

32000D0520

L 215/7

EIROPAS KOPIENU OFICIĀLAIS VĒSTNESIS

25.8.2000.

KOMISIJAS LĒMUMS

(2000. gada 26. jūlijs)

atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK par pienācīgu aizsardzību, kas noteikta ar privātuma “drošības zonas” principiem un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija

(paziņots ar dokumenta numuru C(2000) 2441)

(Dokuments attiecas uz EEZ)

(2000/520/EK)

EIROPAS KOPIENU KOMISIJA,

ņemot vērā Eiropas Kopienas dibināšanas līgumu,

ņemot vērā Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvu 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti ⁽¹⁾ un jo īpaši tās 25. panta 6. punktu,

tā kā:

- (1) Atbilstīgi Direktīvai 95/46/EK dalībvalstīm ir jāparedz, ka personas datu nosūtīšana trešai valstij var notikt tikai tad, ja attiecīgā trešā valsts nodrošina pienācīgu datu aizsardzības līmeni un ja pirms nosūtīšanas ievēro dalībvalsts tiesību aktus, kas atbilst citiem minētās direktīvas noteikumiem.
- (2) Komisija var atzīt, ka trešā valsts nodrošina pienācīgu aizsardzības līmeni. Šādā gadījumā personas datus no dalībvalsts drīkst nosūtīt bez papildu garantijām.
- (3) Atbilstīgi Direktīvai 95/46/EK, datu aizsardzības līmenis jānovērtē, ņemot vērā visus apstākļus vienā vai vairākās datu nosūtīšanas darbībās, un attiecībā uz dažiem nosacījumiem. Individuālo aizsardzības darbu grupa attiecībā uz personas datu apstrādi, kas ir izveidota ar minēto direktīvu ⁽²⁾, ir izdevusi norādījumus par šādu novērtējumu veikšanu ⁽³⁾.

- (4) Ņemot vērā trešo valstu dažādās pieejas datu aizsardzībai, atbilstības novērtējums jāveic un jebkurš lēmums, kurš pamatojas uz Direktīvas 95/46/EK 25. panta 6. punktu, jāizpilda tā, lai tas patvaļīgi vai nepamatoti nediskriminētu trešās valstis, kur dominē līdzīgi apstākļi, un neradītu slēptus tirdzniecības šķēršļus, ņemot vērā Kopienas pašreizējās starptautiskās saistības.

- (5) Nosūtot datus no Kopienas uz Amerikas Savienotajām Valstīm, ir jāpanāk pienācīgs datu aizsardzības līmenis, kas atzīts ar šo lēmumu, ja organizācijas ievēro privātuma “drošības zonas” principus to personas datu aizsardzībai, kurus nosūta no kādas dalībvalsts uz Amerikas Savienotajām Valstīm (še turpmāk — “principi”), un ņem vērā visbiežāk uzdotos jautājumus (“frequently asked questions”, še turpmāk — “FAQ”), kas sniedz norādījumus par Amerikas Savienoto Valstu valdības 2000. gada 21. jūlijā izdoto principu īstenošanu. Turklāt organizācijām jāpublicē sava slepenības politika un jāpakļaujas Federālās tirdzniecības komisijas [Federal Trade Commission (FTC)] jurisdikcijai saskaņā ar Federal Trade Commission Act 5. paragrāfu, kas aizliedz negodīgu vai maldinošu rīcību vai praksi, kuru veic tirdzniecībā vai kura to ietekmē, vai arī citas oficiālas iestādes jurisdikcijai, kas efektīvi nodrošina atbilstību principiem, kuri noteikti saskaņā ar FAQ.

- (6) Uz tām nozarēm un/vai datu apstrādi, kas nav nevienas no šā lēmuma VII pielikumā uzskaitīto Amerikas Savienoto Valstu valdības iestāžu jurisdikcijā, šis lēmums neattiecas.

⁽¹⁾ OV L 281, 23.11.1995., 31. lpp.

⁽²⁾ Darba grupas Interneta adrese ir: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

⁽³⁾ WP 12: “Personas datu nosūtīšana uz trešām valstīm: ES datu aizsardzības direktīvas 25. un 26. panta piemērošana”, Darba grupa pieņēmusi 1998. gada 24. jūlijā.

- (7) Lai nodrošinātu šā lēmuma pareizu piemērošanu, ir svarīgi, lai ieinteresētās personas, piemēram, datu subjekti, datu nosūtītāji un datu aizsardzības iestādes, varētu atzīt tās organizācijas, kas stingri ievēro principus un FAQ. Tālab ASV Tirdzniecības ministrijai vai tās pārstāvim jāaņem uzturēt un darīt sabiedrībai zināmu to organizāciju

sarakstu, kas pašas apliecina, ka tās stingri ievēro principus, kuri īstenoti saskaņā ar FAQ, un kas ir vismaz vienas no šā lēmuma VII pielikumā uzskaitīto valdības iestāžu jurisdikcijā.

IR PIENĒMUSI ŠO LĒMUMU.

1. pants

- (8) Pārredzamības labad un lai panāktu dalībvalstu kompetento iestāžu spēju nodrošināt indivīdu aizsardzību attiecībā uz viņu personas datu apstrādi, šajā lēmumā jānosaka izņēmuma apstākļi, kuros konkrētu datu plūsmas apturēšana ir attaisnojama, neatkarīgi no pienācīgas aizsardzības konstatācijas.
- (9) “Drošības zona”, kas ir noteikta ar principiem un FAQ, varbūt ir jāpārskata, ņemot vērā pieredzi, attīstību attiecībā uz privātas dzīves aizsardzību apstākļos, kad tehnoloģijas pastāvīgi atvieglo personas datu nosūtīšanu un apstrādi, un ņemot vērā iesaistīto izpildiestāžu ziņojumus par veikto piemērošanu.
- (10) Indivīdu aizsardzības darba grupa attiecībā uz personas datu apstrādi, kas ir izveidota ar Direktīvas 95/46/EK 29. pantu, ir sniegusi atzinumus par aizsardzības līmeni, kurš Amerikas Savienotajās Valstīs ir noteikts ar “drošības zonas” principiem, un tie ir ņemti vērā, sagatavojot šo lēmumu ⁽¹⁾.
- (11) Šajā lēmumā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi Komiteja, kura izveidota saskaņā ar Direktīvas 95/46/EK 31. pantu,

1. Direktīvas 95/46/EK 25. panta 2. punktā attiecībā uz visām darbībām, uz kurām attiecas minētā direktīva, uzskata, ka “privātuma” drošības zonas “principi” (še turpmāk — “principi”), kas izklāstīti šā lēmuma I pielikumā un kas īstenoti atbilstīgi norādījumiem, kuri sniegti ASV Tirdzniecības ministrijas 2000. gada 21. jūlijā izdotajos visbiežāk uzdotajos jautājumos (še turpmāk — “FAQ”), kas izklāstīti šā lēmuma II pielikumā, nodrošina pienācīgu to personas datu aizsardzības līmeni, ko no Kopienas nosūta Amerikas Savienoto Valstu organizācijām, ņemot vērā šādus ASV Tirdzniecības ministrijas izdotus dokumentus:

- a) III pielikumā izklāstīto pārskatu par “drošības zonas” piemērošanu;
- b) Lēmuma IV pielikumā izklāstīto memorandu par kaitējuma atlīdzināšanu par privātas dzīves aizskārumiem, un ASV likumos noteiktām skaidrām atļaujām;
- c) Lēmuma V pielikumā doto vēstuli no *Federal Trade Commission*;
- d) VI pielikumā doto vēstuli no ASV Transporta ministrijas.

2. Attiecībā uz katru datu nosūtīšanu jābūt izpildītiem šādiem nosacījumiem:

- a) organizācija, kas saņem datus, ir skaidri un publiski darījusi zināmu savu apņemšanos ievērot principus, kas īstenoti atbilstīgi FAQ; un
- b) organizācija pakļaujas Amerikas Savienoto Valstu to valdības iestāžu tiesību aktos noteiktajām pilnvarām, kas uzskaitītas šā lēmuma VII pielikumā un kas ir pilnvarotas izmeklēt sūdzības un saņemt palīdzību negodīgas vai maldinošas rīcības novēršanai, kā arī zaudējumu atlīdzību indivīdiem, neatkarīgi no viņu mītnes valsts vai valstiskās piederības, ja nav ievēroti atbilstīgi FAQ īstenotie principi.

3. Uzskata, ka organizācijas, kas pašas apliecina, ka tās stingri ievēro atbilstīgi FAQ īstenotos principus, ir izpildījušas 2. punktā noteiktos nosacījumus no dienas, kad organizācija paziņo ASV Tirdzniecības ministrijai (vai tās pārstāvim) par 2. punkta a) apakšpunktā minēto saistību publiskošanu un norāda 2. punkta b) apakšpunktā minētās valdības iestādes nosaukumu.

(1) WP 15: Atzinums 1/99 par datu aizsardzības līmeni Amerikas Savienotajās Valstīs un notiekošajām apspriedēm starp Eiropas Komisiju un Amerikas Savienotajām Valstīm.
WP 19: Atzinums 2/99 par 1999. gada 19. aprīlī ASV Tirdzniecības ministrijas izdoto “Starptautisko” drošības zonas “principu” atbilstību.
WP 21: Atzinums 4/99 par visbiežāk uzdotajiem jautājumiem, ko ASV Tirdzniecības ministrija izdos saistībā ar ierosinātajiem “drošības zonas” principiem par “Starptautisko” drošības zonas “principu” atbilstību.
WP 23: Darba dokuments par pašreizējo situāciju notiekošajās apspriedēs starp Eiropas Komisiju un Amerikas Savienotajām Valstīm par “Starptautiskajiem” drošības zonas “principiem”.
WP 27: Atzinums 7/99 par datu aizsardzības līmeni, ko nodrošina “drošības zonas” principi, kurus ASV Tirdzniecības ministrija 1999. gada 15. un 16. novembrī publicējusi kopā ar visbiežāk uzdotajiem jautājumiem (FAQ) un citiem ar tiem saistītajiem dokumentiem.
WP 31: Atzinums 3/2000 par ES un ASV dialogu par “drošības zonas” režīmu.
WP 32: Atzinums 4/2000 par aizsardzības līmeni, ko nodrošina “Privātuma” drošības zonas “principi”.

