega pristana samo zaradi obdelave podatkov, ne zahteva predhodno dovoljenje (ali pa bodo države članice tako dovoljenje dale avtomatično), kakršno se zahteva za pogodbe s prejemniki podatkov, ki niso pristopili k varnemu pristanu ali kako drugače ne zagotavljajo ustrezne zaščite podatkov.

FAQ 11 – Reševanje sporov in uveljavljanje

V: *Kako se izvajajo zahteve glede reševanja sporov po načelu uveljavljanja in kako se bo obravnavalo vztrajno neizpolnjevanje načel s strani organizacije?*

O: Načelo uveljavljanja navaja zahteve za uveljavljanje varnega pristana. O izpolnjevanju zahtev iz točke (b) tega načela določa FAQ o preverjanju (FAQ 7). To FAQ 11 obravnava točki (a) in (c), ki obe zahtevata neodvisne pritožbene mehanizme. Ti mehanizmi so lahko različni, morajo pa izpolnjevati zahteve načela uveljavljanja. Organizacije lahko izpolnijo te zahteve z: (1) usklajenostjo ravnanja s programi varstva zasebnosti zasebnega sektorja, ki v svojih pravilih vsebujejo načela varnega pristana in vključujejo učinkovite mehanizme uveljavljanja, kakor so opisani v načelu uveljavljanja; (2) usklajenostjo ravnanja z zakonskimi ali z drugimi predpisi predvidenimi nadzornimi organi, ki zagotavljajo obravnavo posameznikovih pritožb in reševanje sporov; ali (3) zavezo za sodelovanje z organi za zaščito podatkov v Evropski uniji ali z njihovimi pooblaščenimi predstavniki. Ta seznam je ilustrativen in ne omejuje. Zasebni sektor lahko oblikuje tudi druge mehanizme za zagotovitev uveljavljanja, če izpolnjujejo zahteve načela uveljavljanja in FAQ. Treba je paziti, da so zahteve načela uveljavljanja dodatek k zahtevam iz odstavka 3 uvoda k načelom, ki zahtevajo, da mora biti samourejanje izvedljivo po členu 5 Federal Trade Commission Act ali podobnem zakonu.

Pritožbeni mehanizmi.

Porabnike je treba spodbujati, da se s svojimi pritožbami najprej obrnejo na ustrezno organizacijo in šele nato uporabijo neodvisne pritožbene mehanizme. Neodvisnost pritožbenega mehanizma je konkretno vprašanje, na katerega se lahko odgovori na več načinov, na primer s pregledno sestavo in financiranjem ali z dokazi

o preteklem poslovanju. Kakor zahteva načelo uveljavljanja, mora biti pritožbeni mehanizem za posameznika zlahka dostopen in stroškovno ugoden. Službe za reševanje sporov morajo preučiti vse pritožbe, ki jih prejmejo od posameznikov, razen kadar so očitno neutemeljene in neresne. To ne izključuje možnosti, da organizacija, ki izvaja pritožbeni mehanizem, vzpostavi izločitvene pogoje, vendar morajo biti ti pogoji pregledni in upravičeni (na primer izključitev pritožb, ki ne sodijo na področje uporabe programa ali jih mora preučiti drug forum) ter ne smejo spodkopavati zavezanosti k preučevanju zakonitih pritožb. Pritožbeni mehanizmi morajo poleg tega zagotoviti, da posamezniki ob vložitvi pritožbe dobijo celotne in zlahka dostopne informacije o postopkih reševanja sporov. Takšna informacija mora v skladu z načeli varnega pristana vsebovati obvestilo o praksi varstva zasebnosti tega mehanizma [1]. Pritožbeni mehanizmi morajo tudi sodelovati pri oblikovanju sredstev, ki lajšajo postopek reševanja pritožb, kot je standardni obrazec za pritožbe.

Pravna sredstva in sankcije.

Vsako pravno sredstvo, ki ga zagotovi služba za reševanje sporov, bi moralo učinkovati tako, da organizacija, če je to izvedljivo, spremeni ali popravi posledice neizpolnjevanja načel in da so njeni nadaljnji postopki v skladu z načeli ali da se ustavi obdelava osebnih podatkov posameznika, ki je vložil pritožbo. Sankcije morajo biti dovolj stroge, da zagotovijo ravnanje organizacije v skladu z načeli. Razpon različno strogih sankcij bo službam za reševanje sporov omogočil ustrezen odziv na različne stopnje neizpolnjevanja načel. Sankcije morajo obsegati javno objavo ugotovitev o neskladnosti z načeli in zahtevo, da se v nekaterih okoliščinah podatki zbrišejo [2]. Druge sankcije lahko vključujejo tudi začasni odvzem in odstranitev pečata, odškodnine za posameznike za škodo, nastalo zaradi neizpolnjevanja načel, ter sodno prepoved. Kadar organizacije ne upoštevajo odločitev služb, morajo službe za reševanje sporov in samourejevalna službe iz zasebnega sektorja o tem obvestiti državen organe z ustreznimi pristojnostmi ali sodišča in Ministrstvo za trgovino (ali od njega pooblaščenega predstavnika).

Ukrepi Federal Trade Commission.

Federal Trade Commission se je zavezala, da bo prednostno pregledovala zadeve, ki ji jih prejme od organizacij s samourejevalnim sistemom varstva zasebnosti, kakršni sta BBBonline in TRUSTe, in države članice EU, v zvezi z domnevnim neizpolnjevanjem načel varnega pristana ter ugotavljala, ali je bil kršen oddelek 5 Federal Trade Commission Act, ki prepoveduje nepoštena in goljufiva dejanja in prakse v trgovini. Če Federal Trade Commission ugotovi, da obstaja(-jo) razlog(-i) za prepričanje, da je bil kršen oddelek 5, lahko zadevo reši tako, da izda upravni odlok, ki prepoveduje sporno ravnanje, ali da se pritoži na zvezno okrožno sodišče. Če tam uspe lahko doseže odločbo zveznega sodišča z enakim učinkom. Federal Trade Commission lahko uveljavi denarne kazni za kršitev upravnega odloka o prepovedi in lahko sproži civilni ali kazenski postopek za kršitev odločbe zveznega sodišča. Federal Trade Commission obvesti o vsakem takem ukrepu Ministrstvo za trgovino. Ministrstvo za trgovino spodbuja druga vladna telesa, da ga obvestijo o končnem razpletu predloženih zadev in drugih odločitev v zvezi z izpolnjevanjem načel varnega pristana.

Vztrajno neizpolnjevanje načel.

Pri vztrajnem neizpolnjevanju načel organizacija ni več upravičena do ugodnosti varnega pristana. O vztrajnem neizpolnjevanju načel govorimo, kadar organizacija, ki je Ministrstvu za trgovino (ali od njega pooblaščenemu predstavniku) poslala izjavo s potrditvijo, noče ravnati v skladu s končno ugotovitvijo samourejevalne ali vladne službe ali kadar taka služba ugotovi, da organizacija tako pogosto ravna proti načelom, da njena izjava o usklajenosti z načeli ni več verodostojna. V teh primerih mora organizacija o takih dejstvih takoj obvestiti Ministrstvo za trgovino (ali od njega pooblaščenega predstavnika). Če tega ne stori, se lahko kaznuje po False Statements Act (18 U.S.C. § 1001).

Ministrstvo (ali od njega pooblaščeni predstavnik) bo na svojem javnem seznamu organizacij, ki so samocertificirale zavezanost k načelom varnega pristana, označilo vsako uradno obvestilo o vztrajnem neizpolnjevanju načel, ne glede na to, ali ga prejme od same organizacije, samourejevalne službe ali od vladne službe, vendar šele po izteku tridesetdnevnega (30) roka, v katerem ima organizacija, ki ni ravnala v skladu z načeli, možnost odziva. Javni seznam, ki ga vodi Ministrstvo za trgovino (ali od njega pooblaščeni predstavnik), bo torej jasno pokazal, katerim organizacijam so zagotovljene in katerim organizacijam niso več zagotovljene ugodnosti varnega pristana.

---

[1] Od služb za reševanje sporov se ne zahteva skladnost z načelom uveljavljanja. Od načel lahko odstopajo tudi, kadar pri izvajanju svojih posebnih nalog naletijo na nasprotujoče si obveznosti ali na izrecno pooblastilo.

[2] Službe za reševanje sporov po svoji presoji odločijo, v katerih okoliščinah bodo uporabile te sankcije. Občutljivost zadevnih podatkov je dejavnik, ki ga je treba upoštevati pri odločitvi o zahtevi za izbris podatkov, tak dejavnik je tudi, ali je organizacija zbirala, uporabljala ali razkrivala podatke v očitnem nasprotju z načeli.

Organizacija, ki se prijavi za sodelovanje v samourejevalni službi z namenom, da izpolni pogoje za ponovno sodelovanje v varnem pristanu, mora navedeni službi predložiti vse podatke o svojem prejšnjem sodelovanju v varnem pristanu.

FAQ 12 – Možnost izbire – časovna omejitev zavrnitve

V: *Ali načelo možnosti izbire dopušča posamezniku izbiro samo na začetku razmerja ali kadar koli?*

O: Splošni namen načela izbire je zagotoviti, da se osebni podatki uporabljajo in razkrivajo v skladu s pričakovanji in odločitvami posameznika. Posameznik mora torej vedno imeti možnost „zavrnitve“ (ali izbire), da se njegovi osebni podatki uporabljajo za neposredno trženje, ob upoštevanju razumnih rokov, ki jih postavi organizacija in so potrebni za učinkovito upoštevanje zavrnitve. Organizacija lahko tudi od posameznika, ki se je odločil za zavrnitev, zahteva, da z zadostnimi podatki potrdi svojo istovetnost. V Združenih državah lahko posamezniki uresničijo to možnost prek osrednjega programa „zavrnitve“, kot je Direct Marketing Association's Mail Preference Service. Organizacije, ki sodelujejo v Direct Marketing Association's Mail Preference Service, bi morale na razpoložljivost teh storitev opozarjati tiste potrošnike, ki ne želijo prejemati trgovskih informacij. Vsekakor bi moral imeti posameznik za uresničitev te možnosti na voljo dostopen in stroškovno ugoden mehanizem.

Podobno lahko organizacija uporabi informacije za nekatere namene neposrednega trženja, kadar ni izvedljivo, da bi posamezniku zagotovila možnost zavrnitve pred uporabo podatkov, če organizacija posamezniku takoj ponudi možnost, da sočasno (na zahtevo pa kadar koli) zavrne (brez stroškov za posameznika) nadaljnje prejemanje neposrednih tržnih komunikacij in organizacija ravna v skladu s posameznikovimi željami.

FAQ 13 – Potovalne informacije

V: *Kdaj se lahko organizacijam zunaj Evropske unije prenesejo podatki o rezervacijah na potniških letalih in druge potovalne informacije, kot so podatki o pogostih letalskih ali hotelskih rezervacijah in posebni oskrbi, na primer o posebnih obrokih zaradi verskih zahtev ali fizični pomoči?*

O: Takšni podatki se lahko prenesejo v različnih okoliščinah. Po členu 26 Direktive se lahko osebni podatki prenesejo v tretjo državo, ki ne zagotavlja ustrezne ravni varstva podatkov v smislu člena 25(2), pod pogojem, (1) da je treba zagotoviti storitve, ki jih zahteva potrošnik, ali izpolniti pogoje dogovora, kakršen je dogovor o „pogostem letalskem potniku“; ali (2) da potrošnik s tem nedvoumno soglaša. Ameriške organizacije, podpisnice varnega pristana, zagotavljajo ustrezno varstvo osebnih podatkov in torej lahko prejmejo podatke iz Evropske unije, ne da bi jim bilo treba izpolnjevati navedene pogoje ali druge pogoje iz člena 26 Direktive. Ker varni pristan vključuje posebna pravila za občutljive podatke, se takšni podatki (ki jih je na primer treba zbrati v zvezi z potrošnikovo potrebo po fizični pomoči) lahko prenesejo udeleženkam varnega pristana. V vsakem primeru pa mora organizacija, ki prenaša podatke, spoštovati pravo države članice EU, v kateri deluje, ki lahko med drugim vsebuje tudi posebne pogoje glede ravnanja z občutljivimi podatki.

FAQ 14 – Farmacevtski in medicinski izdelki

1. V: *Ali se uporablja pravo držav članic ali načela varnega pristana, če so osebni podatki, zbrani v EU, preneseni v Združene države za farmacevtske raziskave in/ali druge namene?*

1. O: Pravo držav članic se uporablja za zbiranje osebnih podatkov in za vsako njihovo obdelavo, ki se izvaja pred prenosom v Združene države. Načela varnega pristana se uporabijo takoj, ko so podatki preneseni v Združene države. Podatki, ki se uporabljajo za farmacevtske raziskave in druge namene, morajo biti po potrebi brezimni.

2. V: *Osebni podatki, pridobljeni v posebnih medicinskih ali farmacevtskih raziskovalnih študijah, imajo pogosto dragoceno vlogo v prihodnjih znanstvenih raziskovanjih. Ali lahko organizacija uporabi podatke za novo znanstveno raziskovalno dejavnost, kadar se osebni podatki, zbrani v raziskovalni študiji, prenesejo v ameriško organizacijo v varnem pristanu?*

2. O: Da, če sta bila najprej zagotovljena primerno obvestilo in možnost izbire. Takšno obvestilo mora vsebovati informacijo o vseh prihodnjih posebnih uporabah podatkov, kot so občasno spremljanje, sorodne študije ali trženje. Razume se, da ni mogoče podrobno navesti vseh prihodnjih uporab podatkov, ker lahko uporaba podatkov za novo raziskavo izhaja iz novega razumevanja prvotnih podatkov, novih medicinskih odkritij in napredka ter razvoja na področju javnega zdravja in urejanja. Po potrebi mora zato obvestilo vsebovati pojasnilo, da se osebni podatki v prihodnosti morda uporabijo za medicinske in farmacevtske raziskave, ki niso predvidene. Če uporaba podatkov ni v skladu s splošnim raziskovalnim namenom(-i), za katerega so bili podatki prvotno zbrani ali za katerega je posameznik naknadno dal soglasje, je treba pridobiti novo soglasje.

3. V: *Kaj se zgodi s podatki posameznika, če se prostovoljno ali na zahtevo nosilne organizacije odloči za umik iz kliničnega poskusa?*

3. O: Udeleženci se lahko kadar koli odločijo za umik iz kliničnega poskusa ali so zaprošeni, da tako storijo. Vsi podatki, ki so zbrani pred umikom, se lahko še naprej obdelujejo skupaj z drugimi podatki, zbranimi med kliničnim poskusom, vendar samo, če je bil udeleženec jasno seznanjen s tem, ko je privolil v sodelovanje pri poskusu.