2. pants

Šis lēmums attiecas tikai uz pienācīgu aizsardzību, ko Amerikas Savienotās Valstis nodrošina saskaņā ar principiem, kas īstenoti atbilstīgi FAQ, lai izpildītu Direktīvas 95/46/EK 25. panta 1. punkta prasības, un tas neietekmē citu minētās direktīvas noteikumu piemērošanu, kuri neļauj personas datus apstrādāt dalībvalstīs, jo īpaši tās 4. pantu.

3. pants

1. Neskarot dalībvalstu kompetento iestāžu pilnvaras rīkoties, lai nodrošinātu to valsts tiesību aktu ievērošanu, kuri ir pieņemti atbilstīgi noteikumiem, izņemot Direktīvas 95/46/EK 25. pantu, tās var īstenot savas pašreizējās pilnvaras, lai aizliegtu vai pārtrauktu datu plūsmu uz organizāciju, kas pati ir apliecinājusi, ka tā stingri ievēro atbilstīgi FAQ īstenotos principus, lai individuāls aizsargātu attiecībā uz viņu personas datus apstrādi, ja:

- a) šā lēmuma VII pielikumā minētā Amerikas Savienoto Valstu valdības iestāde vai neatkarīgs tiesību aizsardzības mehānisms, šā lēmuma I pielikumā izklāstītā piemērošanas principa a) punkta nozīmē, ir noteicis, ka organizācija neievēro atbilstīgi FAQ īstenotos principus; vai
- b) ir liela iespējamība, ka principi nav ievēroti; ir pamats uzskatīt, ka attiecīgais piemērošanas mehānisms neietver vai neietvers piemērotus un savlaicīgus pasākumus, lai attiecīgo gadījumu atrisinātu; nosūtīšanas turpināšana datu subjektiem radītu būtiska kaitējuma draudus; un dalībvalsts kompetentās iestādes šajos apstākļos ir darījušas visu iespējamo, lai organizācijai to paziņotu un dotu iespēju atbildēt.

Pārtraukšanu atceļ, tiklīdz ir nodrošināta atbilstīgi FAQ īstenoto principu ievērošana un attiecīgajām kompetentajām iestādēm Kopienā ir par to paziņots.

2. Ja pieņem pasākumus, pamatojoties uz 1. punktu, tad dalībvalstis par to nekavējoties informē Komisiju.

3. Dalībvalstis un Komisija arī informē viena otru par gadījumiem, kad ar to institūciju darbībām, kas Amerikas Savienotajās Valstīs ir atbildīgas par atbilstīgi FAQ īstenoto principu ievērošanu, šāda ievērošana nav panākta.

4. Ja saskaņā ar 1., 2. un 3. punktu apkopotā informācija liecina par to, ka kāda no iestādēm, kas Amerikas Savienotajās Valstīs ir

atbildīga par atbilstīgi FAQ īstenoto principu ievērošanu, savu uzdevumu pilda neefektīvi, tad Komisija informē ASV Tirdzniecības ministriju un, vajadzības gadījumā, iesniedz pasākumu projektu saskaņā ar Direktīvas 95/46/EK 31. pantā noteikto procedūru, nolūkā panākt, lai šo lēmumu atceltu vai apturētu, vai lai ierobežotu tā darbības jomu.

4. pants

1. Šo lēmumu var pielāgot jebkurā laikā, ņemot vērā pieredzi saistībā ar tā īstenošanu un/vai, ja ASV tiesību aktos ietver prasības nodrošināt augstāku aizsardzības līmeni, nekā to nodrošina principi un FAQ.

Komisija jebkurā gadījumā trīs gadus pēc paziņošanas dalībvalstīm novērtē šā lēmuma īstenošanu, pamatojoties uz pieejamo informāciju, un par visiem atbilstīgajiem atzinumiem ziņo Komitejai, kas izveidota saskaņā ar Direktīvas 95/46/EK 31. pantu, tostarp par pierādījumiem, kuri varētu ietekmēt novērtējumu, ka šā lēmuma 1. pantā paredzētie noteikumi nodrošina pienācīgu aizsardzību Direktīvas 95/46/EK 25. panta nozīmē, un par pierādījumiem, ka šo lēmumu īsteno diskriminējošā veidā.

2. Komisija, vajadzības gadījumā, saskaņā ar Direktīvas 95/46/EK 31. pantā norādīto procedūru iesniedz pasākumu projektu.

5. pants

Dalībvalstis veic visus vajadzīgos pasākumus, lai šo lēmumu izpildītu, vēlākais, deviņdesmit dienas pēc tā paziņošanas dalībvalstīm.

6. pants

Šis lēmums ir adresēts dalībvalstīm.

Briselē, 2000. gada 26. jūlijā

Komisijas vārdā —

Komisijas loceklis

Frederik BOLKESTEIN

I PIELIKUMS

PRIVĀTUMA “DROŠĪBAS ZONAS” PRINCIPI

izdevusi ASV Tirdzniecības ministrija 2000. gada 21. jūlijā

Eiropas Savienības visaptverošais tiesību akts par privātās dzīves aizsardzību — Direktīva par datu aizsardzību (Direktīva) stājās spēkā 1998. gada 25. oktobrī. Tajā izvirzīta prasība personas datus nosūtīt tikai uz tādām valstīm ārpus ES, kuras nodrošina “pienācīgu” privātuma aizsardzības līmeni. Gan Amerikas Savienoto Valstu, gan Eiropas Savienības mērķis ir uzlabot savu pilsoņu privātuma aizsardzību, taču Amerikas Savienotajās Valstīs ir citāda pieeja privātuma aizsardzībai, nekā Eiropas Savienībā. Amerikas Savienotās Valstis izmanto sektorālo pieeju, kas balstās gan uz ārējiem, gan iekšējiem normatīvajiem aktiem. Ņemot vērā šīs atšķirības, daudzas ASV organizācijas ir izteikušas neskaidrību par ES prasītā “atbilstības standarta” ietekmi uz personas datu nosūtīšanu no Eiropas Savienības uz Amerikas Savienotajām Valstīm.

Lai mazinātu šo neskaidrību un nodrošinātu šādu datu nosūtīšanai paredzamāku struktūru, Tirdzniecības ministrija saskaņā ar likumā noteiktajām pilnvarām izdod šo dokumentu un visbiežāk uzdotos jautājumus (“principi”), lai veicinātu, sekmētu un attīstītu starptautisko tirdzniecību. Principus izstrādāja, apspriežoties ar nozares uzņēmumiem un plašu sabiedrību, lai veicinātu tirdzniecību starp Amerikas Savienotajām Valstīm un Eiropas Savienību. Ir paredzēts, ka tos izmantos tikai tās ASV organizācijas, kas personas datus saņem no Eiropas Savienības, un kuras izpilda “drošības zonas” nosacījumus, un uz kurām tādējādi var attiecināt no tās izrietošo pieņemumu par “atbilstību”. Tā kā principi ir izstrādāti tikai šim īpašajam mērķim, to pieņemšana citiem mērķiem var būt nepiemērota. Principus nevar izmantot, lai aizstātu valsts noteikumus, ar kuriem īsteno šo direktīvu un kuri attiecas uz personas datu apstrādi dalībvalstīs.

Organizāciju lēmumi pretendēt uz “drošības zonu” ir pilnībā brīvprātīgi, un organizācijas var to pazīņot dažādos veidos. Organizācijām, kas nolemj stingri ievērot principus, principi jāizpilda, lai iegūtu un saglabātu “drošības zonas” priekšrocības, un par to jāpaziņo publiski. Piemēram, ja organizācija pievienojas kādai privātā sektora noteiktai pašregulatīvai slepenības programmai, kas stingri ievēro principus, tā iegūst tiesības uz “drošības zonu”. Organizācijas to var panākt arī, izstrādājot savu pašregulatīvu slepenības politiku, ja tā atbilst principiem. Ja organizācija, kas izvēlējusies kādu no abiem minētajiem variantiem, pārkāpj principus, tad tai piemēro sankcijas saskaņā ar *Federal Trade Commission Act* 5. paragrāfu, kas aizliedz negodīgu vai maldinošu darbību, vai arī saskaņā ar citiem normatīvajiem aktiem, kuri aizliedz šādu darbību. (Skatīt pielikumā to ASV oficiālo iestāžu sarakstu, ko ir atzinusi Eiropas Savienība.) Turklāt organizācijas, uz ko attiecas tādi normatīvie akti, administratīvie akti vai citi tiesību akti vai noteikumi, kuri efektīvi aizsargā personu privāto dzīvi, arī var pretendēt uz “drošības zonas” priekšrocībām. Visos gadījumos minētās priekšrocības organizācija saņem no dienas, kad tā pati apliecina Tirdzniecības ministrijai (vai tās pārstāvim), ka tā stingri ievēro principus saskaņā ar norādījumiem, kuri doti visbiežāk uzdotajā jautājumā par pašsertifikāciju.

Šo principu ievērošanu var ierobežot: a) ciktāl tas ir vajadzīgs, lai ievērotu valsts drošību, sabiedrības intereses vai izpildītu piemērošanas prasības; b) ar likumu, valdības noteikumiem vai tiesu praksi, kas rada pretrunīgus pienākumus, vai paredz skaidras atļaujas, ja, izmantojot šādu atļauju, organizācija var pierādīt, ka principu neievērošana ir tikai tiktāl, ciktāl ir vajadzīgs, lai ievērotu sevišķi svarīgas likumīgās intereses, kuras izriet no šādas atļaujas; vai c) ja direktīva vai dalībvalsts tiesību akti pieļauj izņēmumus vai atkāpes, ar nosacījumu, ka šādos izņēmumos vai atkāpēs piemēro pielīdzināmās situācijās. Saskaņā ar mērķi uzlabot privātās dzīves aizsardzību organizācijām jācenšas šos principus īstenot pilnībā un pārredzamā veidā, tostarp savā slepenības politikā norādot to, vai ar b) punktu atļautos izņēmumus attiecībā uz principiem piemēros regulāri. Tā paša iemesla dēļ organizācijām, ja iespējams, jāizvēlas labāka aizsardzība, ja izvēli atļauj principi un/vai ASV tiesību akti.

Organizācijas praktisku vai citu iemeslu dēļ var vēlēties principus attiecināt uz visām savām datu apstrādes darbībām, bet pienākums tos piemērot nosūtītajiem datiem ir tikai pēc tam, kad tās ir pievienojušās “drošības zonai”. Lai varētu pretendēt uz “drošības zonu”, organizācijām šie principi nav obligāti jāpiemēro manuāli apstrādājamai personiskajai informācijai. Organizācijām, kas vēlas gūt labumu no “drošības zonas”, saņemot manuāli apstrādājamu informāciju

no ES, principi jāpiemēro visai šāda veida informācijai pēc tam, kad tās pievienojas “drošības zonai”. Organizācija, kas vēlas “drošības zonas” priekšrocības attiecināt arī uz cilvēkresursu personisko informāciju, kas nosūtīta no ES izmantošanai saistībā ar darba attiecībām, tas jānorāda Tirdzniecības ministrijai (vai tās pārstāvim), veicot pašsertifikāciju, kā arī tai jāievēro prasības, kuras noteiktas visbiežāk uzdotajā jautājumā par pašsertifikāciju. Organizācijas varēs arī nodrošināt aizsardzības pasākumus, kas vajadzīgi saskaņā ar Direktīvas 26. pantu, ja tās iekļauj principus rakstiskos nolīgumos ar pusēm, kuras nosūta datus no ES, ievērojot materiālās tiesību normas attiecībā uz privātumu, ja Komisija un dalībvalstis uz šādiem tipveida līgumiem atļauj attiecināt pārējos noteikumus.

ASV tiesību akti attieksies uz jautājumiem par “drošības zonas” principu (tostarp visbiežāk uzdoto jautājumu) interpretāciju un ievērošanu, kā arī “drošības zonas” organizāciju attiecīgajām slepenības politikām, izņemot ja organizācijas ir apņēmušās sadarboties ar Eiropas datu aizsardzības iestādēm. Ja nav norādīts citādi, visus “drošības zonas” principu noteikumus un visbiežāk uzdotos jautājumus piemēro attiecīgā gadījumā.

“Personas dati” un “personiskā informācija” ir tādi dati par identificētu vai identificējamu individu, uz kuriem attiecas Direktīva un kuras ASV organizācija ir saņēmusi no Eiropas Savienības un jebkādā veidā reģistrējusi.

INFORMĒŠANA

Organizācijai jāinformē indivīdi par to, kādiem mērķiem tā vāc un izmanto informāciju par viņiem, kādā veidā var vērsties pie organizācijas ar jautājumiem vai sūdzībām, kāda veida trešām personām tā izpauž informāciju un kādas ir izvēles iespējas un līdzekļi, ko organizācija indivīdiem piedāvā, lai ierobežotu informācijas izmantošanu un izpaušanu. Šis paziņojums jāsniedz skaidrā un viegli saprotamā veidā. To nosūta indivīdiem, pirmo reizi lūdzot tos sniegt personisko informāciju organizācijai, vai cik drīz vien iespējams pēc tam, bet jebkurā gadījumā pirms organizācija šādu informāciju izmanto citiem mērķiem, izņemot tos, kuriem nosūtītāja organizācija to sākotnēji ievākusi vai apstrādājusi, vai to pirmo reizi izpaužusi trešai personai ⁽¹⁾.

IZVĒLE

Organizācijai indivīdiem jāpiedāvā iespēja izvēlēties (atteikt), vai viņu personisko informāciju a) izpauž trešai personai ⁽¹⁾ vai b) izmantos mērķim, kas ir nesavienojams ar mērķi(-iem), kuram(-iem) to sākotnēji ievāca vai indivīds pēc tam atļāva izmantot. Izvēles izdarīšanai indivīdiem jānodrošina skaidri un viegli saprotami, gatavi un pieejami mehānismi.

Attiecībā uz sensitīvu informāciju (t.i., personisko informāciju, kas ietver medicīniskos datus vai datus par veselības stāvokli, norāda personas rasi vai etnisko izcelsmi, politiskos uzskatus, reliģisko vai filozofisko pārliecību, dalību arodbiedrībā, vai ietver datus par indivīda seksuālo dzīvi), ir vajadzīga personas piekrišana vai skaidra (atļaujoša) izvēle, ja informāciju izpauž trešai personai vai izmantos citam mērķim izņemot tos, kuriem tā sākotnēji ievākta vai indivīds pēc tam atļāvis izmantot, izdarot izvēli. Jebkurā gadījumā organizācijai jebkāda informācija, kas ir saņemta no trešās puses, jāapstrādā kā sensitīva informācija, ja trešā puse to identificē un apstrādā kā sensitīvu.

TĀLĀKA NOSŪTĪŠANA

Izpaužot informāciju trešai personai, organizācijām jāpiemēro informēšanas un izvēles principi. Ja organizācija vēlas informāciju nosūtīt trešai personai, kas darbojas kā pārstāvis, kā aprakstīts nobeiguma piezīmē, tā var to darīt, ja tā pirms tam apliecina, ka trešā persona atbalsta principus vai ka uz to attiecas direktīva vai cits atzinums par atbilstību, vai ja tā noslēdz rakstisku līgumu ar šādu trešo personu, kurā prasīts, lai trešā persona nodrošina vismaz tādu pašu privātās dzīves aizsardzības līmeni, kādu prasa attiecīgie principi. Ja organizācija šīm prasībām atbilst, tā nav atbildīga (ja vien organizācija nepiekrīt pretējam) par to, ka trešā persona, kurai tā šādu informāciju nosūta, to apstrādā tādā veidā, kas ir pretrunā kādiem ierobežojumiem vai iebildumiem, izņemot ja organizācija ir zinājusi vai ja tai vajadzējais zināt, ka trešā persona to apstrādās šādā neatbilstīgā veidā un ja organizācija nav veikusi piemērotus pasākumus, lai šādu apstrādi nepieļautu vai pārtrauktu.

⁽¹⁾ Informēšanas vai izvēles principi nav obligāti jāpiemēro, ja datus izpauž trešai personai, kas darbojas kā pārstāvis, lai pildītu uzdevumus organizācijas vārdā un saskaņā ar tās norādījumiem. Taču tālākas nosūtīšanas princips uz šāda veida izpaušanu attiecas.

DROŠĪBA

Organizācijām, kas izveido, uztur, izmanto vai izplata personisko informāciju, jāveic samērīgi drošības pasākumi, lai to aizsargātu no pazaudēšanas, ļaunprātīgas izmantošanas, neatļautas piekļuves, izpaušanas, izmaiņšanas un iznīcināšanas.

DATU INTEGRITĀTE

Saskaņā ar principiem personiskajai informācijai jāatbilst mērķiem, kuriem tā paredzēta. Organizācija nedrīkst personisko informāciju apstrādāt tādā veidā, kas ir nesavienojams ar tiem mērķiem, kuriem tā sākotnēji savākta, vai kuriem indivīds pēc tam atļāvis to izmantot. Ciktāl tas ir vajadzīgs šiem mērķiem, organizācijai jāveic samērīgi pasākumi, lai nodrošinātu, ka dati saistībā ar paredzētajiem mērķiem ir ticami, precīzi, pilnīgi un aktuāli.

PIEKĻUVE

Indivīdiem jābūt piekļuvei personiskajai informācijai par viņiem, kas ir organizācijas rīcībā, un iespējai šo informāciju labot, mainīt vai dzēst, ja tā ir neprecīza, izņemot, ja apgrūtinājums vai izmaksas saistībā ar piekļuves nodrošināšanu būtu neatbilstīgas indivīda privātās dzīves apdraudējumam attiecīgajā gadījumā vai ja tas pārkāptu citu personu tiesības.

PIEMĒROŠANA

Efektīvai privātās dzīves aizsardzībai jāietver mehānismi, lai nodrošinātu principu ievērošanu, to indivīdu tiesību aizsardzību, uz kuriem dati attiecas un kurus ir ietekmējusi principu neievērošana, un sekas organizācijai, ja principi nav ievēroti. Šādiem mehānismiem jāietver vismaz: a) gatavi un pieejami neatkarīgi tiesību aizsardzības mehānismi, saskaņā ar kuriem izmeklē un risina katra indivīda sūdzības un domstarpības, atsaucoties uz principiem, kā arī atlīdzina kaitējumu, ja to paredz piemērojamie tiesību akti vai privātā sektora iniciatīvas; b) paveiktā darba kontroles procedūras, lai pārbaudītu, vai apliecinājumi un apgalvojumi, ko uzņēmumi ir izteikuši par savu slepenības praksi, ir patiesi, un vai šī prakse ir īstenota tā, kā norādīts; un c) pienākums risināt problēmas, kas rodas saistībā ar to, ka organizācijas, kuras ir pasludinājušas, ka stingri ievēro principus, to nedara, un sekas attiecībā uz šādām organizācijām. Sankcijām jābūt pietiekami stingrām, lai nodrošinātu, ka organizācijas principus ievēro.