4. V: *Podjetja za farmacevtske in medicinske pripomočke smejo zagotoviti osebne podatke iz kliničnih poskusov, izvedenih v EU, nadzornim organom v Združenih državah za regulativne in nadzorne namene. Ali so podobni prenosi dovoljeni tudi drugim strankam, ki niso nadzorni organi, kot so sedežem podjetij in drugim raziskovalcem?*

4. O: Da, v skladu z načeloma obvestila in možnosti izbire.

5. V: *Zaradi zagotovitve objektivnosti pri mnogih kliničnih poskusih udeleženci, pa tudi raziskovalci, nimajo dostopa do podatkov o vrsti zdravljenja posameznega udeleženca. To bi namreč lahko ogrozilo veljavnost raziskovalne študije in rezultatov. Ali bodo udeleženci takih kliničnih poskusov (imenovanih „slepe" študije) imeli dostop do podatkov o svojem zdravljenju med poskusom?*

5. O: Ne, takšnega dostopa udeležencu ni treba zagotoviti, če je o tej omejitvi bil poučen, ko je pristopil k poskusu, in bi razkritje takih podatkov ogrozilo celovitost raziskovalnega dela. Privolitev udeleženca, da sodeluje pri poskusu pod takšnimi pogoji, je razumen razlog za opustitev pravice do dostopa. Po končanem poskusu in opravljeni analizi rezultatov bi morali udeleženci dobiti dostop do svojih podatkov, če tako zahtevajo. Zahtevati bi jih morali najprej pri zdravniku ali drugem zdravstvenem delavcu, ki je vodil zdravljenje med kliničnim poskusom, potem pa pri nosilnem podjetju.

6. V: *Ali mora podjetje za farmacevtske ali medicinske pripomočke uporabiti načela varnega pristana o obvestilu, izbiri, prenosu tretjemu in dostopu pri spremljanju varnosti in učinkovitosti svojih izdelkov, vključno s poročanjem o neugodnih dogodkih in sledenjem pacientov/subjektov, ki uporabljajo nekatera zdravila ali medicinske pripomočke (na primer srčni spodbujevalec)?*

6. O: Ne, če zavezanost k načelom posega v upoštevanje zakonskih zahtev. To velja za poročanje, na primer, zdravstvenih delavcev podjetjem za farmacevtske in medicinske pripomočke, pa tudi za poročanje podjetij za farmacevtske in medicinske pripomočke vladnim agencijam, kot je Food and Drug Administration.

7. V: *Ob nastanku raziskovalnih podatkov jih vodja raziskave nespremenljivo kodira z edinstvenimi šifrirnim ključem, tako da ni mogoče odkriti istovetnosti posameznih subjektov podatkov. Farmacevtske družbe, ki so nosilke takih raziskav, ne dobijo šifrirnega ključa. Samo raziskovalec ima edinstveni šifrirni ključ, s katerim lahko v posebnih okoliščinah prepozna subjekt raziskave (na primer, če se zahteva nadaljnja zdravniška pozornost). Ali gre pri prenosu tako šifriranih podatkov iz EU v Združene države za prenos osebnih podatkov, za katerega veljajo načela varnega pristana?*

7. O: Ne. Pri takem prenosu ne gre za prenos osebnih podatkov, za katerega veljajo načela.

FAQ 15 – Informacije iz javnih evidenc in javnosti dostopnih podatkov

V: *Ali je treba uporabiti načela o obvestilu, izbiri in prenosu tretjemu pri podatkih iz javnih evidenc in pri javnosti dostopnih podatkih?*

O: Pri podatkih iz javnih evidenc ni treba uporabiti načel obvestila, izbire ali prenosa tretjemu, če niso povezani s podatki iz evidenc, ki niso javne, in se spoštujejo vsi pogoji glede vpogleda v podatke, ki jih je določil ustrezni pristojni organ.

Prav tako na splošno ni treba uporabiti načel obvestila, izbire ali prenosa tretjemu pri javnosti dostopnih podatkih, razen če evropski pošiljatelj navede, da pri teh podatkih veljajo omejitve, ki zahtevajo, da organizacija uporabi navedena načela pri nameravani uporabi podatkov. Organizacije niso odgovorne za način, kako take podatke uporabljajo tisti, ki jih pridobijo iz objavljenih gradiv.

Če se ugotovi, da je organizacija v nasprotju z načeli namenoma objavila osebne podatke, zato da bi ona ali druge organizacije izkoristile te izjeme, organizacija ne bo več upravičena do ugodnosti varnega pristana.

PRILOGA III

Pregled uveljavljanja varnega pristana

Zvezna in državna pooblastila v zvezi z nepoštenim in goljufivim ravnanjem ter varstvom zasebnosti

Ta memorandum je splošen opis pooblastil Federal Trade Commission (FTC) po oddelku 5 Federal Trade Commission Act (15 U.S.C. §§ 41–58, kakor so bili spremenjeni), da ukrepa proti tistim, ki ne varujejo zasebnosti osebnih podatkov v skladu njihovimi zagotovili in/ali zavezo, da bodo tako ravnali. Memorandum obravnava tudi izjeme od teh pooblastil ter sposobnost drugih zveznih in državnih agencij, da ukrepajo, kadar FTC nima pooblastil ([1]).

Pooblastilo FTC v zvezi z nepoštenim in goljufivim ravnanjem

Oddelek 5 Federal Trade Commission Act določa, da so „nepoštena in goljufiva dejanja ali ravnanje v trgovini ali v zvezi s trgovino“ nezakonita. 15 U.S.C. § 45(a)(1). Oddelek 5 FTC pooblašča, da prepreči takšna dejanja in ravnanja. 15 U.S.C. § 45 (a)(2). FTC lahko zato po opravljenem uradnem zaslišanju izda odlok o prepovedi, da bi ustavila kaznivo dejanje. 15 U.S.C. § 45(b). Če je to v javnem interesu, lahko FTC na ameriškem okrožnem sodišču zahteva začasno ali trajno prepoved. 15 U.S.C. § 53(b). Kadar so nepoštena ali goljufiva dejanja ali ravnanja zelo razširjena ali če je že izdala odlok o prepovedi, lahko Komisija izda upravni odlok, s katerim prepove zadevna dejanja ali ravnanja. 15 U.S.C. § 57a.

Kdor ne ravna v skladu z odlokom FTC, se lahko kaznuje z denarno kaznijo do 11 000 USD, vsak nadaljnji dan kršitve pa se šteje za ločeno kršitev ([2]). Podobno za vsakega, ki vede krši odlok FTC, ogovarja s kaznijo 11 000 USD za vsako kršitev. 15 U.S.C. § 45(m). Kazenski pregon lahko začne Ministrstvo za pravosodje ali, če to odkloni, FTC. 15 U.S.C. § 56.

Pooblastila FTC in zasebnost

Pri izvajanju svojih pooblastil iz oddelka 5 FTC zavzema stališče, da je lažna navedba o razlogu za zbiranje podatkov o potrošniku in načinu uporabe goljufivo ravnanje ([3]). Na primer, FTC je leta 1998 vložila pritožbo proti GeoCities, ker je podatke, ki jih je zbral na svojih spletnih straneh, razkril tretji stranki za akviziterske namene, in sicer kljub drugačnim zagotovilom brez predhodnega dovoljenja ([4]). Osebje FTC utemeljuje kot nepošteno ravnanje tudi zbiranje osebnih podatkov od otrok ter prodajo in razkrivanje navedenih podatkov brez soglasja staršev ([5]).

([1]) Tu ne govorimo o vseh različnih zveznih zakonih, ki obravnavajo zasebnost v posebnih okoliščinah, ali državnih zakonih in običajnem pravu, ki bi se lahko uporabili. Zakoni na zvezni ravni, ki urejajo komercialno zbiranje in uporabo osebnih podatkov, vključujejo poleg drugih Cable Communications Policy Act (47 U.S.C. § 551), Driver's Privacy Protection Act (18 U.S.C. §2721), Electronic Communications Policy 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) in Video Privacy Protection Act (18 U.S.C. § 2710). Mnoge države imajo analogno zakonodajo za ta področja. Glej na primer Mass. Gen. Laws ch. 1678 § 16 (ki prepoveduje, da bi finančne ustanove razkrile finančne podatke svojih strank tretji stranki, razen v primeru soglasja stranke ali zaradi pravnega postopka), N.Y. Pub. Health Law § 17(ki omejuje uporabo in razkrivanje podatkov o zdravstvenem in duševnem stanju in ki pacientom podeljuje pravico do dostopa do teh podatkov).

([2]) Okrožno sodišče Združenih držav lahko v taki tožbi odredi ukrep pravnega varstva s prepovedjo in pravičnim nadomestilom kot ustrezno izvršitev odloka FTC. 15 U.S.C. § 45(1).

([3]) „Goljufivo ravnanje“ je opredeljeno kot predstavitev, opustitev ali ravnanje, ki razumne potrošnike verjetno pomembno zavede.

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

([5]) Glej pismo osebja, poslano Center for Media Education, www.ftc.gov/os/1997/9707/conmed.htm. Tudi Childern's Online Privacy Protection Act iz leta 1998 podeljuje FTC posebno zakonsko pooblastilo, da uredi zbiranje osebnih podatkov od otrok, ki ga izvajajo operaterji internetnih in računalniških storitev. Glej 15 U.S.C. §§ 6501-6506. Zakon zlasti zahteva, da operaterji računalniških storitev obvestijo in pridobijo preverljivo soglasje staršev pred zbiranjem, uporabljanjem ali razkrivanjem osebnih informacij o otrocih. Id § 6502(b). Zakon podeljuje staršem tudi pravico do dostopa do podatkov in do zavrnitve dovoljenja za nadaljnjo uporabo podatkov. Id.

V pismu generalnemu direktorju Evropske komisije Johnu Moggu je predsednik FTC Pitofsky omenil omejitve pooblastil FTC v zvezi z varstvom zasebnosti v primerih, ko ni bilo lažnih navedb (ali sploh nikakršnih navedb) o tem, kako se bodo zbrani podatki uporabljali. Pismo predsednika FTC Pitofskyja Johnu Moggu (23. september 1998). Vendar pa bodo morale družbe, ki želijo pristopiti k varnemu pristanu, dati izjavo, da bodo zbrane podatke varovale v skladu s predpisanimi smernicami. Posledično se tako dejanje, kadar družba z izjavo potrdi, da bo varovala osebne podatke, potem pa tega ne stori, šteje za lažno navedbo in „goljufivo ravnanje“ v smislu oddelka 5.

Ker pristojnosti FTC zajemajo nepoštena in goljufiva dejanja ali ravnanje „v trgovini ali v zvezi s trgovino“, FTC nima pristojnosti nad zbiranjem in uporabo osebnih podatkov za netrgovinske namene, na primer za zbiranje dobrodelnih prispevkov. Glej pismo Pitofskyja, str. 3. Vsekakor mora uporaba osebnih podatkov v kakršnem koli trgovinskem poslovanju zadostiti tej zakonski zahtevi. Tako se bo na primer delodajalec, ki bo prodal osebne podatke svojih zaposlenih za namene neposrednega trženja, znašel v zakonskem okviru oddelka 5.

Izjeme iz oddelka 5

Oddelek 5 je glede pooblastil FTC v zvezi z nepoštenimi in goljufivimi dejanji in ravnanjem uveljavil izjeme v zvezi:

— s finančnimi ustanovami, vključno z bankami, hranilnicami in posojilnicami ter kreditnimi zadrugami;

— s telekomunikacijskimi operaterji in splošnimi meddržavnimi prevozniki;

— z letalskimi prevozniki in

— z embalerji in trgovci z živino.

Glej 15 U.S.C. § 45(a)(2). Vsako izjemo in zadevno pravno pooblastilo obravnavamo spodaj.

Finančne ustanove ([1])

Prva izjema se uporablja v zvezi z „bankami, hranilnicami in posojilnicami, opisanimi v oddelku 18(f)(3) [15 U.S.C. § 57a(f)(3)]“, ter v zvezi z „zveznimi kreditnimi zadrugami, opisanimi v oddelku 18(f)(4) [15 U.S.C. § 57a(f)(4)]“ ([2]). Za te finančne ustanove namesto tega veljajo predpisi, ki so jih izdali Federal Reserve Board, Office of Thrift Supervision ([3]) ali Nationaln Credit Union Administration Board. *Glej* 15 U.S.C. § 57a(f). Tem nadzornim organom je naročeno, da izdajo potrebne predpise za preprečevanje nepoštenih in goljufivih ravnanj v teh finančnih ustanovah ([4]) in da ustanovijo ločen odsek, ki se bo ukvarjal s pritožbami potrošnikov. 15 U.S.C. § 57a(f)(1). Nazadnje, pooblastilo za uveljavljanje v bankah, hranilnicah in posojilnicah izhaja iz oddelka 8 Federal Deposit Insurance Act (12 U.S.C. § 1818), v zveznih kreditnih zadrugah pa iz oddelkov 120 in 206 Federal Credit Union Act. 15 U.S.C. §§ 57a(f)(2)-(4).

Čeprav zavarovalništvo ni posebej vključeno v seznam izjem iz oddelka 5, McCarran-Ferguson Act (15 U.S.C. § 1011 *et seq*.) na splošno prepušča ureditev zavarovalniške dejavnosti posameznim državam ([5]). Nadalje, na podlagi poglavja

([1]) 12. novembra 1999 je predsednik Clinton podpisal Gramm-Leach-Blikey Act (Pub. l. 106-102, kodificiran v 15 U.S.C. § 6801 et seq.). Zakon omejuje finančne ustanove pri razkrivanju osebnih podatkov njihovih strank. Zakon od finančnih ustanov med drugim zahteva, da vse stranke obvestijo o svoji politiki in praksi varstva zasebnosti v zvezi z dajanjem osebnih podatkov povezanim in nepovezanim ustanovam. Zakon pooblašča FTC, zvezne organe za bančništvo in druge organe, da izdajo predpise glede izvajanja varstva zasebnosti, kakor zahteva zakon. Organi so v ta namen izdali predlagane predpise.

([2]) Ta izjema se po svojih določbah ne uporablja za sektor vrednostnih papirjev. V zvezi z nepoštenimi in goljufivimi dejanji in ravnanjem sodijo zato borzni posredniki in trgovci ter drugi v dejavnosti vrednostnih papirjev v sočasne pristojnosti Securities and Exchange Commission in FTC.

([3]) Izjema v oddelku 5 se je prvotno nanašala na Federal Home Loan Bank Board, ki ga je avgusta 1989 ukinil Financial Institutions Reform, Recovery and Enforcement Act iz leta 1989. Njegove naloge so bile prenesene na Office of Thrift Supervision ter na Resolution Trust Corporation, Federal Deposit Insurance Corporation in Housing Finance Board.

([4]) Ko oddelek 5 izloči finančne ustanove iz pristojnosti FTC, hkrati tudi določi, da kadar FTC izda predpis glede nepoštenih in goljufivih dejanj in ravnanj, morajo tudi odbori za urejanje finančnega poslovanja sprejeti vzporedne predpise v 60 dneh. Glej 15 U.S.C. § 57a(f)(1).

([5]) „Za zavarovalniško dejavnost in za vse, ki se z njo ukvarjajo, veljajo zakoni številnih držav, ki zadevajo urejanje in obdavčenje te dejavnosti.“ 15 U.S.C. § 1012(a).

2(b) McCarran-Ferguson Act noben zvezni zakon ne bo razveljavil, oslabil ali nadomestil državnega predpisa, razen kadar navedeni zakon posebej zadeva zavarovalniško dejavnost. 15 U.S.C. § 1012(b). Vendar se določbe FTC Act uporabljajo za zavarovalništvo samo, kadar teh dejavnosti ne ureja državno pravo. *Id*. Opozoriti tudi velja, da McCarran-Ferguson Act daje prednost državnim zakonom samo v zvezi z zavarovalniško dejavnostjo. FTC torej ohranja preostanek pooblastila v zvezi z nepoštenimi ali goljufivimi ravnanji v zavarovalnicah, kadar se ne ukvarjajo z zavarovalniško dejavnostjo. To na primer vključuje, da zavarovalnica prodaja osebne podatke svojih zavarovancev za namene neposrednega trženja izdelkov, ki niso povezani z zavarovalništvom ([1]).