*Pielikums***To ASV oficiālo iestāžu saraksts, ko Eiropas Savienība ir atzinusi**

Eiropas Savienība atzīst, ka šādas ASV valdības iestādes ir pilnvarotas izmeklēt sūdzības un iegūt palīdzību negodīgas vai maldinošas rīcības novēršanai, kā arī kompensāciju indivīdiem, neatkarīgi no viņu mītnes valsts vai valstiskās piederības, ja nav ievēroti atbilstīgi FAQ īstenotie principi:

- *Federal Trade Commission*, pamatojoties uz pilnvarojumu saskaņā ar *Federal Trade Commission Act* 5. paragrāfu,
- Transporta ministrija, pamatojoties uz pilnvarojumu saskaņā ar *United States Code* 49. sadaļas 41712. paragrāfu.

II PIELIKUMS

VISBIEŽĀK UZDOTIE JAUTĀJUMI (FAQ)

FAQ 1 — Sensitīvi dati

Jaut.: *Vai organizācijai vienmēr jādod skaidra (atļaujoša) izvēle attiecībā uz sensitīviem datiem?*

Atb.: Nē, šāda izvēle nav obligāta, ja apstrāde ir: 1) datu subjekta vai citas personas sevišķi svarīgās interesēs; 2) vajadzīga, lai celtu likumīgas prasības vai aizstāvētu tās; 3) vajadzīga, lai sniegtu medicīnisko aprūpi vai noteiktu diagnozi; 4) veikta kāda fonda, asociācijas vai jebkuras citas bezpeļņas organizācijas likumīgu darbību laikā ar politisku, filozofisku, reliģisku vai ar arod biedrībām saistītu mērķi, un ar nosacījumu, ka apstrāde attiecas tikai uz šīs organizācijas locekļiem vai personām, kas ar šo organizāciju uztur regulārus sakarus saistībā ar tās mērķiem, un ka datus neizpauž trešām personām bez datu subjektu piekrišanas; 5) vajadzīga, lai izpildītu organizācijas pienākumus darba tiesību jomā; vai 6) saistīta ar datiem, ko indivīds acīmredzami ir publicējis.

FAQ 2 — Izņēmumi attiecībā uz žurnālistiku

Jaut.: *Nemot vērā ASV konstitūcijā noteikto preses brīvības aizsardzību un direktīvā noteikto izņēmumu attiecībā uz žurnālistu materiālu, vai “drošības zonas” principi attiecas uz personisko informāciju, kas savākta, uzturēta vai izplatīta žurnālistiskiem mērķiem?*

Atb.: Ja ar ASV konstitūcijas pirmo grozījumu noteiktās tiesības uz brīvu presi saduras ar privātās dzīves aizsardzības interesēm, pirmajam grozījumam jāreglamentē šo interešu sabalansēšana attiecībā uz ASV personu vai organizāciju darbībām. “Drošības zonas” principu prasības neattiecas uz personisko informāciju, kas ir savākta publicēšanai, apraidei vai citām žurnālistikas materiālu publiskas paziņošanas formām, neatkarīgi no tā, vai tā ir vai nav izmantota, kā arī uz informāciju, kura ir atrodama iepriekš publicētos materiālos, kas ir izplatīti no mediju arhīviem.

FAQ 3– Sekundārā atbildība

Jaut.: *Vai saskaņā ar “drošības zonas” principiem Interneta pakalpojumu sniedzēji, telekomunikāciju uzņēmumi vai citas organizācijas ir atbildīgas, ja tās citu organizāciju vārdā tikai nosūta, virza, maina vai uzglabā informāciju, kas var būt pretrunā principu noteikumiem?*

Atb.: Nē. Tāpat kā Direktīva, “drošības zona” nerada sekundāro atbildību. Ciktāl organizācija darbojas tikai kā nodošanas kanāls trešās personas nosūtītajiem datiem un nenosaka šo personas datu apstrādes mērķus un līdzekļus, tai nav jāuzņemas atbildība.

FAQ 4 — Investīciju bankas un revīzija

Jaut.: *Revidentu un investīciju bankieru darījumi var būt saistīti ar personas datu apstrādi bez indivīda piekrišanas vai ziņas. Kādos apstākļos tas ir atļauts atbilstīgi informēšanas, izvēles un piekļuves principiem?*

Atb.: Investīciju bankieri vai auditori var informāciju apstrādāt bez indivīda ziņas vienīgi tiktāl un tikai tādu laikposmu, kas ir vajadzīgs, lai izpildītu ar likumu noteiktās prasības vai sabiedrības interešu prasības, un citos apstākļos, kad šo principu piemērošana kaitētu organizācijas likumīgajām interesēm. Šīs likumīgās intereses ietver uzraudzību, vai uzņēmumi ievēro savas juridiskās saistības, un likumīgas grāmatvedības darbības, kā arī tādas konfidencialitātes nepieciešamību, kas ir saistīta ar iespējamu pārņemšanu, apvienošanu, kopuzņēmumiem vai citiem līdzīgiem darījumiem, kurus investīciju bankieri vai revidenti veic.

FAQ 5 — Datu aizsardzības iestāžu nozīme

Jaut.: *Kā uzņēmumi, kas apņemas sadarboties ar Eiropas datu aizsardzības iestādēm (DPA), šīs saistības uzņemas, un kā tās īsteno?*

Atb.: Saskaņā ar “drošības zonu” tām ASV organizācijām, kas saņem personas datus no ES, jāapņemas izmantot efektīvus mehānismus, lai nodrošinātu “drošības zonas” principu ievērošanu. Konkrētāk, kā izklāstīts piemērošanas principā, tām jānodrošina: a) to indivīdu tiesību aizsardzība, uz kuriem dati attiecas, b) paveiktā darba kontroles procedūras, lai pārbaudītu, vai apliecinājumi un apgalvojumi, ko tās ir izteikušas par savu slepenības praksi, ir patiesi, un c) pienākums risināt problēmas, kas rodas saistībā ar principu neievērošanu, un sekas attiecībā uz šādām organizācijām. Organizācijai jāizpilda piemērošanas principa a) un c) punkti, ja tā, sadarbojoties ar datu aizsardzības iestādēm, stingri ievēro šajā jautājumā noteiktās prasības.

Organizācija var apņemties sadarboties ar datu aizsardzības iestādēm, savā “drošības zonas” apliecinājumā Tirdzniecības ministrijai (skatīt FAQ 6 par pašsertifikāciju), paziņojot, ka tā:

- 1) ir nolēmusi izpildīt “drošības zonas” piemērošanas principa a) un c) punkta prasības, apņemties sadarboties ar datu aizsardzības iestādēm;
- 2) sadarbosies ar datu aizsardzības iestādēm, izmeklējot un risinot sūdzības, kas ir iesniegtas saskaņā ar “drošības zonu”; un
- 3) ievēros visus datu aizsardzības iestāžu dotos ieteikumus, ja tās ņem vērā, ka organizācijai jāveic īpaši pasākumi, lai ievērotu “drošības zonas” principus, to skaitā pasākumi stāvokļa izlabošanai vai kompensācijas pasākumi to indivīdu labā, ko principu neievērošana ir ietekmējusi, un sniegs datu aizsardzības iestādēm rakstisku apstiprinājumu, ka šādi pasākumi ir veikti.

Datu aizsardzības iestādes sadarbību sniegs kā informāciju un ieteikumus šādā veidā:

- Datu aizsardzības iestāžu ieteikumus nodos ar datu aizsardzības iestāžu neformālas komisijas starpniecību, kas izveidota Eiropas Savienības līmenī un kas, cita starpā, palīdzēs nodrošināt saskaņotu un viendabīgu pieeju.
- Komisija sniegs ieteikumus attiecīgām ASV organizācijām par neatrisinātām indivīdu sūdzībām par tādas personiskās informācijas apstrādi, kas ir nosūtīta no ES saskaņā ar “drošības zonu”. Šie ieteikumi būs izstrādāti, lai nodrošinātu, ka “drošības zonas” principus piemēro pareizi, un tie iekļaus tādas tiesību aizsardzības līdzekļus attiecīgajam(-iem) indivīdam(-iem), ko datu aizsardzības iestādes uzskata par piemērotiem.
- Komisija šādus ieteikumus sniegs, atbildot uz pieprasījumiem no attiecīgajām organizācijām un/vai sūdzībām, kas saņemtas tieši no indivīdiem, par organizācijām, kuras ir apņēmušas sadarboties ar datu aizsardzības iestādēm “drošības zonas” nolūkiem, tai pašā laikā iedrošinot un, vajadzības gadījumā, palīdzot šādiem indivīdiem pirms tam izmantot iekšējo sūdzību izskatīšanas kārtību, ko organizācija var piedāvāt.
- Ieteikumus sniegs tikai pēc tam, kad abām strīdā iesaistītajām pusēm būs bijusi pienācīga iespēja sniegt atsaukmes un visus pierādījumus, ko tās vēlas. Komisija centīsies ieteikumus sniegt, cik vien drīz to atļauj šī prasība par pienācīgu izskatīšanu. Parasti komisija centīsies sniegt ieteikumus 60 dienās pēc sūdzības vai pieprasījuma saņemšanas un, ja iespējams, ātrāk.
- Ja tā sūdzības uzskatīs par pamatotām, komisija publicēs tai iesniegto sūdzību izskatīšanas rezultātus.
- Ar komisijas starpniecību sniegtie ieteikumi neuzliek komisijai vai atsevišķām datu aizsardzības iestādēm nekādu atbildību.