Splošni prevozniki

Druga izjema iz oddelka 5 zajema tiste splošne prevoznike, za katere „veljajo zakoni, ki urejajo trgovino". 15 U.S.C. § 45(a)(2). V tem primeru se „zakoni, ki urejajo trgovino" nanašajo na podnaslov IV naslova 49 United States Code in na Communications Act iz leta 1934 (47 U.S.C. § 151 *et seq*.) (Communications Act). *Glej* 15 U.S.C. § 44.

49 U.S.C. podnaslov IV (meddržavni promet) zajema prevoznike po železnici, po cesti, po vodi, posrednike, špediterje, izvajalce transporta po ceveh. 49 U.S.C. § 10101 *et seq*. Za vse te različne prevoznike veljajo predpisi Surface Transportation Board, neodvisne agencije Ministrstva za promet. 49 U.S.C. §§ 10501, 13501 in 15301.V vsakem primeru je prevozniku prepovedano razkriti podatke o vrsti, namembnem kraju in drugih vidikih njegovega tovora, ki bi lahko škodili odpremniku. *Glej* 49 U.S.C. §§ 11904, 14908 in 16103. Opozarjamo, da se te določbe nanašajo na podatke v zvezi z odpremnikovim tovorom in torej očitno ne zajemajo osebnih podatkov odpremnika, ki niso povezani z zadevnim tovorom.

Communications Act določa, da „trgovino po žičnih in radijskih komunikacijah med ameriškimi državami in s tujino" ureja Federal Communications Commission (FCC). *Glej* 47 U.S.C. §§ 151 in 152. Poleg splošnih telekomunikacijskih operaterjev se Communications Act uporablja tudi za podjetja, kot so ponudniki televizijskih in radijskih radiodifuznih ter kabelskih storitev, ki niso splošni operaterji. Zato ta zadnja podjetja ne izpolnjujejo pogojev za izjemo iz oddelka 5 FTC Act. FTC je torej pristojna za preiskovanje nepoštenega in goljufivega ravnanja v teh podjetjih, medtem ko je FCC sočasno pristojna za izvrševanje svojih neodvisnih pooblastil na tem področju, kakor je opisano spodaj.

Po Communications Act ima „vsak telekomunikacijski operater", vključno z operaterji krajevnih telefonskih central, dolžnost varovati zasebnost zaščitenih naročniških podatkov stranke ([2]). 47 U.S.C. § 222(a). Communications Act je bil poleg tega spremenjen s Cable Communications Policy Act iz leta 1984 (Cable Act), 47 U.S.C. § 521 *et seq*., da bi poleg tega splošnega pooblastila v zvezi z varstvom zasebnosti izrecno določil, da morajo kabelski operaterji varovati zasebnost „podatkov, ki omogočajo osebno prepoznavanje" kabelskih naročnikov. 47 U.S.C. § 551 ([3]). Cabel Act kabelskim operaterjem omejuje zbiranje osebnih podatkov in od njih zahteva, da obvestijo naročnika o vrsti zbranih podatkov in kako se bodo ti podatki uporabljali. Cabel Act podeljuje naročnikom pravico do dostopa do svojih podatkov in od kabelskih operaterjev zahteva, da te podatke uničijo, ko jih ne potrebujejo več.

Communications Act pooblašča FCC, da uveljavlja ti dve določbi o zasebnosti bodisi na lastno pobudo bodisi kot odgovor na zunanjo pritožbo ([4]). 47 U.S.C. §§ 205, 403; id § 208. Če FCC ugotovi, da je telekomunikacijski operater (vključno s kabelskim operaterjem) kršil določbe o zasebnosti iz poglavja 222 ali iz poglavja 551, se lahko odloči za

([1]) FTC je izvajala pristojnosti nad zavarovalnicami v različnih primerih. Tako je FTC uvedla postopek proti zavarovalnici zaradi goljufivega oglaševanja v državi, v kateri ni imela dovoljenja za opravljanje dejavnosti. FTC je svojo pristojnost oprla na dejstvo, da ne obstaja učinkoviti državni predpis, ker je bilo podjetje dejansko zunaj zakonskega okvira države. Glej FTC proti Travellers Health Association, 362 U.S. 293 (1960).
Kar zadeva države, jih je 17 sprejelo vzorčni Insurance Information and Privacy Protection Act, ki ga je pripravil National Association of Insurance Commissioners (NAIC). Zakon vsebuje določbe glede obvestila, uporabe in razkritja ter dostopa. Skoraj vse države so tudi sprejele vzorčni Unfair Insurance Practicies Act navedenega NAIC, ki je posebej usmerjen v nepoštene trgovske prakse v zavarovalništvu.

([2]) Izraz „zaščiteni naročniški podatki uporabnika" pomeni podatke v zvezi s količino, tehnično konfiguracijo, vrsto, namembnim naslovom in vrednostjo strankine uporabe telekomunikacijskih storitev in podatke o telefonskem računu. 47 U.S.C. § 222(f)(1). Izraz pa ne zajema podatkov o seznamu naročnikov. Id.

([3]) Zakonodaja ne opredeljuje posebej izraza „podatki, ki omogočajo individualno prepoznavanje".

([4]) Pooblastilo obsega pravico do povračila škode za kršitev zasebnosti po obeh poglavjih 222 Communications Act in, v zvezi s kabelskimi operaterji, po poglavju 551 Cabel Act, ki spreminja Communications Act. Glej tudi 47 U.S.C. § 551(f)(3) (civilna tožba na zveznem okrožnem sodišču ni izključno pravno varstvo, ki je kabelskemu naročniku na voljo poleg vseh drugih oblik zakonitega pravnega varstva).

tri osnovne ukrepe. Prvič, po zaslišanju in ugotovitvi kršitve lahko FCC odredi, da operater plača *denarno odškodnino* ([1]). 47 U.S.C. § 209. Namesto tega lahko FCC izda upravni odlok o prepovedi operaterjevega kaznivega dejanja. 47 U.S.C. § 205(a). Lahko pa FCC odredi, da kršitelj „*spoštuje (vsak) predpis in ravnanje ter ravna v skladu z njim*“, ki ga morebiti predpiše FCC. *Id*.

Fizične osebe, ki menijo, da je telekomunikacijski ali kabelski operater kršil ustrezne določbe Communications Act ali Cabel Act, se lahko bodisi pritožijo FCC ali vložijo tožbo na zveznem okrožnem sodišču. 47 U.S.C. § 207. Kadar zvezno sodišče v tožbi proti telekomunikacijskemu operaterju zaradi kršitve širšega oddelka 222 Communications Act o varstvu zaščitenih naročniških podatkov uporabnika odloči v prid tožnika, dobi tožnik povrnjeno dejansko odškodnino in odvetniške stroške. 47 U.S.C. § 206. Tožniku, ki na sodišču vloži pritožbo zaradi kršitve zasebnosti po posebnih določbah glede kabelskih operaterjev oddelka 551 Cabel Act, lahko sodišče poleg povračila dejanske odškodnine in odvetniških stroškov prisodi še dodatno odškodnino in povračilo za razumne pravdne stroške. 47 U.S.C. § 551(f).

FCC je sprejela podrobna pravila za izvajanje oddelka 222. *Glej* 47 CFR 64.2001-2009. Pravila navajajo posebne varovalke za zaščito pred nepooblaščenim dostopom do zaščitenih omrežnih naročniških podatkov. Ureditev zahteva, da telekomunikacijski operaterji:

— izdelajo in uporabljajo sisteme programske opreme, ki „pokaže“ stanje naročnikovega obvestila/privolitve ob prvem pojavu naročnikovega dokumenta na zaslonu;

— vzdržujejo elektronsko „revizijsko sled“, ki pomaga izslediti, kdo in zakaj je imel dostop do uporabnikovega računa, tudi kadar je uporabnikov dokument odprt;

— usposablja svoje osebje za pooblaščeno uporabo zaščitenih naročniških omrežnih podatkov z izvajanjem ustreznih disciplinskih postopkov;

— vzpostavijo postopek nadzornega preverjanja za zagotovitev skladnosti s predpisi pri izvajanju trženja zunaj svojega omrežja; in

— potrdijo FCC enkrat letno, da ravnajo v skladu s temi predpisi.

Letalski prevozniki

Ameriški in tuji letalski prevozniki, za katere velja Federal Aviation Act iz leta 1958, so tudi izvzeti iz oddelka 5 FTC Act. *Glej* 15 U.S.C. § 45(a)(2). Sem sodijo vsi, ki z zrakoplovi opravljajo prevoz blaga, potnikov ali pošte med ameriškimi državami in v tujino. *Glej* 49 U.S.C. § 40102. Letalski prevozniki sodijo v pristojnost Ministrstva za promet. V tem pogledu je minister za promet pristojen, da z ukrepi „prepreči nepošteno, goljufivo, grabežljivo ali protikonkurenčno ravnanje v zračnem prevozu“. 49 U.S.C. § 40101(a)(9). Minister za promet lahko, če je to v interesu javnosti, uvede preiskavo o morebitnem nepoštenem ali goljufivem ravnanju ameriškega ali tujega letalskega prevoznika ali agencije za prodajo letalskih vozovnic. 49 U.S.C. § 41712. Po zaslišanju lahko minister za promet z odlokom ustavi nezakonito ravnanje. *Id*. Kolikor nam je znano, minister za promet ni uporabil tega pooblastila pri obravnavanju varstva osebnih podatkov letalskih potniko ([2]).

Dve določbi, ki varujeta zasebnost osebnih podatkov, se pri letalskih prevoznikih uporabljata v posebnih okoliščinah. Prvič, Federal Aviation Act ščiti zasebnost kandidatov za pilote. *Glej* 49 U.S.C. § 44936(f). Zakon dopušča, da letalski prevoznik pridobi podatke o kandidatovih prejšnjih zaposlitvah, vendar daje kandidatu pravico do obvestila, da delodajalec zahteva te podatke, pravico, da soglaša s to zahtevo, da popravi netočnosti v podatkih in da so podatki na vpogled samo tistim, ki odločajo o zaposlitvi. Drugič, predpisi Ministrstva za promet zahtevajo, da so podatki s seznama potnikov, ki jih potrebuje vlada za primer letalske nesreče, „zaupne narave in se lahko razkrijejo samo Ministrstvu za zunanje zadeve, National Transport Board (na njegovo zahtevo) in Ministrstvu za promet“. 14 CFR del 243, § 243.9(c) (kakor je bilo dodano s 63 FR 8258).

([1]) Vendar pa odsotnost neposredne škode tožniku ni razlog za zavrnitev pritožbe. 47 U.S.C. § 208(a).

([2]) Izvedeli smo, da si letalski prevozniki prizadevajo obravnavati vprašanje zasebnosti. Predstavniki prevoznikov so razpravljali o predlaganih načelih varnega pristana in njihovi možni uporabi pri letalskih prevoznikih. Razprava je vključevala tudi predlog, da letalsko prevozništvo sprejme politiko zasebnosti, udeležena podjetja pa bi izrecno privolila, da zanje velja pristojnost Ministrstva za promet.

Embalerji in trgovci z živino

Packers and Stockyards Act iz leta 1921 (7 U.S.C. § 181 *et seq*.) opredeljuje kot nezakonito „vsako nepošteno, neupravičeno diskriminatorno ali goljufivo ravnanje ali sredstvo, ki ga izvaja ali uporabi kateri koli embaler v zvezi z živino, mesom, mesnimi izdelki ali z nepredelanimi živinskimi izdelki ali kateri koli trgovec s perutnino v zvezi z živo perutnino".7 U.S.C. § 192(a); *glej* tudi 7 U.S.C. § 213(a) (ki prepoveduje „vsako nepošteno, neupravičeno diskriminatorno ali goljufivo ravnanje ali sredstvo" v zvezi z živino). Minister za kmetijstvo je prvenstveno odgovoren za izvajanje teh določb, medtem ko je FTC pristojna za poslovanje v trgovini na drobno in v perutninski dejavnosti. 7 U.S.C. § 227(b)(2).

Ni jasno razvidno, ali bo ravnanje embalerjev in trgovcev z živino, ki ni v skladu z načeli varstva osebnih podatkov, Minister za kmetijstvo v skladu z navedeno politiko tolmačil kot „goljufivo" po Packers and Stockyards Act. Vendar se izjeme iz oddelka 5 uporabljajo za osebe, partnerstva in podjetja samo, „če zanje velja Packers and Stockyards Act". Če torej varstvo osebnih podatkov ni sporno v okviru Packers and Stockyards Act, potem se izjema iz oddelka 5 morda sploh ne uporabi in sodijo embalerji in trgovci z živino v tem pogledu v pristojnost FTC.

Državna pooblastila v zvezi z „nepoštenim in goljufivim ravnanjem"

Glede na analizo, ki jo je pripravilo osebje FTC, velja, da so v „vseh 50 državah ter v District of Columbia, Guamu, Portoriku in na Deviških otokih ZDA za preprečevanje nepoštene ali goljufive trgovinske prakse sprejeli zakone, ki so bolj ali manj podobni Federal Trade Commission Act (FTCA)." FTC fact sheet, ponatisnjen v „Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation", 59 Tul, L. Rev. 427 (1984). V vseh primerih je organ pregona pristojen za „vodenje preiskav prek uporabe sodnega poziva ali zahtev civilne preiskave, za pridobitev zagotovil o prostovoljnem ravnanju v skladu z zakonom, za izdajo odloka o prepovedi in za pridobitev sodne prepovedi nepoštene, nevestne ali goljufive trgovske prakse. *Id*. V 46 jurisdikcijah zakon dopušča zasebne tožbe za dejansko, dvojno, trojno odškodnino ali dodatne odškodnine, v nekaterih primerih pa povračilo sodnih in odvetniških stroškov. *Id*."

Floridski Deceptive and Unfair trade Practicies Act na primer pooblašča državnega tožilca, da vodi preiskave in vloži civilne tožbe proti „nelojalni konkurenci, nepošteni, nevestni ali goljufivi trgovinski praksi", vključno z lažnim ali zavajajočim oglaševanjem, zavajajočimi franšiznimi ali poslovnimi priložnostmi, sleparsko prodajo po telefonu in piramidskimi shemami. *Glej* tudi N.Y. General Business Law § 349 (ki prepoveduje nepoštena dejanja in goljufivo ravnanje pri opravljanju dejavnosti).

Anketa, ki jo je letos izvedel National Association of Attorneys General (NAAG), potrjuje te ugotovitve. Med 43 državami, ki so odgovorile, imajo vse zakone o „mini-FTC" ali zakone, ki zagotavljajo primerljivo zaščito. Prav tako je po tej anketi 39 držav navedlo, da bi bile pristojne za pritožbe nerezidentov. Zlasti v zvezi z varstvom osebnih podatkov potrošnikov je 37 od 41 držav, ki so odgovorile, navedlo, da bi reševale pritožbe glede podjetij v njihovi jurisdikciji, ki ne spoštujejo samo izjavljene politike varstva osebnih podatkov.