Kā iepriekš minēts, organizācijām, kas izvēlas šo strīdu izšķiršanas veidu, jāņem vērā datu aizsardzības iestāžu ieteikumus. Ja organizācija 25 dienās no ieteikumu sniegšanas tos neievēro un nav sniegusi pietiekamu pamatojumu par kavēšanos, komisija paziņo pati par savu nodomu vai nu iesniegt lietu *Federal Trade Commission*, vai citai ASV federālajai vai štata iestādei, kam ir likumā noteiktas pilnvaras veikt piemērošanas nodrošināšanas darbības krāpšanas vai sagrozījumu gadījumā vai secināt, ka vienošanās par sadarbību ir būtiski pārkāpta un tādēļ jāuzskata par spēkā neesošu. Pēdējā gadījumā komisija informē Tirdzniecības ministriju (vai tās pārstāvi), lai varētu noteiktajā kārtībā grozīt “drošības zonas” dalībnieku sarakstu. Ja netiek ievērota apņemšanās sadarbīties ar datu aizsardzības iestādēm, kā arī “drošības zonas” principi, to var tiesiski apstrīdēt kā maldinošu darbību saskaņā ar 5. paragrāfu *Federal Trade Commission Act* vai saskaņā ar citu attiecīgu likumu.

Organizācijām, kas izvēlas šo iespēju, jāmaksā gada maksa, kas ir paredzēta, lai segtu komisijas darbības izmaksas, un tām var papildus prasīt segt visas vajadzīgās tulkošanas izmaksas, kuras rodas saistībā ar tādu pieprasījumu vai sūdzību izskatīšanu komisijā, kuri vērsti pret šīm organizācijām. Ikgadējais maksājums nepārsniedz USD 500 un ir zemāks mazākiem uzņēmumiem.

Iespēja sadarbīties ar datu aizsardzības iestādēm būs organizācijām, kas pievienojas “drošības zonai” trīs gadu laikposmā. Datu aizsardzības iestādes šo kārtību pārskata pirms šā laikposma beigām, ja to ASV organizāciju skaits, kas izvēlas šo iespēju, ir pārāk liels.

FAQ 6 — Pašsertifikācija

Jaut.: Kā organizācija pati apliecina, ka tā stingri ievēro “drošības zonas” principus?

Atb.: “Drošības zonas” priekšrocības nodrošina no dienas, kad organizācija pati apliecina Tirdzniecības ministrijai (vai tās pārstāvim), ka tā stingri ievēro principus atbilstīgi turpmāk minētajiem norādījumiem.

Lai organizācija pati apliecinātu “drošības zonu”, tā var Tirdzniecības ministrijai (vai tās pārstāvim) nosūtīt vēstuli, kuru parakstījusi tās amatpersona organizācijas vārdā, kas pievienojas “drošības zonai”, un kurā ir vismaz šāda informācija:

- 1) organizācijas nosaukums, pasta adrese, e-pasta adrese, telefona un faksa numuri;
- 2) organizācijas darbību apraksts attiecībā uz personisko informāciju, kas saņemta no ES; un
- 3) organizācijas slepenības politikas apraksts attiecībā uz šādu personisko informāciju, tostarp norādot: a) vai slepenības politika ir pieejama publiski, b) dienu, kurā ir sākusies tās īstenošana, c) kontaktbiroju, kas izskata sūdzības, piekļuves pieprasījumus un visus citus jautājumus, kuri rodas saistībā ar “drošības zonu”, d) konkrētu oficiālu iestādi, kuras jurisdikcijā ir izskatīt prasības pret organizāciju attiecībā uz negodīgu vai maldinošu rīcību un privātās dzīves aizsardzību reglamentējošu likumu vai noteikumu pārkāpšanu (un kuras ir uzskaitītas principu pielikumā), e) to slepenības programmu nosaukumus, kurās organizācija piedalās, f) pārbaudes metodi (piem., iekšēja, trešās personas) ⁽¹⁾ un g) neatkarīgu tiesību aizsardzības mehānismu, kas ir pieejams neatrisināto sūdzību izmeklēšanai.

Ja organizācija vēlas, lai “drošības zonas” priekšrocības attiektos uz informāciju par cilvēkresursiem, kas nosūtīta no ES izmantošanai saistībā ar darba attiecībām, tā var to darīt, ja ir oficiāla iestāde, kuras jurisdikcijā ir izskatīt tās prasības pret organizāciju, kas rodas saistībā ar principu pielikumā uzskaitīto informāciju par cilvēkresursiem. Turklāt organizācijai tas jānorāda savā vēstulē un jāizsaka apņemšanās sadarbīties ar attiecīgo ES iestādi vai iestādēm atbilstīgi FAQ 9 un FAQ 5 pēc vajadzības un ievērot šādu iestāžu sniegtos ieteikumus.

Ministrija (vai tās pārstāvis) uzturēs visu to organizāciju sarakstu, kas šādas vēstules ir atsūtījušas, tā nodrošinot “drošības zonas” priekšrocību pieejamību, un šādu sarakstu atjauninās, pamatojoties uz ikgadējam vēstulēm un paziņojumiem, kuri saņemti atbilstīgi FAQ 11. Šādas pašsertifikācijas vēstules jāatsūta ne retāk kā reizi gadā. Pretējā gadījumā organizāciju no saraksta svītros, un “drošības zonas” priekšrocības tai vairs nenodrošinās.

⁽¹⁾ Skat. FAQ 7 par pārbaudi.

Gan sarakstu, gan organizāciju iesniegtās pašsertifikācijas vēstules padarīs publiski pieejamas. Visām organizācijām, kas pašas apliecina "drošības zonu", savos attiecīgajos publicētajos slepenības politikas paziņojumos jānorāda, ka tās stingri ievēro "drošības zonas" principus.

Apņemšanās stingri ievērot "drošības zonas" principus laika ziņā nav ierobežota attiecībā uz datiem, kuri saņemti laikposmā, kad organizācija izmanto "drošības zonas" priekšrocības. Tās apņemšanās nozīmē, ka tā turpinās šādiem datiem piemērot principus tik ilgi, kamēr organizācija tos glabā, izmanto vai izpauž, pat ja pēc tam tā kāda iemesla dēļ no "drošības zonas" izstājas.

Organizācijai, kas apvienošanās vai pārņemšanas rezultātā pārstās pastāvēt kā atsevišķa juridiska persona, par to iepriekš jāpaziņo Tirdzniecības ministrijai (vai tās pārstāvim). Paziņojumā arī jānorāda, vai iegūstošai juridiskajai personai vai juridiskajai personai, kas rodas apvienošanās rezultātā, 1) "drošības zonas" principi turpinās būt saistoši saskaņā ar likumu, kurš reglamentē pārņemšanu vai apvienošanu, vai 2) tā izvēlas pati apliecināt, ka tā stingri ievēro "drošības zonas" principus, vai ieviest citus aizsardzības pasākumus, piemēram rakstisku vienošanos, ka tā nodrošinās "drošības zonas" principu stingru ievērošanu. Ja nepiemēro ne 1), ne 2) punktu, visi dati, kas ir iegūti saistībā ar "drošības zonu", nekavējoties jāizdzēš.

Organizācijai nav jāpiemēro "drošības zonas" principi visai personiskajai informācijai, bet tie ir jāpiemēro visiem personas datiem, kas saņemti no ES, pēc tam, kad organizācija pievienojusies "drošības zonai".

Federal Trade Commission vai cita attiecīga valsts iestāde var tiesiski apstrīdēt jebkuru sagrozījumu plašai sabiedrībai par organizācijas "drošības zonas" principu stingru ievērošanu. Faktu sagrozīšana Tirdzniecības ministrijai (vai tās pārstāvim) var būt tiesiski apstrīdama saskaņā ar Likumu par nepatiesām ziņām (18 U. S. C. § 1001).

FAQ 7 — Pārbaude

Jaut.: *Kā organizācijas nodrošina paveiktā darba kontroles procedūras, lai pārbaudītu, vai apliecinājumi un apgalvojumi, ko tās ir izteikušas par savu "drošības zonas" praksi, ir patiesi un ka šī slepenības prakse ir īstenotā kā aprakstīts un atbilstīgi "drošības zonas" principiem?*

Atb.: Lai izpildītu piemērošanas principa pārbaudes prasības, organizācija šādus apliecinājumus un apgalvojumus var pārbaudīt ar pašnovērtēšanu vai ārējām atbilstības pārbaudēm.

Izmantojot pašnovērtēšanas pieeju, šādi pārbaudei būtu jānorāda, ka organizācijas publicētā slepenības politika attiecībā uz personisko informāciju, kas saņemta no ES, ir precīza, saprotama, izvietota redzamā vietā, pilnībā īstenota un pieejama. Tai arī būtu jānorāda, ka tās slepenības politika atbilst "drošības zonas" principiem; ka indivīdi ir informēti par iekšējo sūdzību izskatīšanas kārtību un par neatkarīgiem mehānismiem, ar kuriem viņi var iesniegt sūdzību; ka tai ir izstrādātas darbinieku apmācības procedūras, lai politiku īstenotu, un procedūras darbinieku sodīšanai par tās neievērošanu; un ka tai ir izstrādātas iekšējās procedūras, kā veikt periodisku, objektīvu pārskatīšanu attiecībā uz iepriekš minēto. Ziņojumu, kas apliecina pašnovērtēšanu, vismaz reizi gadā jāparaksta amatpersonai vai citam organizācijas pilnvarotam pārstāvim un jāuzrāda pēc indivīdu pieprasījuma vai saistībā ar izmeklēšanu vai sūdzību par neatbilstību.

Organizācijām jāglabā savas atskaites par privātuma "drošības zonas" prakses īstenošanu un pēc pieprasījuma saistībā ar izmeklēšanu vai sūdzību par neatbilstību jāuzrāda neatkarīgai institūcijai, kas ir atbildīga par sūdzību izmeklēšanu, vai iestādei, kuras jurisdikcijā ir lietas par negodīgu un maldinošu rīcību.

Ja organizācija ir izvēlējusies ārēju atbilstības pārbaudi, šādi pārbaudei ir jāparāda, ka slepenības politika attiecībā uz personisko informāciju, kas saņemta no ES, atbilst "drošības zonas" principiem, ka tos ievēro un ka indivīdi ir informēti par mehānismiem, ar kuriem viņi var iesniegt sūdzības. Pārbaudes metodes var neierobežoti pēc vajadzības iekļaut revīziju, izlases veida pārskatīšanu, "mānekļu" vai tehnoloģijas ierīču

izmantošanu. Ziņojums, kas apliecina, ka ārējā atbilstības pārbaude ir veiksmīgi pabeigta, vismaz reizi gadā jāparaksta vai nu pārbaudes veicējam, vai organizācijas amatpersonai, vai citam organizācijas pilnvarotam pārstāvim un jāuzrāda pēc individu pieprasījuma vai saistībā ar izmeklēšanu vai sūdzību par neatbilstību.

FAQ 8 — Piekļuve

Piekļuves princips:

Indivīdiem jābūt piekļuvei personiskajai informācijai par viņiem, kas ir organizācijas rīcībā, un jāvar šo informāciju labot, mainīt vai dzēst, ja tā ir neprecīza, izņemot ja apgrūtinājums vai izmaksas saistībā ar piekļuves nodrošināšanu būtu neatbilstīgas indivīda privātās dzīves apdraudējumam attiecīgajā gadījumā vai ja būtu pārkāptas citu personu likumīgās tiesības.

1. Jaut.: *Vai tiesības uz piekļuvi ir absolūtas?*

1. Atb.: Nē. Saskaņā ar “drošības zonas” principiem tiesības uz piekļuvi ir būtiskas privātās dzīves aizsardzībai. Jo īpaši, tās ļauj indivīdiem pārliecināties par tās informācijas precizitāti, ko par viņiem glabā. Tomēr attiecībā uz organizācijas pienākumu nodrošināt piekļuvi personiskajai informācijai, kas ir tās rīcībā par indivīdu, jāievēro proporcionalitātes princips vai samērīguma princips, un pienākums atsevišķos gadījumos jāmazina. 1980. gada ESAO Privātās dzīves aizsardzības pamatnostādņu paskaidrojuma rakstā ir skaidri noteikts, ka organizācijas pienākums attiecībā uz piekļuvi nav absolūts. Tas neprasa pārāk rūpīgu meklēšanu, kas ir atļauta, piemēram, ar tiesas pavēsti, kā arī neprasa piekļuvi visām dažādajām organizācijas informācijas uzglabāšanas formām.

Pieredze drīzāk liecina, ka, atbildot uz indivīdu pieprasījumiem pēc piekļuves, organizācijām pirmkārt būtu jāvadās pēc pieprasījuma pamatojuma(-iem). Piemēram, ja pieprasījums pēc piekļuves ir neskaidrs vai attiecas uz plašu jomu, organizācija var indivīdu iesaistīt dialogā, lai labāk saprastu pieprasījuma pamatojumu un atrastu atbilstīgo informāciju. Organizācija var jautāt, ar kuru organizācijas daļu(-ām) indivīds ir sazinājies un/vai par tās informācijas (vai tās izmantošanas) raksturu, kurai prasa piekļuvi. Tomēr indivīdam nav jāpamato pieprasījumi pēc piekļuves saviem datiem.

Izdevumi un apgrūtinājums ir svarīgi faktori, un tie jāņem vērā, bet tie nav galvenie, nosakot, vai piekļuves nodrošināšana ir pamatota. Piemēram, ja informāciju izmanto lēmumiem, kas indivīdu būtiski ietekmēs (piem., tādu svarīgu priekšrocību atteikšana vai piešķiršana kā apdrošināšana, hipotēka vai darbs), tad atbilstīgi šo FAQ pārējiem noteikumiem organizācijai būtu informācija jāizpauž pat tad, ja to sniegt būtu salīdzinoši grūti vai dārgi.

Ja pieprasīta informācija nav sensitīva informācija vai ja to neizmanto lēmumiem, kas indivīdu būtiski ietekmēs (piem., nesensitīvi tirgvedības dati, kurus izmanto, lai noteiktu, vai indivīdam būtīgu katalogu), bet tā ir viegli pieejama un tās sniegšana nav dārga, tad organizācijai jāsniedz piekļuve faktiskajai informācijai, ko organizācija par indivīdu glabā. Attiecīgā informācija varētu ietvert faktus, kas iegūti no indivīda, faktus, kuri konstatēti darījuma laikā, vai faktus, kas iegūti no citām personām un kas attiecas uz indivīdu.

Atbilstīgi piekļuves pamatraksturam organizācijām vienmēr godprātīgi jācenšas piekļuvi nodrošināt. Piemēram, ja konkrēta informācija jāaizsargā un to var viegli nošķirt no pārējās informācijas, kurai prasa piekļuvi, tad organizācijai aizsargājamā informācija jānošķir un jāsniedz pārējā informācija. Ja organizācija nosaka, ka piekļuve kādā konkrētā gadījumā jāliedz, tā indivīdam, kas prasa piekļuvi, sniedz paskaidrojumu, kāpēc ir pieņemts šāds lēmums un norāda, kur var saņemt papildu informāciju.

2. Jaut.: *Kas ir konfidenciāla komercinformācija un vai organizācijas drīkst liegt piekļuvi, lai to aizsargātu?*

2. Atb.: Konfidenciāla komercinformācija (kā šis termins ir izmantots Federālajos civilprocesa normatīvos par informācijas atklāšanu) ir informācija, attiecībā uz kuru organizācija ir veikusi pasākumus, lai to pasargātu no izpaušanas, ja izpaušana palīdzētu kādam konkurentam tirgū. Īpašā datorprogramma, ko organizācija izmanto, kā piemēram, modelēšanas programma, vai ziņas par šo programmu var būt konfidenciāla komercinformācija. Ja konfidenciālu komercinformāciju var viegli nošķirt no pārējās informācijas, kurai

prasa piekļuvi, tad organizācijai konfidencialā komercinformācija jānošķir un jāpadara pieejama nekonfidencialā informācija. Organizācijas var liegt vai ierobežot piekļuvi, ja tās nodrošināšana atklātu viņu pašu konfidencialu komercinformāciju, kā definēts iepriekš, piemēram, secinājumus par tirgvedību vai organizācijas izveidoto klasifikāciju, vai citu konfidencialu komercinformāciju, ja uz šādu informāciju attiecas līgumsaistības par konfidencialitāti, apstākļos, kad šādu saistību ievērot konfidencialitāti parasti uzņemas vai uzliek.

3. Jaut.: *Vai sniegtot piekļuvi, organizācija drīkst indivīdiem izpaust personisko informāciju par viņiem, kas ir iegūta no tās datubāzēm, vai arī ir jāsniedz piekļuve pašai datu bāzei?*
3. Atb.: Piekļuvi var sniegt, organizācijai izpaužot indivīdam informāciju, un nav prasības sniegt indivīdam piekļuvi organizācijas datu bāzei.
4. Jaut.: *Vai organizācijai ir jāpārstrukturē savas datu bāzes, lai varētu sniegt piekļuvi?*
4. Atb.: Piekļuve jāsniedz tikai tad, ja organizācija uzglabā informāciju. Piekļuves princips nerada pienākumu saglabāt, uzturēt, reorganizēt vai pārstrukturēt datnes ar personisko informāciju.
5. Jaut.: *Šajās atbildēs ir skaidri norādīts, ka atsevišķos apstākļos piekļuvi var liegt. Kādos citos apstākļos organizācija drīkst indivīdiem liegt piekļuvi viņu personiskajai informācijai?*
5. Atb.: Šādi apstākļi ir ierobežoti, un jānorāda piekļuves atteikuma iemesli. Organizācija var atteikt sniegt piekļuvi informācijai, ja tās izpaušana var būt pretrunā svarīgu sabiedrības interešu aizsardzībai, piemēram, valsts drošībai, aizsardzībai vai sabiedrības drošībai. Turklāt piekļuvi var liegt, ja personisko informāciju apstrādā tikai pētnieciskiem vai statistiskiem mērķiem. Citi iemesli, lai piekļuvi liegtu vai ierobežotu, ir šādi:
- a) likuma izpildes vai tiesību piemērošanas kavēšana, tostarp pārkāpumu novēršana, izmeklēšana vai atklāšana, kā arī tiesības uz taisnīgu tiesu;
 - b) rīcības kavēšana, tostarp saistībā ar civilprasību izskatīšanu tiesā, lietu izmeklēšanu vai atklāšanu, kā arī tiesības uz taisnīgu tiesu;
 - c) tādas personiskās informācijas izpaušana, kas attiecas uz citu(-iem) indivīdu(-iem), ja šādu informāciju nevar nošķirt;
 - d) juridiskas vai citas profesionālas priekšrocības neievērošana vai pienākuma neizpilde;
 - e) vajadzīgās konfidencialitātes neievērošana attiecībā uz turpmākām vai notiekošām sarunām, piemēram tādām sarunām, kas ietver publiski kotētu uzņēmumu pārņemšanu;
 - f) kaitējums darbinieku drošības izmeklēšanai vai šķērējietas procesiem;
 - g) apdraudējums konfidencialitātei, kas var būt vajadzīga ierobežotos laikposmos saistībā ar plāniem par jaunu darbinieku pieņemšanu un korporatīvu reorganizāciju; vai
 - h) apdraudējums konfidencialitātei, kas var būt vajadzīga saistībā ar pareizu saimnieciskās vai finanšu vadības uzraudzību, pārbaudi vai reglamentējošām funkcijām; vai
 - i) citi apstākļi, kuros apgrūtinājums vai izmaksas saistībā ar piekļuves nodrošināšanu būtu nesamērīgas vai pārkāptu citu likumīgās tiesības vai intereses.