PRILOGA IV

Odškodnina za kršitev zasebnosti, zakonska pooblastila ter združitve in prevzemi po pravu Združenih držav Amerike

To je odgovor na zahtevo Evropske komisije po pojasnitvi ameriškega prava glede (a) odškodninskih zahtevkov zaradi kršitve zasebnosti, (b) „izrecnih pooblastil" v ameriškem pravu v zvezi z uporabo osebnih podatkov na način, ki ni združljiv z načeli varnega pristana, in (c) učinek združitve in prevzema na obveznosti, prevzete po načelih varnega pristana.

A. **Odškodnina za kršitev zasebnosti**

Neizpolnjevanje načel varnega pristana je lahko vzrok številnim zasebnim odškodninskim zahtevkom glede na ustrezne okoliščine. Zaradi neizpolnjevanja izjavljenih politik varstva zasebnosti so organizacije iz varnega pristana odgovorne zlasti za lažne navedbe. Zasebne odškodninske tožbe zaradi kršitve zasebnosti omogoča tudi običajno pravo. Tudi mnogi zvezni in državni zakoni zagotavljajo zasebnikom povračilo škode zaradi kršitve zasebnosti.

Pravica do povračila škode zaradi vdora v osebno zasebnost je pridobljena po ameriškem običajnem pravu.

Uporaba osebnih podatkov na način, ki ni združljiv z načeli varnega pristana, je lahko vzrok pravne odgovornosti po številnih pravnih teorijah. Na primer, organizacijo iz varnega pristana, ki ne spoštuje svoje zaveze k načelom varnega pristana, lahko zaradi lažnih navedb tožijo odgovorni za prenos podatkov in prizadeti posamezniki. Po Restatement of the Law, Second, Torts ([1]) velja naslednje:

> Kdor z goljufivimi nameni lažno navaja dejstva, mnenja, namene ali pravo, da bi drugega napeljal na dejanje ali ga odvrnil od dejanja, je drugemu odgovoren za škodo, ki jo je drugi utrpel, ko se je upravičeno zanašal na lažne navedbe.

Restatement, § 525. Lažna navedba je „goljufiva", če je dana z vednostjo ali prepričanjem, da je lažna. *Id*., § 526. Praviloma je povzročitelj goljufivega zavajanja potencialno odgovoren vsem, od katerih pričakuje ali namerava, da se bodo zanesli na lažno navedbo, za škodo, ki so jo zaradi tega morebiti utrpeli. *Id*. 531. Še več, kdor goljufivo zavaja drugega, je lahko odgovoren tretjemu, če storilec kaznivega dejanja pričakuje ali namerava, da bo drugi njegovo lažno navedbo prenesel tretjemu, ki se bo po njej ravnal. *Id*., § 533.

V smislu varnega pristana je ustrezna navedba javna izjava organizacije, da bo spoštovala načela varnega pristana. Po takšni zavezi je zavestno ravnanje proti načelom lahko razlog, da tisti, ki so se zanašali na lažno navedbo, vložijo tožbo zaradi lažne navedbe. Ker je obveznost zavezanosti k načelom izrečena javnosti na splošno, lahko tako posamezniki, ki so subjekti podatkov, pa tudi odgovorni za podatke v Evropi, ki prenese osebne podatke organizaciji v Združenih državah, tožijo ameriško organizacijo zaradi lažnih navedb ([2]). Še več, ameriška organizacija jim je odškodninsko odgovorna zaradi „neprekinjenega zavajanja" tako dolgo, dokler se v svojo škodo zanašajo na njihovo lažno navedbo. Restatement, § 535.

([1]) Druga formulacija zakona – Odškodninska odgovornost; Ameriški pravni inštitut (1997).

([2]) Tak je na primer primer, ko so posamezniki dali svoje soglasje kontrolorju podatkov, da lahko prenese podatke v ZDA, ker so se zanesli na zavezo ameriške organizacije k spoštovanju načel varnega pristana.

Kdor se je zanesel na goljufivo lažno navedbo, ima pravico do povračila škode. V skladu z Restatement.

Prejemnik goljufive lažne navedbe ima pravico s tožbo zaradi prevare od storilca zahtevati povračilo za premoženjsko škodo, katere pravna podlaga je lažna navedba.

Restatement, § 549. Priznana škoda vključuje dejansko izgubo denarja in izgubljene „ugodnosti kupčije“ v trgovinskem poslovanju. *Id.*: *glej*, na primer Boling proti Tennessee State Bank, 890 S.W.2d 32 (1994) (banka je posojilojemalcem odškodninsko odgovorna za 14 825 USD nadomestila za škodo, ki jo je povzročilo razkritje osebnih podatkov in poslovnih načrtov posojilojemalcev predsedniku banke, pri katerem je bilo ugotovljeno navzkrižje interesov).

Pri goljufivi lažni navedbi je potrebna dejanska vednost ali vsaj prepričanje, da je navedba lažna, vendar lahko odgovornost velja tudi za lažno navedbo iz malomarnosti. Po Restatement se vsak, ki da lažno navedbo med opravljanjem dejavnosti, poklica ali službe ali kakršne koli denarne transakcije šteje za odgovornega, „če pri pridobivanju ali sporočanju informacij ne ravna z razumno mero pazljivosti in pristojnosti“. Restatement, § 552(1). Drugače kakor pri goljufivem zavajanju je škoda zaradi zavajanja iz malomarnosti omejena na dejansko denarno izgubo. *Id.*, § 552B(1).

V nedavnem primeru je na primer Superior Court v Connecticutu odločilo, da ravnanje podjetja za dobavo električne energije, ki ni hotelo razkriti svojih zapisov plačil stranke nacionalnim kreditnim agencijam, pomeni podlago za tožbo zaradi lažne navedbe. *Glej* Brouillard proti United Illuminating Co. 1999 Comm. super. LEXIS 1754. V tem primeru so tožniku zavrnili posojilo, ker je obtoženec navedel plačila, ki niso prispela v 30 dneh po datumu izstavitve računa, kot „zamude“. Tožnik je trdil, da ga o takšni politiki niso obvestili, ko je pri obtožencu naročil dobavo električne energije. Sodišče je bilo še posebej mnenja, da „je lahko zahtevek zaradi lažne navedbe iz malomarnosti utemeljen z ravnanjem obtoženca, ki ni spregovoril, ko bi po dolžnosti moral.“ Ta primer tudi kaže, da goljufivi namen ni nujen element tožbe za lažne navedbe iz malomarnosti. Ameriška organizacija, ki iz malomarnosti ne razkrije v celoti, kako bo uporabila osebne podatke, ki jih je prejela po varnem pristanu, torej lahko velja za odgovorno zaradi lažne navedbe.

Če so bili zaradi kršitve načel varnega pristana zlorabljeni osebni podatki, lahko po običajnem pravu subjekt podatkov vloži tudi zahtevek zaradi vdora v zasebnost. Ameriško pravo že dolgo priznava tožbe v zvezi z vdorom v zasebnost. V primeru iz leta 1905 ([1]) je vrhovno sodišče v državi Georgia ugotovilo, da pravica do zasebnosti izhaja iz naravnega in običajnega prava, ko je odločalo o zasebnem državljanu, čigar fotografijo je zavarovalnica brez njegove privolitve in vednosti uporabila v svojem reklamnem oglasu. Ob navajanju zdaj znanih tem iz ameriškega prava zasebnosti je sodišče ugotovilo, da je bila uporaba fotografije „zlobna“, „lažna“ in je „tožnika osmešila pred svetom.“ ([2]) Temelji odločitve Pavesich so prevladali in z manjšimi spremembami postali osnova ameriškega prava na tem področju. Državna sodišča so dosledno podpirala tožbe s področja vdora v zasebnost in zdaj vsaj 48 držav sodno priznava kak tak primer tožbe ([3]). Poleg tega ima vsaj 12 držav ustavne določbe, ki ščitijo pravico njihovih državljanov do miru pred motečimi posegi v njihovo zasebnost ([4]) in lahko v nekaterih primerih varujejo tudi pred posegom nevladnih subjektov. *Glej* na primer Hill proti NCAA, 865 P.2d 633 (Ca. 1994); *glej* tudi *S. Ginder, Lost and Found in Cyberspace*: *Information Privacy in the age of internet*, 34 S.D.L. Rev. 1153 (1997). (Ustave nekaterih držav vsebujejo določbe o varstvu zasebnosti, ki presegajo določbe o varstvu zasebnosti v ameriški ustavi. Aljaska, Kalifornija, Florida, Havaji, Illinois, Louisiana, Montana, Južna Karolina in Washington imajo širši obseg varstva zasebnosti.)

Second Restatement of Torts je strokovno utemeljen pregled prava na tem področju. Restatement odraža splošno sodno prakso, ko pojasni, da „pravica do zasebnosti“ obsega štiri značilne primere odškodninske odgovornosti v tem okviru. *Glej* Restatement, § 652A. Prvič, tožba zaradi „motečega posega v intimno zasebnost“ se lahko uvede proti obtožencu, ki namenoma, fizično ali kako drugače, zmoti drugega v njegovi intimi ali odmaknjenosti ali poseže v

([1]) Pavesich proti New England Life Ins. Co. 50 SL 68 (Ga. 1905).

([2]) Id., na 69.

([3]) Elektronsko iskanje po podatkovni zbirki Westlaw je odkrilo 2703 evidentiranih primerov zasebnih tožb na državnih sodiščih v zvezi z „zasebnostjo“. Rezultate tega iskanja smo predhodno posredovali Komisiji.

([4]) Glej na primer Ustavo Aljaske, čl. 1, odd. 22; Arizone, čl. 2 odd. 8; Kalifornije, čl. 1, odd. 1; Floride, čl. 1, odd. 23; Havajev, čl. 1, odd. 5; Illinoisa, čl. 1, odd. 6; Louisiane, čl. 1, odd. 5; Montane, čl. 2, odd. 10; New Yorka, čl. 1, odd. 12; Pensilvanije, čl. 1, odd. 1; Južne Karoline, čl. 1, odd. 10; in Washingtona, čl. 1, odd. 7.

njegove zadeve in skrbi ([1]). Drugič, primer „prisvojitve“ je lahko utemeljen, kadar si kdo prisvoji ime ali podobnost drugega za svojo lastno rabo in korist ([2]). Tretjič, „objava zasebnih dejstev“ je kazniva, kadar je vsebina objavljenega gradiva za razumno osebo izjemno žaljiva in ni zakonita zadeva javnosti ([3]). In četrtič, tožba za „publiciteto v lažni luči“ je ustrezna, kadar obtoženec vedoma ali iz lahkomiselnosti drugega prikaže javnosti v lažni luči, ki bi bila za razumno osebo izjemno žaljiva ([4]).

V smislu načel varnega pristana lahko „moteč poseg v intimno zasebnost“ obsega nepooblaščeno zbiranje osebnih podatkov, medtem ko je nepooblaščena uporaba osebnih podatkov v trgovske namene lahko vzrok za tožbo zaradi prilastitve. Podobno je lahko razkritje osebnih podatkov, ki niso točni, vzrok za odškodninsko odgovornost zaradi „publicitete v lažni luči“, če so podatki takšni, da je zadoščeno standardu izjemne žaljivosti za razumno osebo. Nazadnje, vdor v zasebnost, ki je posledica objave ali razkritja kočljivih osebnih podatkov, je lahko vzrok za tožbo zaradi „objave zasebnih dejstev“. (*Glej* spodaj navedene ponazoritvene primere).

Kar zadeva odškodnino, ima zaradi vdora v zasebnost prizadeta stran pravico do povračila za:

(a) škodo, ki jo je njenemu interesu zasebnosti povzročil vdor;

(b) duševno trpljenje, ki ga je dokazano trpela, če je takšno trpljenje običajna posledica takega vdora; in

(c) posebno škodo, katere pravna podlaga je vdor.

Restatement, § 652H. Glede na splošno uporabnost odškodninskega prava in številnost tožb, ki obsegajo različne vidike interesa zasebnosti, je denarna odškodnina verjetno nadomestilo za tiste, ki utrpijo vdor v svojo zasebnost zaradi neizpolnjevanja načel varnega pristana.

In res so sodišča polna primerov domnevnih vdorov v zasebnost v podobnih okoliščinah. Postopek AmSouth Bancorporation *et al*., 717 So. 2d 357, na primer, je primer skupinske tožbe, ker je obtoženec domnevno „izkoristil zaupanje vlagateljev v banko, ko je drugim pokazal zaupne podatke o bančnih vlagateljih in njihovih računih“, da bi povezanemu podjetju omogočil prodajo vzajemnih skladov in drugih naložb. V takih primerih se pogosto prisodi odškodnina. Pri Vassiliades proti Garfinckel's, Brooks Bros., 492 A.2d 580 (D.C.App. 1985) je pritožbeno sodišče zavrnilo sodbo nižjega sodišča in odločilo, da uporaba fotografij tožnice „pred“ in „po“ plastični operaciji v predstavitvi v blagovnici predstavlja vdor v zasebnost na podlagi objave zasebnih dejstev. Pri Candebat proti Flanagan, 487 So.2d 207 (Miss. 1986) je obtožena zavarovalnica uporabila prometno nezgodo, v kateri se je tožnikova žena hudo poškodovala, v oglaševalski akciji. Tožnik jih je tožil zaradi vdora v zasebnost. Sodišče je odločilo, da tožnik lahko dobi odškodnino zaradi čustvenega trpljenja na podlagi prilastitve identitete. Pravdni postopki zaradi prilastitve se vodijo, četudi tožnik ni slaven. *Glej* na primer Staruski proti Continental Telephone Co., 154 Vt. 568 (1990) (obtoženec se je komercialno okoristil z uporabo imena in fotografije svojega zaposlenega v časopisnem oglasu). Pri Pulla proti Amoco Oil Co., 882 F.Supp. 836 (S.D. Iowa 1995) je delodajalec vdrl v intimno zasebnost svojega zaposlenega, tožnika, ko je drugemu zaposlenemu naročil preiskavo izpiskov s tožnikovih kreditnih kartic, da bi preveril njegovo odsotnost z dela zaradi bolezni. Sodišče je podprlo odločitev porote, da prisodi 2 USD dejanske odškodnine in 500 000 USD dodatne odškodnine. Nek drug delodajalec je bil spoznan za krivega, ker je v listu podjetja objavil članek o svojem zaposlenem, ki je dobil odpoved, ker je domnevno ponaredil podatke o svoji delovni dobi. *Glej* Zinda proti Louisiana-Pacific Corp., 140 Wis.2d 277 (Wis.App. 1987). Članek je z objavo zasebnih dejstev vdrl v tožnikovo zasebnost, ker je časopis krožil po skupnosti. Nazadnje, zaradi posega v intimno zasebnost je bil zakonsko odgovoren kolidž, na katerem so opravljali krvne preiskave študentov, domnevno zaradi rdečk, v resnici pa zaradi ugotavljanja okužbe s HIV. *Glej* Doe proti High-Tech Institute, Inc. 972 P.2d 1060 (Colo.App. 1998). (Glede drugih evidentiranih tožb *glej* Restatement, § 652H, Dodatek.)