Organizācijai, kas pieprasa izņēmumu, jāparāda tā piemērojamība (kas parasti tā arī ir). Kā minēts iepriekš, indivīdiem jānorāda iemesli, kāpēc pieeja liegta vai ierobežota, un kontaktpunkti, kur var saņemt papildu informāciju.

6. Jaut.: *Vai organizācija var iekasēt samaksu, lai segtu piekļuves nodrošināšanas izmaksas?*

6. Atb.: Jā. ESAO pamatnostādņēs ir noteikts, ka organizācijas drīkst iekasēt samaksu, ja tā nav pārmērīgi augsta. Tādējādi organizācija par piekļuvi var iekasēt samērīgu samaksu. Samaksas iekasēšana var palīdzēt novērst atkārtotus un nenozīmīgus pieprasījumus.

Organizācijas, kas nodarbojas ar publiski pieejamas informācijas pārdošanu tādējādi var iekasēt organizācijas parasto samaksu, atbildot uz piekļuves pieprasījumiem. Individīdi piekļuvi savai informācijai var prasīt arī organizācijai, kas datus ir apkopojusi sākotnēji.

Piekļuvi nedrīkst atteikt, pamatojoties uz izmaksām, ja indivīds piedāvā tās segt.

7. Jaut.: *Vai organizācijai ir jāsniedz piekļuve personiskajai informācijai, kas ir iegūta no publiskiem reģistriem?*

7. Atb.: Pirmkārt, jāpaskaidro, ka publiski reģistri ir tie reģistri, ko glabā valdības iestādes vai struktūrvienības jebkurā līmenī un kas parasti ir sabiedrībai pieejami. Uz šādu informāciju nav jāattiecinā piekļuves princips, kamēr tā nav kopā ar citu personisko informāciju, izņemot ja nelielu daļu no informācijas no reģistra, kas nav publiska, izmanto publiskā reģistra rādītāja sastādīšanai vai organizācijai. Tomēr jāievēro visi izmantošanas nosacījumi, ko noteikusi attiecīgā kompetentā iestāde. Ja publiskā reģistra informācija ir kopā ar citu informāciju no reģistra, kas nav publiska (kas nav īpaši noteikta iepriekš), organizācijai tomēr jāsniedz pieeja visai šādai informācijai, pieņemot, ka uz to neattiecas citi atļauti izņēmumi.

8. Jaut.: *Vai pieejas princips jāpiemēro publiski pieejamai personiskajai informācijai?*

8. Atb.: Tāpat kā ar publisko reģistru informāciju (skatīt 7. jaut.), nav jāsniedz pieeja informācijai, kas jau ir publiski pieejama plašai sabiedrībai, ja vien tā nav kopā ar informāciju, kura nav publiski pieejama.

9. Jaut.: *Kā organizācija var sevi aizsargāt pret atkārtotiem vai nenozīmīgiem pieprasījumiem pēc piekļuves?*

9. Atb.: Organizācijai uz šādiem pieprasījumiem pēc piekļuves nav jāatbild. Tādēļ organizācijas var iekasēt samērīgu samaksu un noteikt piemērotus limitus attiecībā uz to, cik reizes noteiktā laikā posmā izskata viena indivīda pieprasījumus pēc piekļuves. Nosakot šādus ierobežojumus, organizācijai jāņem vērā tādi faktori kā informācijas atjaunināšanas biežums, datu izmantošanas mērķis un informācijas raksturs.

10. Jaut.: *Kā organizācija var sevi aizsargāt pret krāpnieciskiem pieprasījumiem pēc piekļuves?*

10. Atb.: Organizācijai jāsniedz piekļuve tikai tad, kad tai ir iesniegta pietiekama informācija, kas apstiprina pieprasījuma iesniedzēja identitāti.

11. Jaut.: *Vai ir noteikts termiņš, kurā jāsniedz atbildes uz piekļuves pieprasījumiem?*

11. Atb.: Jā, organizācijām jāatbild bez pārmērīgas kavēšanās un samērīgā laikposmā. Šo prasību var izpildīt dažādi, kā norādīts 1980. gada ESAO Privātās dzīves aizsardzības pamatnostādņu paskaidrojuma rakstā. Piemēram, par datu apstrādi atbildīgo personu, kas ar regulāriem intervāliem datu subjektiem sniedz informāciju, var atbrīvot no pienākuma uzreiz atbildēt uz indivīdu pieprasījumiem.

FAQ 9 — Cilvēkresursi

1. Jaut.: *Vai "drošības zona" attiecas uz tādas personiskās informācijas nosūtīšanu no ES uz Amerikas Savienotajām Valstīm, kas savākta saistībā ar darba attiecībām?*

1. Atb.: Jā, ja ES uzņēmums nosūta pakalpojumu sniedzējam Amerikas Savienotās Valstīs tādu personisko informāciju par saviem (esošajiem vai bijušajiem) darbiniekiem, kas savākta saistībā ar darba attiecībām, uz nosūtīšanu attiecas "drošības zonas" priekšrocības. Tādos gadījumos uz informācijas vākšanu un tās apstrādi

pirms nosūtīšanas attiecas tās ES valsts tiesību akti, kurā informācija savākta, un jāievēro visi nosacījumi vai ierobežojumi attiecībā uz tās nosūtīšanu atbilstīgi šiem tiesību aktiem.

“Drošības zonas” principus piemēro tikai nosūtot vai pieklūstot atsevišķi identificētiem datiem. Statistikas ziņojumi, kas atsaucas uz kopējiem nodarbinātības datiem un/vai anonimizētu vai ar pseidonīmu reģistrētu datu izmantošanu, nerada privātās dzīves apdraudējumu.

2. Jaut.: *Kā informēšanas un izvēles principi attiecas uz šādu informāciju?*

2. Atb.: ASV organizācija, kas saskaņā ar “drošības zonu” ir no ES saņēmusi informāciju par darbiniekiem, drīkst to izpaust trešām personām un/vai izmantot to dažādiem mērķiem tikai atbilstīgi informēšanas un izvēles principiem. Piemēram, ja organizācija ir paredzējusi personisko informāciju, kas ir savākta darba attiecību laikā, izmantot mērķiem, kuri nav saistīti ar nodarbinātību, piemēram, tirdzniecības paziņojumiem, ASV organizācijai pirms tam jādod indivīdiem, kurus tas skar, izvēle, ja vien tie jau nav atļāvuši informāciju izmantot šādiem mērķiem. Turklāt šādu izvēli nedrīkst izmantot, lai ierobežotu darba iespējas vai šādus darbiniekus jebkādā veidā sodītu.

Jāpiebilst, ka atsevišķi vispārēji piemērojami nosacījumi attiecībā uz nosūtīšanu no dažām dalībvalstīm var liegt šādu informāciju izmantot citādi pat pēc nosūtīšanas ārpus ES, un šādi nosacījumi ir jāievēro.

Turklāt darba devējiem jādara viss iespējamais, lai ievērotu darbinieku vēlmes attiecībā uz slepenību. Tas var ietvert, piemēram, ierobežotu piekļuvi datiem, atsevišķu datu padarīšanu par anonīmiem un kodu vai pseidonīmu piešķiršanu, ja īstie vārdi nav vajadzīgi konkrētajam pārvaldības mērķim.

Organizācijai nav jāpiemēro informēšanas un izvēles principi, ciktāl un tādu laikposmu, kas ir vajadzīgs, lai nekaitētu organizācijas likumīgajām interesēm, paaugstinot amatā, pieņemot darbā, vai attiecībā uz citiem līdzīgiem lēmumiem par nodarbinātību.

3. Jaut.: *Kā piemēro piekļuves principu?*

3. Atb.: FAQ par piekļuvi sniedz norādījumus par iemesliem, kas var pamatot piekļuves atteikumu vai ierobežojumu attiecībā uz pieprasījumu saistībā ar cilvēkresursiem. Protams, Eiropas Savienības darba devējiem jāievēro vietējie noteikumi un jānodrošina, ka Eiropas Savienības darbiniekiem ir piekļuve šādai informācijai, kā to prasa viņu mītnes valsts tiesību akti, neatkarīgi no datu apstrādes un uzglabāšanas vietas. “Drošības zona” prasa, lai organizācija, kas Amerikas Savienotajās Valstīs šādus datus apstrādā, sadarbotos, sniedzot šādu piekļuvi tieši vai ar ES darba devēja starpniecību.

4. Jaut.: *Kā saskaņā ar “drošības zonas” principiem notiek piemērošana attiecībā uz darbinieku datiem?*

4. Atb.: Ciktāl informāciju izmanto tikai saistībā ar darba attiecībām, atbildīgs par darbinieku datiem pirmkārt ir ES uzņēmums. Tas nozīmē, ka, ja Eiropas darbinieki sūdzas par viņu datu aizsardzības tiesību pārkāpumiem un nav apmierināti ar iekšējās pārbaudes, sūdzības un pārsūdzības procedūru rezultātiem (vai piemērojāmām šķīrējtiesas procedūrām saskaņā ar līgumu ar arodbiedrību), viņi jānosūta uz štata vai valsts datu aizsardzības iestādi vai uz iestādi, kas ir atbildīga par darba jautājumiem, tajā jurisdikcijā, kur darbinieks strādā. Tas ietver arī gadījumus, kad par viņu personas datu pretlikumīgu apstrādi, kas ir notikusi Amerikas Savienotajās Valstīs, ir atbildīga tā ASV organizācija, kura informāciju ir saņēmusi no darba devēja, nevis pats darba devējs, un tādējādi tas nozīmē, ka, iespējams, ir pārkāpti “drošības zonas” principi, nevis valsts tiesību akti, ar kuriem īsteno direktīvu. Tas ir visefektīvākais veids, kā atrisināt bieži sastopamos gadījumus, kad tiesības un pienākumi, kas ir noteikti vietējā darba likumā, darba līgumos un datu aizsardzības likumā, daļēji sakrīt.