Združenim državam pogosto očitajo pretirano pravdarstvo, vendar to tudi pomeni, da se posamezniki lahko, in tudi se, zakonsko pritožijo, kadar menijo, da jim je bila storjena krivica. Številni vidiki ameriškega sodnega sistema tožniku, posamezniku ali skupini, olajšajo pot na sodišče. Število odvetnikov je razmeroma višje kakor v večini drugih držav,

([1]) Id., naslov 28, oddelek 62B.
([2]) Id., naslov 28, oddelek 652C.
([3]) Id., naslov 28, oddelek 652D.
([4]) Id., naslov 28, oddelek 652E.

zaradi česar je pravno zastopstvo zlahka dosegljivo. Odvetnik, ki zastopa tožnika v zasebni tožbi, navadno obračuna honorar v odstotku od dosežene odškodnine, kar omogoča tudi revnejšim tožnikom, da poiščejo pravno varstvo. Tako pridemo do pomembnega dejavnika – v Združenih državah navadno vsaka stranka zase krije odvetniške stroške in druge izdatke. To je v nasprotju s prevladujočim pravilom v Evropi, kjer mora tisti, ki izgubi tožbo, drugemu povrniti stroške. Ne bi se hoteli spuščati v razpravo o prednostih enega in drugega sistema, vendar ameriško pravilo verjetno manjkrat odvrne posameznike od zakonitih zahtevkov zaradi strahu, da ne bi mogli plačati stroškov obeh strank v primeru, da bi tožbo izgubili.

Posamezniki lahko tožijo za odškodnino, četudi so njihovi zahtevki razmeroma majhni. Večina, če ne vse sodne oblasti v Ameriki imajo sodišča za majhne zahtevke, ki zagotavljajo poenostavljen in cenejši postopek za pravne spore, ki so pod zakonsko določeno mejo ([1]). Tudi možnost dodatne odškodnine ponuja finančno nadomestilo posameznikom, ki morda niso utrpeli tako velike škode, da bi tožili zaradi nedopustnega poslovodenja. Nazadnje, posamezniki, ki so enako oškodovani, lahko združijo sredstva in zahtevke ter vložijo skupinsko tožbo.

Dober primer sposobnosti posameznikov, da sodno izterjajo odškodnino, je pravdni postopek, ki se vodi proti Amazon.com zaradi vdora v zasebnost. Amazon.com, veliki internetni prodajalec, je tarča skupinske tožbe, v kateri tožniki trdijo, da niso bili obveščeni in niso privolili, da bo organizacija zbirala njihove osebne podatke, ko so uporabljali računalniški program „Alexa“, ki je v lasti Amazona. V navedenem primeru se tožniki sklicujejo na kršitev Computer Fraud and Abuse Act in zlorabi zaradi nezakonitega dostopa do njihovih shranjenih sporočil ter na kršitev Electronic Communications Privacy Act zaradi nezakonitega prestrezanja njihovih elektronskih in telefonskih sporočil. Sklicujejo se tudi na vdor v zasebnost po običajnem pravu. Vse to izhaja iz pritožbe, ki jo je decembra vložil neki izvedenec za varnost zasebnosti na internetu. Tožniki zahtevajo 1 000 USD odškodnine za posameznega člana skupine ter plačilo odvetniških stroškov in dobička, ki ga je organizaciji prinesla kršitev zakonov. Glede na to, da gre morda tudi za večmilijonsko število skupinskih tožnikov, lahko skupna odškodnina znaša milijarde dolarjev. Obtožbe preiskuje tudi FTC.

Zvezna in državna zakonodaja na področju zasebnosti pogosto zagotavljata zasebne tožbe za denarno odškodnino.

Neizpolnjevanje načel varnega pristana ni vzrok le za civilno odškodninsko odgovornost po odškodninskem pravu, ampak lahko pomeni tudi kršitev kakega od več sto zveznih in državnih zakonov o zasebnosti. Mnogi od teh zakonov, ki urejajo ravnanje z osebnimi podatki na vladni ravni in v zasebnem sektorju, dopuščajo tožbo posameznika v primeru kršitve. Na primer:

Electronic Communications Privacy Act iz leta 1986. ECPA prepoveduje nepooblaščenoprestrezanje klicev po mobilnih telefonih in medračunalniških prenosih podatkov. Posledica kršitve je lahko civilna odškodninska odgovornost za najmanj 100 USD za vsak dan kršitve. Zaščita ECPA zajema tudi nepooblaščen dostop in razkritje shranjenih elektronskih komunikacij. Za kršitelje velja odškodninska odgovornost za povzročeno škodo in zaseg dobička, ki je nastal s kršitvijo.

Telecommunications Act iz leta 1996. Po oddelku 702 se smejo omrežni zaščiteni naročniški podatki (customer proprietary network information – CPNI) uporabiti izključno za zagotovitev telekomunikacijskih storitev. Naročniki storitev se lahko bodisi pritožijo Federal Communications Commission bodisi sprožijo pravni spor na zveznem okrožnem sodišču ter zahtevajo odškodnino in povračilo odvetniških stroškov.

Consumer Credit Reporting Reform Act iz leta 1996. Zakon iz leta 1996 je spremenil Fair Credit Reporting Act iz leta 1970 (FCRA), s čimer je zahteval boljšo obveščenost in pravice do dostopa za subjekte poročil o kreditni sposobnosti. Reformni zakon je odredil tudi nove omejitve za prodajalce poročil o kreditni sposobnosti potrošnika. Potrošniki lahko izterjajo odškodnino za kršitev in povračilo odvetniških stroškov.

([1]) Komisiji smo predhodno že predložili podatke o tožbah z majhnimi zahtevki.

Tudi državni zakoni ščitijo posameznikovo zasebnost v najrazličnejših okoliščinah. Področja, na katerih so države ukrepale, obsegajo bančne podatke, naročnine za kabelsko televizijo, poročila o kreditni sposobnosti, potrdila o delovni dobi, vladne evidence, genetske podatke in zdravstvene kartoteke, zavarovalniške kartoteke, šolske kartoteke, elektronske komunikacije in izposojo videokaset ([1]).

B. **Izrecna zakonska pooblastila**

Načela varnega pristana vsebujejo izjemo, ko zakoni, predpisi in sodna praksa ustvarijo „kolizijo obveznosti ali izrecna pooblastila, pod pogojem, da lahko organizacija pri izvajanju takih pooblastil dokaže, da njeno neizpolnjevanje načel sega le tako daleč, kolikor je potrebno za izpolnitev prednostnih zakonitih interesov, ki jih taka pooblastila podpirajo.“ Povsem jasno je, da kadar ameriško pravo odreja nasprotno obveznost, morajo ameriške organizacije, ne glede na to, ali so udeleženke varnega pristana ali ne, ravnati v skladu z zakonom. Kar zadeva izrecna pooblastila je sicer res, da je namen načel varnega pristana premostiti razlike med ameriškim in evropskim režimom varstva zasebnosti, dolžni pa smo upoštevati posebne pravice naših izvoljenih predstavnikov zakonodajne oblasti. Omejenost izjeme od stroge zavezanosti načelom varnega pristana je način, kako najti ravnotežje, ki bo ustreglo zakonitim interesom obeh strani.

Izjema je omejena na primere, ko obstaja izrecno pooblastilo. Kar zadeva vprašanje praga, mora torej ustrezni zakon, predpis ali sodna odločba dati pozitivno pooblastili za določeno ravnanje organizacije v varnem pristanu ([2]). Drugače povedano, izjema se ne uporablja, kadar zakon molči. Poleg tega se izjema uporabi samo, kadar je izrecno pooblastilo v koliziji z zavezanostjo k načelom varnega pristana. Celo tedaj izjema „sega le tako daleč, kolikor je potrebno za izpolnitev prednostnih zakonitih interesov, ki jih taka pooblastila podpirajo.“ Če ponazorimo, kadar zakon preprosto pooblasti organizacijo za posredovanje osebnih informacij vladnemu organu, se izjema ne bo uporabila. Nasprotno pa, kadar zakon posebej pooblasti organizacijo za posredovanje osebnih informacij vladnemu organu brez privolitve posameznika, bo to pomenilo „izrecno pooblastilo“ za ravnanje, ki je v koliziji z načeli varnega pristana. Lahko pa sta v izjemo zajeti tudi specifični izjemi v zvezi s pozitivnima zahtevama po zagotovitvi obvestila in soglasja (ker je to enakovredno posebni odobritvi, da se podatki razkrijejo brez obvestila in soglasja). Na primer, zakon, ki zdravnike pooblašča, da zdravstvene kartoteke svojih pacientov posredujejo zdravstvenim službam brez predhodnega soglasja pacientov, dopušča izjemo glede načel obvestila in izbire. To pooblastilo pa ne dopušča, da zdravnik te iste zdravstvene kartoteke posreduje organizacijam za vzdrževanje zdravja ali komercialnim farmacevtskim raziskovalnim laboratorijem, ker bi to preseglo obseg namenov iz zakonskega pooblastila in torej tudi obseg izjeme ([3]). navedeno zakonsko pooblastilo je lahko „samostojno“ pooblastilo za posebno ravnanje z osebnimi podatki, vendar, kakor kažejo primeri spodaj, gre največkrat za izjemo od obsežnejšega zakona, ki prepoveduje zbiranje, uporabo ali razkritje osebnih podatkov.

Telecommunications Act iz leta 1996

V večini primerov so pooblastila za uporabo v skladu z zahtevami Direktive in načeli ali pa bi uporabo dopustila katera od drugih dovoljenih izjem. Na primer, po oddelku 702 Telecommunications Act (kodificiran v 47 U.S.C. § 222) so telekomunikacijski operaterji dolžni ohraniti zaupnost osebnih podatkov, ki jih pridobijo med zagotavljanjem svojih storitev naročnikom. Ta določba telekomunikacijskim operaterjem posebej dovoljuje:

(1) uporabo podatkov o naročnikih za zagotovitev telekomunikacijskih storitev, vključno z objavo naročniških imenikov;

(2) zagotavljanje podatkov o naročnikih drugim na pisno zahtevo naročnika; in

(3) zagotavljanje podatkov o naročnikih v zbirni obliki.

([1]) Nedavno elektronsko iskanje po podatkovni zbirki Westlaw je razkrilo 994 evidentiranih tožb na državnih sodiščih v zvezi z odškodnino in vdorom v zasebnost.

([2]) Zgolj v pojasnilo, ustreznemu zakonskemu organu ne bo treba posebej navesti načel varnega pristana.

([3]) Podobno se zdravnik iz tega primera tudi ne bi mogel zanašati na to, da bi zakonsko pooblastilo prevladalo nad pacientovo možnostjo zavrnitve v primeru neposrednega trženja, ki jo zagotavlja FAQ 12. Obseg uporabe vsake izjeme „izrecnega pooblastila“ je nujno omejen z obsegom pooblastila po ustreznem zakonu.

Glej 47 U.S.C. § 222(c)(1)-(3). Zakon dovoljuje tudi izjemo, da telekomunikacijski operaterji uporabijo podatke o naročniku:

(1) da začnejo, opravijo, obračunajo in izterjajo plačilo svojih storitev;

(2) da se zaščitijo pred goljufivim, žaljivim ali nezakonitim vedenjem; in

(3) da zagotovijo prodajo po telefonu, napotitve in upravne storitve med klicem, ki ga je začel naročnik [1].

Id., § 222(d)(1)-(3). Nazadnje, telekomunikacijski operaterji so dolžni izdajateljem telefonskih imenikov zagotoviti seznam naročnikov, ki lahko vsebuje samo ime, naslov, telefonsko številko in zvrst dejavnosti naročnikov. *Id.*, § 222(e).

Do izjeme za „izrecno pooblastilo" lahko pride, kadar telekomunikacijski operaterji uporabijo omrežne zaščitene naročniške podatke, da bi preprečili goljufivo ali drugo nezakonito ravnanje. Ampak celo v tem primeru bi takšen postopek lahko opredelili, da je v „interesu javnosti", in bi ga torej načela dopuščala.

Predlagana pravila Ministrstva za zdravje in človeške vire (Department of Health and Human Services)

Ministrstvo za zdravje in človeške vire je predlagalo pravila glede standardov za varstvo zasebnosti zdravstvenih podatkov, ki jih je mogoče individualno prepoznati. *Glej* 64 Fed. Reg. 59.918 (2. november 1999) (ki bo kodificiran v 45 C.F.R., točke 160-164). Pravila bi izvajala zahteve glede zasebnosti iz Health Insurance Portability and Accountability Act iz leta 1996. Pub. L 104-191. Predlagana pravila bi na splošno prepovedala, da pokrite organizacijske enote (na primer sistemi splošnega zdravstvenega zavarovanja, klirinške hiše zdravstvenega varstva in ponudniki zdravstvene oskrbe, ki pošiljajo zdravstvene podatke v elektronski obliki) uporabijo ali razkrijejo zaščitene zdravstvene podatke brez posameznikovega pooblastila. *Glej* predlagani 45 C.F.R. § 164.506. Predlagano pravilo bi zahtevalo, da se zaščiteni zdravstveni podatki razkrijejo samo za dva namena: 1. za dovoljenje posameznikom, da pregledajo in prepišejo zdravstvene podatke o sebi, *glej id*. § 164.514; in 2. za izvrševanje pravil, *glej id*. § 164.522.

Predlagana pravila bi dovoljevala uporabo in razkritje zaščitenih zdravstvenih podatkov brez posebnega pooblastila posameznika v omejenih okoliščinah. Mednje sodijo na primer nadzor sistema zdravstvenega varstva, postopki kazenskega pregona in urgentni primeri. *Glej id*. v § 164.510. Predlagana pravila podrobno navajajo omejitve take uporabe in razkritja. Poleg tega bi bila dovoljena uporaba in razkritje omejena na najmanjšo potrebno količino podatkov. *Glej id*. v § 164.506.

Dovoljene oblike uporabe, ki jih predlagani predpisi posebej odobrijo, so na splošno v skladu z načeli varnega pristana ali jih dovoljuje kaka druga izjema. Na primer, kazenski pregon in sodni postopki so dovoljeni, prav tako medicinsko raziskovanje. Druge oblike uporabe, na primer nadzor sistema zdravstvenega varstva, delovanje javnega zdravstva in vladni sistemi zdravstvenih podatkov služijo interesu javnosti. Razkritje podatkov za obdelavo vplačil in premij zdravstvenega varstva je nujno za zagotovitev zdravstvenega varstva. Uporaba v urgentnih primerih za posvetovanje s svojci o zdravljenju, kadar pacientovega soglasja „ni mogoče pridobiti, ker je to neizvedljivo ali nerazumno", ali pri ugotavljanju identitete in vzroka smrti umrlega ščiti življenjske interese subjekta podatkov in drugih. Uporaba podatkov pri upravljanju aktivnih vojaških enot in drugih posebnih skupin posameznikov omogoča pravilno izvedbo vojaške naloge in podobne nujne zadeve; v vsakem primeru pa bi take oblike uporabe le malo, če sploh, vplivale na potrošnike na splošno.

Ostane samo še uporaba osebnih podatkov v ustanovah zdravstvenega varstva za izdelavo imenika pacientov. Takšna uporaba nemara res ni na ravni „življenjskega interesa", vendar imeniki koristijo pacientom, njihovim sorodnikom in

[1] Ta izjema ima zelo omejeno področje uporabe. Po njenih pogojih lahko telekomunikacijski operater uporabi omrežne zaščitene naročniške samo med klicem, ki ga je začel naročnik. Še več, FTC nas je opozorila, da telekomunikacijski operater ne sme uporabiti omrežnih zaščitenih naročniških podatkov za trženje storitev, ki presegajo okvir naročnikovega povpraševanja. Nazadnje, ker mora naročnik odobriti uporabo svojih podatkov za ta namen, to določilo pravzaprav niti ni izjema.

prijateljem. Tudi obseg te odobrene uporabe je sam po sebi omejen. Zanašanje na izjemo od načel, za katero da pravo „izrecno pooblastilo“ za uporabo v ta namen, predstavlja torej minimalno nevarnost za zasebnost pacientov.

Fair Credit Reporting Act

Evropska komisija je izrazila bojazen, da bi izjema „izrecnih pooblastil“ „dejansko oblikovala ugotovitev o primernosti“ za Fair Credit Reporting Act (FCRA). To ne drži. V odsotnosti posebne ugotovitve o primernosti za navedeni zakon bodo morale tiste ameriške organizacije, ki bi se sicer zanašale na takšno ugotovitev, obljubiti, da se bodo v vseh pogledih držale načel varnega pristana. To pomeni, da kadar zahteve FCRA presegajo raven varstva, ki je vgrajena v načela, ameriškim organizacijam ni treba drugega, kakor da spoštujejo navedeni zakon. In nasprotno, kadar zahteve FCRA zaostajajo za načeli, bodo morale navedene organizacije svoje ravnanje v zvezi s podatki z načeli uskladiti. Izjema ne bi spremenila te osnovne ocene. Po pogojih se izjema uporablja samo, kadar ustrezni zakon izrecno odobri ravnanje, ki bi bilo v neskladju z načeli varnega pristana. Obseg izjeme ni razširjen na področje, kjer zahteve FCRA preprosto ne izpolnjujejo načel varnega pristana ([1]).

Drugače povedano, nimamo namena prikazati, da izjema pomeni, da ima „izrecno pooblastilo“ vse, kar se ne zahteva. Še več, izjema se uporabi samo, kadar je to, kar je z ameriškim zakonom izrecno dovoljeno, v koliziji z zahtevami načel varnega pristana. Ustrezni zakon mora izpolnjevati obe prvini, preden je dovoljen odmik od načel.

Oddelek 604 FCRA na primer izrecno pooblašča agencije, ki poročajo o potrošniških kreditih, za izdajanje poročil o potrošniških kreditih v različnih naštetih okoliščinah. *Glej* FCRA, § 604. Če s tem oddelek 604 agencije, ki poročajo o kreditni sposobnosti, pooblašča, da ravnajo proti načelom varnega pristana, potem bi se morale navedene agencije zanesti na izjemo (razen če bi se seveda uporabila kaka druga izjema). Agencije, ki poročajo o kreditni sposobnosti, morajo spoštovati sodne odločbe in pozive velike porote, uporaba poročil o kreditni sposobnosti v vladnih organih pregona v zvezi z licencami, socialno podporo in otroškimi preživninami pa služi javnemu interesu. *Id.* § 604(a)(1), (3)(D) in (4). Posledično se agenciji, ki poroča o kreditni sposobnosti potrošnikov, ne bi bilo treba zanašati na „izrecno pooblastilo“ za te namene. Kadar ta agencija ravna v skladu s pisnimi navodili potrošnika, je njeno ravnanje popolnoma v skladu z načeli varnega pristana. *Id.*, § 604(a)(2). Podobno se lahko poročila o kreditni sposobnosti dajejo za namene zaposlitve zgolj s pisno privolitvijo potrošnika. (*id.*, §§ 604(a)(3)(B) in (b)(2)(A)(ii)), za kreditno in zavarovalniško poslovanje, ki ju ne začne potrošnik, pa samo, če potrošnik ni zavrnil akviziterske prodaje (*id.*, § 604(c)(1)(B)). FCRA tudi prepoveduje, da bi agencije, ki poročajo o kreditni sposobnosti, dajale zdravstvene informacije za namene zaposlitve brez privolitve potrošnika. *Id.*, § 604(g). Takšne oblike uporabe so v skladu z načeloma obvestila in izbire. Drugi nameni, ki jih odobri oddelek 604, obsegajo transakcije, ki vključujejo potrošnika, in bi jih torej načela dovoljevala. *Glej id.*, § 604(a)(3)(A) in (F).

Preostala uporaba, ki ima „pooblastilo“ prek oddelka 604, je povezana s sekundarnimi kreditnimi trgi. *Id.*, § 604(a)(3)(E). Uporaba poročil o potrošniških kreditih v ta namen ni v koliziji z načeli varnega pristana. FCRA od agencij, ki poročajo o kreditni sposobnosti, res ne zahteva, da potrošnike obvestijo in od njih pridobijo privolitev, kadar izdajajo poročila v ta namen. Vendar znova ponavljamo, da odsotnost zahteve ne pomeni že tudi „izrecnega pooblastila“ za drugačno ravnanje, kakor se zahteva. Podobno oddelek 608 dovoljuje, da agencije, ki poročajo o kreditni sposobnosti, dajejo nekatere osebne podatke vladnim organom. Toda to „pooblastilo“ ne upravičuje tega, da bi agencija, ki poroča o kreditni sposobnosti, prezrla svojo zavezo o ravnanju v skladu z načeli varnega pristana. To je v nasprotju z drugimi našimi primeri, kjer izjeme od pozitivnih zahtev po obvestilu in izbiri izrecno pooblastijo uporabo osebnih podatkov brez obvestila in možnostjo izbire.

Sklep

Celo iz našega omejenega pregleda teh zakonov je jasno razviden vzorec:

— „Izrecno pooblastilo“ v zakonu na splošno dovoljuje uporabo ali razkritje osebnih podatkov brez predhodne privolitve posameznika; tako je izjema omejena na načeli obvestila in izbire.

([1]) Pričujoča razprava se ne sme razumeti kot priznanje, da FCRA ne zagotavlja „ustreznega“ varstva. Vsaka ocena FCRA mora upoštevati varstvo, ki ga zakon zagotavlja v svoji celoti in se ne sme osredotočiti zgolj na izjeme, kakor delamo tukaj.

— V večini primerov so izjeme, ki jih dovoli zakon, podrobno začrtane za uporabo v posebnih okoliščinah in posebnih primerih. V vseh primerih zakon drugače prepoveduje nepooblaščeno uporabo ali razkritje osebnih podatkov, ki ne sodijo v te omejitve.

— V večini primerov pooblaščena uporaba in razkritje odražata zakonodajni značaj in služita interesu javnosti.

— V skoraj vseh primerih je pooblaščena uporaba bodisi v skladu z načeli varnega pristana bodisi sodi v eno od dovoljenih izjem.

Lahko sklepamo, da bo izjema za „izrecno pooblastilo“ že po svoji naravi precej omejena v svojem obsegu.

C. **Združitve in prevzemi**

Delovna skupina iz člena 29 je izrazila bojazen zaradi primerov, ko organizacijo iz varnega pristana prevzame ali se z njo združi podjetje, ki se ni zavezalo k spoštovanju načel varnega pristana. Vendar je delovna skupina očitno domnevala, da tako nastalo podjetje ne bo dolžno uporabiti načel varnega pristana za osebne podatke, ki jih je hranila prevzeta organizacija, kar pa ni nujno primer po ameriškem pravu. Splošno pravilo za prevzeme in združitve v Združenih državah je, da podjetje, ki kupi proste delnice drugega podjetja, praviloma prevzame obveznosti in odgovornosti kupljenega podjetja. *Glej* 15 *Fletcher Cyclopedia of the Law of Private Corporations* § 7117 (1990); *glej* tudi *Model Bus. Corp. Act* § 11.06(3) (1979) (nastala korporacija prevzame vse obveznosti vsakega posameznega pridruženega podjetja). Drugače povedano, zaveza organizacije k načelom varnega pristana bi po tej metodi bila zavezujoča za podjetje, ki bi nastalo z združitvijo ali prevzemom organizacije iz varnega pristana.

Še več, tudi če bi se združitev ali prevzem izvedla z nakupom osnovnih sredstev, bi bile obveznosti kupljenega podjetja v nekaterih okoliščinah zavezujoče za podjetje, ki kupuje. 15 *Fletcher,* § 7122. Celo kadar obveznosti ne bi preživele združitve, je dobro opozoriti, da združitve ne bi preživele niti v primeru, kadar bi bili podatki iz Evrope preneseni po pogodbi – edina izvedljiva alternativa varnemu pristanu pri prenosu podatkov v Združene države. Poleg tega novo besedilo dokumentov o varnem pristanu zahteva, da vsaka organizacija iz varnega pristana uradno obvesti Ministrstvo za trgovino o vsakem prevzemu ter da dovoli nadaljnji prenos podatkov v organizacijo naslednico samo, če organizacija naslednica pristopi k varnemu pristanu. *Glej* FAQ 6. Združene države so zdaj spremenile okvir režima varnega pristana tako, da od ameriških organizacij zahtevajo, da v takih okoliščinah uničijo podatke, ki so jih prejele v okviru varnega pristana, če se njihova obveznost zavezanosti načelom ne bo nadaljevala ali se ne bodo uveljavile druge primerne varovalke.

PRILOGA V

14. julij 2000

John Mogg
Direktor, DG XV
European Commission
Office C 107-6/72
Rue de la Loi/Wetstraat 200
B- 1049 Brussels

Spoštovani gospod Mogg,

Izvedel sem, da se v zvezi s pismom, ki sem vam ga poslal 29. marca 2000, pojavlja več vprašanj. V pojasnilo naših pooblastil na področjih, ki se jih dotikajo vprašanja, vam pošiljam to pismo, v katerem zaradi lažjega sklicevanja v prihodnosti dodajam in povzemam besedilo prejšnjega dopisovanja.

Med svojim obiskom v našem uradu in v svojih pismih ste postavili več vprašanj o pooblastilu Federal Trade Commission Združenih držav Amerike na področju zasebnosti internetnih uporabnikov. Zdi se mi koristno povzeti moje prejšnje odgovore v zvezi z dejavnostjo FCT na tem področju in navesti dodatne podatke o pristojnosti naše službe v zvezi z vprašanji iz vašega zadnjega pisma o zasebnosti potrošnikov. Natančneje sprašujete: (1) ali je FTC pristojna za prenos podatkov, povezanih z zaposlitvijo, če se ga opravi v nasprotju z načeli varnega pristana; (2) ali je FCT pristojna za nepridobitne („pečatne" programe zasebnosti; (3) ali se FTC Act enakovredno uporablja za „neinternetni" in „internetni" svet; in (4) kaj se zgodi, kadar se pristojnosti FTC prekrivajo s pristojnostmi drugih organov pregona.

Uporaba FTC Act pri varstvu zasebnosti

Kakor veste, ima FTC zadnjih pet let vodilno vlogo v prizadevanjih ameriške industrije in skupin potrošnikov, da izoblikujejo celovit odgovor na vprašanje zasebnosti potrošnikov, vključno z zbiranjem in uporabo osebnih podatkov na internetu. Z javnimi delavnicami in stalnim posvetovanjem s predstavniki industrije, potrošnikov in z našimi sodelavci na Ministrstvu za trgovino in v celotni ameriški vladi nam je uspelo opredeliti ključna vprašanja politike in izoblikovati pametne rešitve.

Zakonska pooblastila FTC na tem področju najdemo v oddelku 5 Federal trade Commission Act („FTC Act"), ki prepoveduje „nepoštena ali goljufiva dejanja ali ravnanja" v trgovini ali zvezi z njo [1]. Goljufivo ravnanje je opredeljeno kot lažna navedba, opustitev ali ravnanje, ki razumne potrošnike verjetno pomembno zavede. Ravnanje je nepošteno, če potrošnikom povzroči ali je verjetno, da bo povzročilo, bistveno škodo, ki se ji ni mogoče razumno izogniti in je ne odtehtajo kompenzacijske ugodnosti za potrošnike ali konkurenco [2].

Nekatere prakse zbiranja podatkov verjetno kršijo FTC Act. Na primer, če organizacija na spletni strani lažno zatrjuje, da ravna v skladu z navedeno politiko varstva zasebnosti ali sklopom samourejevalnih smernic, FTC Act zagotavlja zakonsko podlago za izpodbijanje take lažne navedbe kot goljufive. Pravzaprav smo to načelo vzpostavili z uspešnim izvajanjem zakona [3]. Poleg tega je FTC zavzela stališče, da lahko izjemno slabo ravnanje glede varstva zasebnosti izpodbija kot nepoštene po oddelku 5, če takšno ravnanje zadeva otroke ali uporabo zelo občutljivih podatkov, kakršni so finančni podatki [4] in zdravstvene kartoteke. FTC bo kot doslej še naprej skrbela za izvajanje zakona z dejavnim spremljanjem, preiskavami in reševanjem zadev, ki jih dobivamo od organizacij s samourejevalnim sistemom in drugih, vključno z državami članicami Evropske unije.

([1]) 15 U.S.C. § 45. Tudi Fair Credit Reporting Act se uporablja pri zbiranju podatkov in prodaji na internetu, ki ustreza zakonski opredelitvi „poročanja o potrošniških kreditih" in „agencije, ki poročajo o potrošniških kreditih".

([2]) 15 U.S.C. § 45(n).

([3]) Glej GeoCities, Docket.No C-3849 (Final Order 12. feb. 1999) (dostopno na www.ftc.gov/os/1999/9902/9823015d%26o.htm); Liberty Financial Cos, Docket No C-3891 (Final Order 12. avg. 1999) (dostopno na www.ftc.gov/opa/1999/9905/younginvestor.htm). *Glej tudi* pravilo Childern's Online Protection Act (COPPA), 16 C.F.R. Part 312 (dostopno na www.ftc.gov/opa/1999/9910/childfinal.htm). Pravilo COPPA je začelo veljati prejšnji mesec in zahteva, da operaterji spletnih strani, ki so namenjene otrokom, mlajšim od 13 let, in vsi, ki zavestno zbirajo osebne podatke od otrok, mlajših od 13 let, izvajajo standarde poštenega ravnanja s podatki, ki jih opredeljuje pravilo.

([4]) Glej FTC proti Touch Tone, Inc., civilna tožba No 99-WM-783 (D.Co) (vložena 21. aprila 1999) na www.ftc.gov/opa/1999/9904/touchtone.htm. Pismo z mnenjem Komisije, 17. julij 1997, izdano kot odgovor na peticijo Center for Media Education, objavljeno na spletu www.ftc.gov/os/1997/9707/conmed.htm.

Podpora FTC samourejanju

FTC že dolgo podpira prizadevanja te gospodarske panoge, da izoblikuje učinkovite programe samourejanja, s katerimi bi zagotovili varstvo zasebnosti potrošnikov na internetu. Toda takšna prizadevanja lahko obrodijo sadove le ob množičnem sodelovanju izvajalcev dejavnosti. Hkrati morajo samourejanje podpreti organi pregona. Iz tega razloga bo FTC prednostno obravnavala sporočene zadeve glede neizpolnjevanja smernic samourejanja, ki jih prejme od organizacij, kakršni sta BBBOnline in TRUSTe. Takšen pristop je v skladu z našim dolgoletnim sodelovanjem z National Advertising Review Board (NARB) pri Better Busines Bureau, ki pritožbe v zvezi z oglaševanjem posreduje FTC. National Advertising Division (NAD) pri NARB rešuje pritožbe v zvezi z nacionalnim oglaševanjem po postopku razsojanja. Kadar organizacija noče ravnati v skladu z odločitvijo NAD, ta zadevo pošlje FTC. Osebje FTC prednostno pregleda sporno oglaševanje, da bi ugotovilo, ali krši FTC Act, in pogosto ji uspe ustaviti sporno ravnanje ali prepričati organizacijo, da obnovi sodelovanje v postopku NARB.

Podobno bo FTC prednostno obravnavala poslane zadeve glede neizpolnjevanja načel varnega pristana, ki jih bo prejela iz držav članic EU. Tako kot pri sporočenih zadevah iz samourejevalskih organizacij bo naše osebje preučilo vse podatke, ki kažejo, ali sporno ravnanje krši oddelek 5 FTC Act. To zavezo vsebujejo tudi načela varnega pristana iz FAQ 11 o uveljavljanju.

GeoCities: Prvi primer FTC v zvezi z zasebnostjo na internetu

Prvi primer zasebnosti na internetu, ki ga je reševala FTC, GeoCities, je temeljil na pooblastilu FTC iz oddelka 5 ([1]). V tem primeru je FTC trdila, da je GeoCities odraslim in otrokom lažno navajal, kako bo uporabljal njihove osebne podatke. V svoji pritožbi je FTC trdila, da je GeoCities navedel, da bo določene osebno določljive podatke, ki jih je zbral na svoji spletni strani, uporabljal zgolj za notranje namene in za to, da bo potrošnikom zagotovil posebne oglaševalske ponudbe, izdelke in storitve, za katere prosijo, ter da določenih dodatnih „neobveznih“ podatkov ne bo prenesel drugim brez njihove privolitve. V resnici je te podatke razkril tretjim strankam, ki so jih uporabile za akvizitersko prodajo članom, ki je presegala okvire tistega, v kar je član privolil. Pritožba je GeoCities tudi obtoževala, da je goljufivo ravnal v zvezi z zbiranjem podatkov od otrok. Po besedilu pritožbe je GeoCities navedel, da sam upravlja otroški del svoje spletne strani in da podatke, ki jih zbere tam, hrani GeoCities. V resnici so ta del spletne strani vodile tretje stranke, ki so zbirale in hranile podatke.

Poravnava je GeoCities prepovedala dajanje lažnih navedb o namenu zbiranja in uporabe osebno določljivih podatkov od potrošnikov in o njih, vključno z otroki. Odločba zahteva, da organizacija postavi na svojo spletno stran jasno in razločno vidno „obvestilo o varstvu zasebnosti“, ki bo potrošnikom povedalo, kateri podatki se zbirajo in v kakšne namene, komu se bodo razkrili, kakšen je dostop do teh podatkov in kako jih potrošniki lahko odstranijo. Za zagotovitev starševskega nadzora je poravnava tudi zahtevala, da mora GeoCities pridobiti soglasje staršev pred zbiranjem osebno določljivih podatkov od otrok, starih manj kakor 12 let. Po tej odločbi mora GeoCities uradno obvestiti svoje člane in jim ponuditi priložnost, da uničijo svoje podatke v podatkovnih zbirkah GeoCities in vseh tretjih strank. Poravnava posebej zahteva, da GeoCities uradno obvesti starše otrok, starih manj kakor 12 let, ter da zbriše njihove podatke, razen če ne dobi pozitivnega soglasja staršev, da se podatki lahko obdržijo in uporabljajo. Nazadnje, od GeoCities se tudi zahteva, da stopi v stik s tretjimi strankami, ki jim je pred tem razkril podatke, ter od navedenih strani zahteva, da prav tako uničijo podatke ([2]).

ReverseAuction.com

Nedavno je FTC vložila tožbo zaradi domnevne kršitve zasebnosti proti neki drugi internetni organizaciji. Januarja 2000 je FTC odobrila pritožbo in sporazumno poravnavo proti ReverseAuction.com, avkcijski spletni strani, ki je domnevno pridobivala osebno določljive podatke s konkurenčne spletne strani (eBay.com) in tem porabnikom pošiljala goljufiva, nezahtevana sporočila po elektronski pošti, da bi z njimi sklenila posel ([3]). V svoji pritožbi smo

([1]) GeoCities, Docket No C-3849 (Final order 12. feb. 1999) (dostopno na www.ftc.gov/os/1999/9902/9823015d%26ohtm).

([2]) FTC je naknadno dosegla poravnavo še v enem primeru v zvezi z zbiranjem osebnih podatkov od otrok po internetu. Liberty Financial Companies, Inc. je upravljala spletno stran Young Investor, ki je bila namenjena otrokom in najstnikom ter vprašanjem denarja in naložb. FTC je trdila, da je na strani lažno predstavljeno, da bodo podatki, zbrani od otrok z anketo, shranjeni anonimno, udeleženci pa bodo dobili elektronske novice in nagrade. V resnici so se podatki o finančnem stanju otroka in družine hranili v obliki, ki je omogočala osebno prepoznavanje, novic in nagrad pa niso poslali. Sporazumna ureditev prepoveduje takšne lažne navedbe v prihodnje in zahteva, da Liberty Financial na svoji otroški spletni strani objavi obvestilo o zasebnosti ter da pred zbiranjem osebnih podatkov od otrok pridobi preverljivo soglasje staršev. Liberty Financial Cos., Docket No C-3891 (Final Order 12. avg. 1999) (dostopno na www.ftc.gov/opa/1999/9905/younginvestor.htm).

([3]) Glej ReverseAuction.com, Inc., civilna tožba No 000032 (D.D.C.) (vložena 6. januarja 2000) (tiskovno sporočilo in izrek obtoženca na www.ftc.gov/opa/2000/01/reverse4.htm).

trdili, da je podjetje ReverseAuction kršilo oddelek 5 FTC Act, ker je pridobivalo osebno določljive podatke, med katerimi so bili tudi elektronski naslovi uporabnikov podjetja eBay in osebna uporabniška identifikacijska imena („uporabnikova izkaznica“), in razpošiljalo goljufiva sporočila po elektronski pošti.

Kakor je opisano v pritožbi, se je podjetje ReverseAuction pred pridobivanjem podatkov prijavilo kot uporabnik eBay in privolilo, da bo spoštovalo uporabniški dogovor in politiko zasebnosti eBay. Dogovor in politika varujeta zasebnost uporabnikov tako, da uporabnikom eBay prepovedujeta zbiranje in uporabljanje osebno določljivih podatkov za nepooblaščene namene, kakršno je pošiljanje nezahtevanih komercialnih sporočil po elektornski pošti. V pritožbi smo tako najprej trdili, da je po oddelku 5 podjetje ReverseAuction lažno navedlo, da bo spoštovalo uporabniški dogovor in politiko varstva zasebnosti eBay. Pritožba je prav tako trdila, da je ravnanje podjetja ReverseAuction, ki je podatke uporabilo za pošiljanje neželenih komercialnih sporočil po elektronski pošti v nasprotju z uporabniškim dogovorom in politiko zasebnosti, nepoštena trgovska praksa po oddelku 5.

Drugič, pritožba je trdila, da so sporočila po elektronski pošti uporabnikom vsebovala goljufiv stavek, ki je vsakega od njih obveščal, da bo njihova uporabniška izkaznica „kmalu potekla“. Nazadnje je pritožba trdila, da so sporočila po elektronski pošti lažno navajala, da je podjetje eBay neposredno ali posredno posredovalo podjetju ReverseAuction osebno določljive podatke svojih uporabnikov ali kako drugače sodelovalo pri širjenju nezaprošenih sporočil.

Poravnava, ki jo je dosegla FTC, v prihodnje podjetju ReverseAuction prepoveduje take kršitve. Zahteva tudi, da ReverseAuction zagotovi obvestilo uporabnikom, ki so se ali se bodo prijavili pri ReverseAuction, ker so prejeli njihova sporočila. Obvestilo te uporabnike obvešča, da njihova uporabniška izkaznica pri eBay ni potekla ter da eBay ni vedel in ni odobril, da ReverseAuction širi nezahtevana sporočila. Obvestilo daje tem uporabnikom tudi možnost, da prekličejo svojo prijavo pri ReverseAuction in zahtevajo izbris svojih osebnih podatkov iz podatkovne baze ReversAuction. Poleg tega odločba zahteva, da ReverseAuction uniči ter se odpove uporabi ali razkritju osebno določljivih podatkov tistih uporabnikov eBay, ki so prejeli sporočila ReverseAuction, vendar se niso prijavili pri ReverseAuction. Nazadnje in v skladu s predhodnimi odločbami glede zasebnosti, ki jih je pridobila FTC, poravnava zahteva, da ReverseAuction na svoji spletni strani objavi svojo politiko varstva zasebnosti, in navaja izčrpne določbe glede vodenja evidenc, ki Zvezni komisiji za trgovino omogočajo spremljanje spoštovanja odločbe.

Primer ReverseAuction izkazuje zavezo FTC, da bo z ukrepi pregona podprla prizadevanje industrije po samourejanju na področju zasebnosti internetnih uporabnikov. Ta primer je pravzaprav neposredno izzval ravnanje, ki je spodkopalo politiko varstva zasebnosti in uporabniški dogovor, ki varujeta zasebnost potrošnika, in bi lahko uničilo uporabnikovo zaupanje v ukrepe, ki jih v zvezi z varstvom zasebnosti sprejmejo internetne organizacije. Ker se je v tem primeru ena organizacija nepošteno polastila osebnih podatkov, ki jih je ščitila politika zasebnosti druge organizacije, ima morda primer še večji pomen glede na bojazni, ki se pojavljajo v zvezi z zasebnostjo pri prenosu podatkov med različnimi državami.

Ne glede na uvedbo kazenskega pregona FTC proti GeoCities, Liberty Financial Cos. in ReverseAuction pa je pooblastilo FTC na nekaterih področjih zasebnosti na internetu bolj omejeno. Kakor smo navedli zgoraj, lahko FTC Act zajema samo tisto zbiranje in uporabo osebnih podatkov, ki vsebuje bodisi goljufivo bodisi nepošteno trgovsko prakso. FTC Act tako verjetno ne bo posegel v ravnanje tistih internetnih organizacij, ki zbirajo osebno določljive podatke od uporabnikov, vendar ne dajejo lažnih navedb o namenu zbiranja niti ne uporabljajo ali širijo podatkov na način, ki bi uporabnikom lahko povzročil bistveno škodo. Prav tako ni v moči FTC, da bi lahko na splošno zahtevala, da se organizacije, ki zbirajo podatke na internetu, držijo politike varstva zasebnosti ali kake določene politike zasebnosti ([1]). Vendar pa bo, kakor je navedeno zgoraj, ravnanje organizacije, ki bo v nasprotju z njeno izjavljeno politiko varstva zasebnosti, verjetno veljalo za goljufivo.

([1]) Iz tega razloga je FTC v svojem kongresnem pričevanju navedla, da bo verjetno potrebna dodatna zakonodaja, ki bo vsem ameriškim potrošniško usmerjenim internetnim komercialnim organizacijam odredila, da spoštujejo posebne poštene prakse v zvezi z informacijami. „Consumer Privacy on the World Wide Web“ pred Subcommittee on Telecommunications, Trade and Consumer Protection pri House Committee on Commerce United States House of representatives, 21. julija 1998 (pričevanje dostopno na www.ftc.gov/os/9807/privac98.htm). FTC je preložila poziv po takšni zakonodaji, ker je želela dati prizadevanjem za samourejevalni sistem priložnost, da dokažejo široko prevzemanje poštenega ravnanja s podatki na spletu. V poročilu FTC o zasebnosti na internetu za Kongres, „Privacy Online: A Report to Congress“, junij 1998 (poročilo dostopno na www.ftc.gov/reports/privacy3/toc.htm), je Komisija priporočila, naj zakonodaja zahteva, da spletne komercialne organizacije pridobijo soglasje staršev pred zbiranjem osebno določljivih podatkov od otrok, mlajših od 13 let. Glej opombo 3 zgoraj. Lansko poročilo FTC, „Self-Regularion and Privacy Online: A Federal Trade Commission Report to Congress“, julij 1999 (poročilo dostopno na www.ftc.gov/os/1999/9907/index.htm#13), je navedlo zadosten napredek na področju samourejanja in zato se je FTC odločila, da ne priporoči zakonodaje. FTC bo v prihodnjih tednih znova poročala kongresu o napredku na področju samourejanja.

Poleg tega pristojnost FTC na tem področju zajema nepoštena ali goljufiva dejanja ali ravnanje samo, če obstajajo „v trgovini ali v zvezi z njo“. Zbiranje podatkov s strani komercialnih organizacij, ki oglašujejo izdelke in storitve, vključno z zbiranjem in uporabo podatkov v komercialne namene, bi verjetno ustrezalo pogoju o „trgovini“. Po drugi strani pa lahko mnogi posamezniki in organizacije zbirajo podatke na spletu brez komercialnih namenov in torej ne sodijo v pristojnost FTC. Primer takšne omejitve so „klepetalnice“ (chat rooms), kadar jih upravljajo nekomercialne organizacije, tj. dobrodelne družbe.

Nazadnje, številne popolne ali delne izločitve iz osnovne pristojnosti nad trgovsko prakso, ki jo ima FTC, omejujejo sposobnost FTC, da zagotovi celovit odgovor na vprašanje zasebnosti na internetu. Sem sodijo izjeme za mnoge informacijsko intenzivne potrošniške dejavnosti, kot so banke, zavarovalnice in letalski prevozniki. Kakor že veste, so ti gospodarski subjekti v pristojnosti drugih zveznih ali državnih organov, denimo zveznih organov za bančništvo in Ministrstva za promet.

V primerih pristojnosti FTC, FTC sprejema in, kolikor dovoljujejo sredstva, ukrepa v zvezi s pritožbami potrošnikov, ki jih prejme po pošti ali po telefonu v svoj Consumer response center (CRC) in v zadnjem času na svojo spletno stran ([1]). CRC sprejema pritožbe vseh potrošnikov, tudi tistih s krajem bivanja v državah članicah Evropske unije. FTC Act pooblašča FTC, da zagotovi pravno varstvo pred prihodnjimi kršitvami FTC Act s sodno prepovedjo ter odškodnino za prizadete potrošnike. Vendar bi najprej preverili, ali gre pri zadevni organizaciji za nepravilno ravnanje, ker ne rešujemo posameznih sporov potrošnikov. V preteklosti je FTC zagotovila odškodnino državljanom Združenih držav Amerike in drugih držav ([2]). FTC bo še naprej z uveljavljanjem svojih pooblastil v ustreznih primerih zagotovila odškodnino državljanom iz tujih držav, ki so bili oškodovani zaradi goljufivega ravnanja, ki sodi v njeno pristojnost.

Podatki o zaposlitvi

V svojem zadnjem pismu želite dodatno pojasnitev pristojnosti FTC na področju podatkov o zaposlitvi. Vaše prvo vprašanje je, ali FTC lahko ukrepa v skladu z oddelkom 5 proti podjetju, ki izjavi, da ravna po načelih varnega pristana, vendar prenaša ali uporablja podatke v zvezi zaposlitvijo na način, s katerim krši ta načela. Zagotavljamo vam, da smo skrbno pregledali zakonodajo o pooblastilih FTC, s tem povezane dokumente in ustrezno sodno prakso ter prišli do sklepa, da ima FTC enake pristojnosti na področju podatkov, povezanih z zaposlitvijo, kakor jih ima na splošno po oddelku 5 FTC Act ([3]). To pomeni, da bi lahko ukrepali v zadevi v zvezi s podatki o zaposlitvi, ob predpostavki, da bi primer izpolnjeval naše obstoječe pogoje (nepoštenost ali goljufija) za začetek pregona v zvezi z varnostjo zasebnosti.

Želeli bi tudi ovreči mnenje, da lahko FTC začne pregon v zvezi z zasebnostjo samo v primerih, ko organizacija ogoljufa posamezne potrošnike. Kakor je jasno razvidno iz nedavnih ukrepov FTC v primeru ReverseAuction ([4]), bo FTC začela pregon v zvezi z zasebnostjo v primerih prenosa podatkov med organizacijami, kadar ena organizacija domnevno ravna nezakonito nasproti drugi organizaciji in tako povzroči morebitno škodo potrošnikom in organizacijam. V takšni situaciji se po naših pričakovanjih lahko najverjetneje pojavi tudi vprašanje podatkov o zaposlitvi, ker se sicer ti podatki o Evropejcih prenašajo iz evropskih organizacij v ameriške, ki so se zavezale, da bodo spoštovale načela varnega pristana.

Želimo pa navesti okoliščino, v kateri je ukrepanje FTC omejeno. To se zgodi v primeru, ko se zadeva že rešuje v tradicionalnem delovnopravnem sporu pri National Labor Relations Board, najverjetneje v zvezi s poravnavo/arbitražo sindikalnega spora ali pritožbo zaradi nepoštenega ravnanja na delovnem mestu. To bi se na

([1]) Glej www.ftc.gov/ftc/complaint.htm za elektronski pritožbeni obrazec Zvezne komisije za trgovino.

([2]) Na primer, v nedavnem primeru o internetni piramidni shemi je FTC zagotovila odškodnino za 15 622 potrošnikov v skupnem znesku približno 5,5 milijona USD. Potrošniki so imeli bivališče v Združenih državah Amerike in v 70 tujih državah. Glej www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftorefund01.htm

([3]) Razen če je posebej izvzeto z zakonom o pooblastilih FTC, je pristojnost, ki jo ima FTC po oddelku 5 nad ravnanjem „v ali v zvezi s trgovino“, po obsegu enaka ustavni moči kongresa iz Commerce Clause, United States proti American Building Maintenance Industries, 422 U.S. 271, 277 n. 6 (1973). Pristojnost FTC torej zajema ravnanje v zvezi z zaposlovanjem v podjetjih in dejavnostih v mednarodni trgovini.

([4]) Glej „Online Auction Site Settles FTC Privacy Charges“, FTC sporočilo za javnost (6. januarja 2000), dostopno na www.ftc.gov/opa/2000/01/reverse4.htm.

primer zgodilo, če bi se delodajalec v kolektivni pogodbi zavezal glede uporabe osebnih podatkov, zaposleni ali sindikat pa bi trdila, da je delodajalec kršil navedeni dogovor. Komisija bi verjetno upoštevala razsodbo navedenega organa ([1]).

Pristojnost za „pečatne" programe

Vaše drugo vprašanje je, ali bi bila FTC pristojna za „pečatne" programe, ki upravljajo mehanizme reševanja sporov v Združenih državah in bi dali lažne navedbe o svoji vlogi pri uresničevanju načel varnega pristana ter reševanju pritožb posameznikov, čeprav tehnično gledano takšni subjekti „ne bi bili pridobitni". Pri ugotavljanju, ali smo pristojnost za subjekt, ki se predstavlja kot nepridobiten, FTC natančno preuči, ali subjekt, ki si sicer ne prizadeva za lastni dobiček, pripomore k dobičku svojih članov. FTC uspešno uveljavlja pristojnost nad takimi subjekti in ni tako dolgo tega, 24. maja 1999, ko je vrhovno sodišče Združenih držav v zadevi California Dental Association proti FTC enoglasno potrdilo pristojnost FTC nad prostovoljnim nepridobitnim združenjem krajevnih zobozdravniških društev v antitrustovski zadevi. Sodišče je odločilo:

> FTC Act si prizadeva vključiti ne le subjekt, „ki organizirano izvaja dejavnost za lastni dobiček", 15 U.S.C. § 44, ampak tudi subjekt, ki izvaja dejavnost za dobiček „svojih članov."…… Le težko bi domnevali, da je kongres tako zamejen pojem zajetih podpornih organizacij, ob priložnosti, ki bi s tem pokazala, namenil izogibanju pristojnosti tam, kjer bi jo nameni FTC Act očitno uveljavili.

Če povzamemo, pri odločanju, ali bomo uveljavili pristojnost nad določenim „nepridobitnim" subjektom, ki upravlja pečatni program, bi potrebovali konkretne podatke o obsegu gospodarske koristi, ki jo je subjekt zagotovil svojim članom, usmerjenim v dobiček. Če bi subjekt izvajal svoj pečatni program na način, ki bi njegovim članom prinesel gospodarsko korist, bi FTC verjetno uveljavila svojo pristojnost. Naj sicer navedem, da bi FTC verjetno imela pristojnost nad goljufivim pečatnim programom, ki daje lažne navedbe o svojem statusu nepridobitne organizacije.

Zasebnost v zunaj internetnega sveta

Tretjič, navajate, da se je najino predhodno dopisovanje osredotočilo na varstvo zasebnosti v internetnem svetu. Internetna zasebnost kot pomembna prvina razvoja elektronske trgovine je sicer res glavna skrb FTC, toda FTC Act sega v leto 1941 in se enakovredno uporablja v neinternetnem svetu. Tako lahko preganjamo organizacije, ki uveljavljajo nepošteno ali goljufivo trgovsko prakso v zvezi z zasebnostjo potrošnika ([2]). Pravzaprav je FTC v tožbi, ki jo je vložila lani, FTC zoper Touch Tone Information, Inc. ([3]), obtožila „informacijskega posrednika" za nelegalno pridobivanje in prodajo zasebnih finančnih podatkov potrošnikov. FTC je trdila, da je Touch Tone pridobil podatke o potrošnikih z „zavajanjem" – izraz uporabljajo zasebni preiskovalci za opis pridobivanja osebnih podatkov o drugih z dajanjem zavajajočih navedb, zlasti po telefonu. Tožba, vložena 21. aprila 1999 na zveznem sodišču v Koloradu, zahteva prepoved in ves nezakonito pridobljen dobiček.

Prekrivajoče se sodne pristojnosti

Vaše zadnje vprašanje govori o medsebojnem vplivanju pristojnosti FTC in drugih organov pregona, zlasti v primeru morebitnega prekrivanja pristojnosti. V FTC smo razvili trdno delovno sodelovanje s številnimi drugimi organi

([1]) Odločitev, ali gre za „nepošteno ravnanje na delovnem mestu" ali za kršitev kolektivne pogodbe, je strokovno vprašanje, ki je običajno prepuščeno izvedencem na sodišču za delovna razmerja, kakršna je arbitraža ali NRLB.

([2]) Kakor vam je znano iz prejšnjih razprav, daje Fair Credit Reporting Act pooblastilo FTC, da zaščiti finančno zasebnost potrošnika na področju uporabe zakona, in FTC je nedavno izdala sklep v zvezi s tem vprašanjem. Glej In the Matter of Trans Union, Docket No 9255 (1. marca 2000) (sporočilo za javnost in mnenje dostopna na www.ftc.gov/os/2000/03/index.htm#1).

([3]) Civilna tožba 99-WM-783 (D.Colo) (dostopna na www.ftc.gov/opa/1999/9904/touchtone.htm) (verjetno bo izdana odločba o sporazumni poravnavi).

pregona, vključno z zveznimi organi za bančništvo in državnimi tožilci. V primeru prekrivajočih se pristojnosti zelo pogosto uskladimo preiskave in tako čimbolj izkoristimo svoje vire. Pogosto tudi predamo zadeve v preiskavo ustreznemu zveznemu ali državnemu organu.

Upam, da vam bo ta pregled v pomoč. Sporočite mi, prosim, če boste potrebovali dodatna pojasnila.

S spoštovanjem,

Robert Pitofsky

PRILOGA VI

John Mogg
Direktor, DG XV
European Commission
Office C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Brussels

Spoštovani generalni direktor Mogg!

Pišem vam na prošnjo Ministrstva za trgovino ZDA, da pojasnim vlogo Ministrstva za promet pri varstvu zasebnosti potrošnikov v zvezi s podatki, ki jih od njih pridobijo letalski prevozniki.

Ministrstvo za promet spodbuja sistem samourejanja kot najmanj vsiljivo in najučinkovitejše sredstvo zagotavljanja zasebnosti podatkov, ki jih potrošniki dajo letalskim prevoznikom, in zato podpira vzpostavitev „varnega pristana“, ki bo letalskim prevoznikom omogočil, da ravnajo v skladu z zahtevami Direktive EU o varstvu zasebnosti pri prenosu podatkov zunaj Evropske unije. Vendar se Ministrstvo zaveda, da lahko sistem samourejanja zaživi samo, če bodo letalski prevozniki, ki se zavežejo varstvu zasebnosti po načelih režima „varnega pristana“, tudi v resnici ravnali po njih. Zato morajo sistem samourejanja podpreti organi pregona. Ministrstvo bo torej na podlagi obstoječega zakonskega pooblastila zagotovilo, da letalski prevozniki ravnajo v skladu z zavezo, ki so jo glede zasebnosti dali javnosti, in obravnavalo zadeve v zvezi z domnevnimi kršitvami, ki nam jih posredujejo samourejevalske organizacije in drugi, vključno z državami članicami Evropske unije.

Pooblastilo Ministrstva za uvedbo pregona na tem področju najdemo v 49 U.S.D. 41712, ki prevozniku prepoveduje „nepošteno ali goljufivo ravnanje ali nelojalno konkurenco“ pri prodaji zračnega prevoza, ki povzroči ali obstaja verjetnost, da povzroči, škodo potrošnikom. Oddelek 41712 je oblikovan po oddelku 5 Federal Trade Commission Act (15 U.S.C. 45). Vendar so letalski prevozniki po 15 U.S.C. 45(a)(2) izvzeti iz pristojnosti FTC iz oddelka 5.

Moj urad opravlja preiskave in pregon po 49 U.S.C. 41712. (*Glej* na primer Ministrstvo za promet, Orders 99-11-5, 9. november 1999; 99-8-23, 26. avgust 1999; 99-6-1, 1. junij 1999; 98-6-24, 22. junij 1998; 89-6-21, 19. junij 1998; 98-5-31, 22. maj 1998; in 97-12-23, 18. december 1997.) Postopke v takšnih primerih uvedemo na podlagi lastnih preiskav ter uradnih in neuradnih pritožb, ki jih prejmemo od posameznikov, potovalnih agencij, letalskih prevoznikov in organov tujih držav.

Rad bi opozoril, da kršitev zasebnosti podatkov, ki jih letalski prevoznik pridobi od potnikov, ni sama po sebi kršitev iz oddelka 41712. Toda kadar se letalski prevoznik uradno in javno zaveže, da bo po načelih „varnega pristana“ zagotavljal zasebnost osebnih podatkov, ki jih pridobi od potnikov, ima Ministrstvo pooblastilo, da uporabi zakonske pristojnosti iz oddelka 41712 in zagotovi ravnanje v skladu z navedenimi načeli. Ko torej potnik da podatke prevozniku, ki se je zavezal k načelom „varnega pristana“, bo vsako neizpolnjevanje teh načel verjetno povzročilo škodo potrošniku in pomenilo kršitev iz oddelka 41712. V mojem uradu bomo dali vso prednost preiskavi vsakega takega domnevnega ravnanja in pregonu vsakega primera, ki kaže na tako ravnanje. O izidu takih primerov bomo obvestili tudi Ministrstvo za trgovino.

Posledica kršitve iz oddelka 41712 je lahko izdaja odloka o prepovedi ter odredba denarne kazni za kršitev navedenega odloka. Čeprav nimamo pooblastila za dodelitev odškodnine ali denarnega nadomestila zasebnim tožnikom, pa je v naši pristojnosti, da potrdimo poravnave, s katerimi se končajo preiskave in tožbe Ministrstva in ki potrošnikom zagotovijo predmete določene vrednosti, bodisi kot olajševalno okoliščino bodisi kot nadomestilo za denarne kazni, ki se sicer plačajo. Tako smo ravnali v preteklosti, tako lahko in tudi bomo ravnali v okviru načel varnega pristana, kadar bodo okoliščine to upravičile. Ob ponavljajočih se kršitvah oddelka 41712, ki jih zagreši kateri koli ameriški letalski prevoznik, bi se pojavilo vprašanje o pripravljenosti letalskega prevoznika, da ravna v skladu z načeli, kar se lahko v izjemno hudih primerih konča z ugotovitvijo, da letalski prevoznik ni več sposoben opravljati dejavnost, in torej z izgubo pooblastila za opravljanje gospodarske dejavnosti. (*Glej* Ministrstvo za promet, Orders 93-6-34, 23.

junij 1993, in 93-6-11, 9. junij 1993. Čeprav ta postopek ni zadeval oddelka 41712, pa se je končal z odvzemom pooblastila za opravljanje dejavnosti zaradi skrajno omalovažujočega odnosa prevoznika do določb Federal Aviation Act, dvostranskega sporazuma ter odločb in predpisov Ministrstva.)

Upam, da vam bodo ta pojasnila v pomoč. Če boste imeli še kakšno vprašanje ali če boste potrebovali nadaljnja pojasnila, mi, prosim, brez oklevanja sporočite.

S spoštovanjem,

Samuel Podberesky
Assistant General Counsel for
Aviation Enforcement and Proceeding

PRILOGA VII

V zvezi s členom 1(2)(b) so naslednji vladni organi Združenih držav pooblaščeni za preiskave pritožb in zagotovitev pravnega varstva v zvezi z nepoštenim ali goljufivim ravnanjem ter odškodnine za posameznike, ne glede na njihovo državo stalnega prebivališča ali državljanstvo, kadar organizacije ne ravnajo po načelih, uresničenih v skladu z FAQ:

1. Federal Trade Commission

2. Ministrstvo za promet ZDA.

Federal trade Commission ukrepa na podlagi pooblastila iz oddelka 5 Federal trade Commission Act. Iz pristojnosti, ki jih ima Federal trade Commission po oddelku 5, so izvzete banke, hranilnice, posojilnice in kreditne zadruge; telekomunikacijski operaterji in splošni prevozniki za meddržavni prevoz, letalski prevozniki ter embalerji in trgovci z živino. Čeprav zavarovalniška dejavnost ni posebej navedena na seznamu izjem v oddelku 5, McCarran-Ferguson Act ([1]) prepušča ureditev zavarovalniške dejavnosti posameznim državam. Vendar pa se določbe FTC Act uporabljajo za zavarovalništvo tam, kjer ta dejavnost ni urejena z državnim zakonom. FTC ohranja preostalo pooblastilo v zvezi z nepoštenim in goljufivim ravnanjem zavarovalnic, kadar se te ne ukvarjajo z zavarovalniško dejavnostjo.

Ministrstvo za promet ZDA ukrepa na podlagi pooblastila iz naslova 49 oddelka 41712 United States Code. Ministrstvo za promet ZDA uvede postopke na podlagi lastnih preiskav ter uradnih in neuradnih pritožb, ki jih prejme od posameznikov, potovalnih agencij, letalskih prevoznikov in organov tujih vlad.

([1]) 15 U.S.C. § 1011 et seq.