Tādēļ ASV organizācijai, kas līdzdarbojas “drošības zonā”, izmanto ES datus par cilvēkresursiem, kuri nosūtīti no Eiropas Savienības saistībā ar darba attiecībām, un vēlas, lai uz šādu nosūtīšanu attiektos “drošības zona”, jāapņemas šādos gadījumos sadarboties ar kompetentajām ES iestādēm izmeklēšanā un ievērot to ieteikumus. Datu aizsardzības iestādes, kas ir piekritis sadarboties šādā veidā, par to paziņo

Eiropas Komisijai un Tirdzniecības ministrijai. Ja ASV organizācija, kas līdzdarbojas “drošības zonā”, vēlas nosūtīt datus par cilvēkresursiem no dalībvalsts, kur datu aizsardzības organizācijas tam nav piekritušas, ir spēkā FAQ 5 noteikumi.

FAQ 10 — 17. pantā noteiktie līgumi

Jaut.: *Vai ir vajadzīgs līgums, neatkarīgi no apstrādātāja līdzdalības “drošības zonā”, ja datus no ES uz Amerikas Savienotajām Valstīm nosūta tika apstrādei?*

Atb.: Jā. Tiem, kas ir atbildīgi par datu apstrādi Eiropas Savienībā, vienmēr ir ieteicams noslēgt līgumu, ja notiek nosūtīšana tikai apstrādei, neatkarīgi no tā, vai apstrādes darbību veic ES vai ārpus tās. Līguma mērķis ir aizsargāt to personu intereses, kas ir atbildīgas par datu apstrādi, t.i., fiziska vai juridiska persona, kura nosaka apstrādes mērķus un līdzekļus un kura ir pilnībā atbildīga par attiecīgā(-o) indivīda(-u) datiem. Tādējādi līgums nosaka, ka jāveic apstrāde un pasākumi, kas vajadzīgi, lai nodrošinātu, ka dati ir aizsargāti.

Tādējādi ASV organizācijai, kas līdzdarbojas “drošības zonā” un saņem personisko informāciju no ES tikai apstrādei, šai informācijai principi nav jāpiemēro, jo atbildīgais par apstrādi ES ir par to atbildīgs attiecībā uz indivīdu saskaņā ar attiecīgajiem ES noteikumiem (kas var būt stingrāki nekā atbilstīgie “drošības zonas” principi).

Tā kā “drošības zonas” dalībnieki nodrošina pienācīgu aizsardzību, līgumiem ar “drošības zonas” dalībniekiem tikai par apstrādi nav vajadzīga iepriekšēja atļauja (vai arī šādu atļauju automātiski piešķir dalībvalstis), kā tas ir vajadzīgs līgumiem ar saņēmējiem, kas nav līdzdalīgi “drošības zonā” un citādi nenodrošina pienācīgu aizsardzību.

FAQ 11 — Strīdu izšķiršana un izpilde

Jaut.: *Kā jāsteno piemērošanas principa strīdu izšķiršanas prasības un kas notiek, ja organizācija principus pastāvīgi neievēro?*

Atb.: Piemērošanas princips nosaka prasības “drošības zonas” piemērošanai. Tas, kā izpildīt šā principa b) punkta prasības, ir izklāstīts jautājumā par pārbaudi (FAQ 7). Šis FAQ 11 attiecas uz a) un c) punktiem, kuros noteikta prasība pēc neatkarīgiem tiesību aizsardzības mehānismiem. Šie mehānismi var būt dažādi, bet tiem jāatbilst piemērošanas principa prasībām. Organizācijas šīs prasības var izpildīt šādi: 1) ievērojot privātajā sektorā izstrādātas slepenības programmas, kuru noteikumus iekļauti “drošības zonas” principi un kas ietver efektīvus tāda veida izpildes mehānismus, kā aprakstīts jautājumā par piemērošanas principu; 2) pakļaujoties juridiskām vai reglamentējošām uzraudzības iestādēm, kas nosaka indivīdu sūdzību izskatīšanu un strīdu izšķiršanu; vai 3) apņemoties sadarboties ar datu aizsardzības iestādēm, kas atrodas Eiropas Savienībā, vai to pilnvarotajiem pārstāvjiem. Šis saraksts ir aptuvenš un nerada ierobežojumus. Privātais sektors var izstrādāt citus mehānismus, lai nodrošinātu piemērošanu, ciktāl tie atbilst piemērošanas principa prasībām un FAQ. Lūdzu ievērojet, ka piemērošanas principa prasības papildina prasības, kas noteiktas principu ievada 3. punktā, ka pašregulējums var būt tiesiski apstrīdams saskaņā ar 5. paragrāfu *Federal Trade Commission Act* vai līdzīgiem likumiem.

Tiesību aizsardzības mehānismi

Pirms izmanto neatkarīgus tiesību aizsardzības mehānismus, patērētāji jārosina iesniegt sūdzības, kas viņiem var rasties par attiecīgo organizāciju. To, vai tiesību aizsardzības mehānisms ir neatkarīgs, dažādos veidos var noskaidrot ar faktiem, piemēram, ar pārredzamu sastāvu un finansēšanu vai ar pierādītiem sasniegumiem.

Kā prasa piemērošanas princips, indivīdiem pieejamai tiesību aizsardzībai jābūt gatavai un viegli pieejamai. Strīdu izšķiršanas iestādēm jāizskata visas sūdzības, kas saņemtas no indivīdiem, ja vien tās nav acīmredzami nepamatotas vai nenozīmīgas. Tas neliedz organizācijai, kas strādā ar tiesību aizsardzības mehānismu, noteikt atbilstības prasības, bet šādām prasībām jābūt pārredzamām un pamatotām (piemēram, lai neiekļautu prasības, kas uz programmu neattiecas vai ir izskatāmas citā iestādē), un tās nedrīkst mazināt apņemšanos izskatīt pamatotas sūdzības. Turklāt ar tiesību aizsardzības mehānismiem indivīdiem jāsniedz pilnīga un viegli pieejama informācija par to, kā darbojas strīdu izšķiršanas procedūra, kad viņi iesniedz sūdzību. Šādai informācijai atbilstīgi “drošības zonas” principiem ⁽¹⁾ jāietver paziņojums par mehānisma slepenības praksi. Tiem arī jāsadarojas tādu līdzekļu izstrādē kā standarta sūdzību veidlapas, lai veicinātu sūdzību atrisināšanas procesu.

Aizsardzības līdzekļi un sankcijas

Visu strīda izšķiršanas iestādes noteikto aizsardzības līdzekļu rezultātā neatbilstība organizācijā jānovērš vai jālabo, ciktāl tas ir iespējams, un jānodrošina, ka turpmāka organizācijas veiktā apstrāde atbilst principiem un ka attiecīgā gadījumā to indivīdu personas datu apstrādi, kas ir iesnieguši sūdzību, pārtrauks. Sankcijām jābūt pietiekami stingrām, lai nodrošinātu, ka organizācija principus ievēro. Vairākas dažādas stingrības pakāpes sankcijas ļaus strīdu izšķiršanas iestādēm pienācīgi reaģēt uz dažādas pakāpes neatbilstību. Sankcijām jāietver gan neatbilstības konstatējumu publicēšana, gan prasība konkrētos apstākļos datus dzēst ⁽²⁾. Citas sankcijas varētu ietvert darbības atļaujas apturēšanu un atņemšanu, atbildību indivīdiem par zaudējumiem, kas radušies neatbilstības rezultātā, un piespiedu izpildi. Privātā sektora strīdu izšķiršanas iestādēm un pašpārvaldes iestādēm par to, ka “drošības zonas” organizācijas neievēro to nolēmumus, jāziņo attiecīgajai kompetentajai valdības iestādei vai tiesām un par to jāpaziņo Tirdzniecības ministrijai (vai tās pārstāvim).

FTC darbība

FTC ir apņēmusies, pirmkārt, pārskatīt pieprasījumus, kas saņemti no organizācijām, kuras pašas reglamentē privātās dzīves aizsardzību, kā piemēram “BBBOnline” un “TRUSTe”, un ES dalībvalstīm, par kurām apgalvo, ka tās neievēro “drošības zonas” principus, lai noteiktu, vai ir pārkāpts FTC Act 5. paragrāfs, kurš tirdzniecībā aizliedz negodīgu vai maldinošu rīcību. Ja FTC secina, ka tai ir pamats uzskatīt, ka 5. paragrāfs ir pārkāpts, tā var jautājumu risināt ar administratīvu rīkojumu par pretlikumīgas darbības pārtraukšanu, vai iesniedzot sūdzību federālajā apgabaltiesā; ja sūdzību apmierina, federālā tiesa taisa nolēmumu ar tādu pašu spēku. FTC var piemērot civiltiesiskas sankcijas par pretlikumīgas darbības pārtraukšanas rīkojuma neievērošanu un var ierosināt civiltiesiskas vai krimināllietas par federālās tiesas nolēmuma neievērošanu. FTC par visām darbībām, ko tā veic, paziņo Tirdzniecības ministrijai. Tirdzniecības ministrija aicina citas valdības iestādes tai ziņot par šādu lietu iznākumiem un citiem nolēmumiem, kas nosaka atbilstību “drošības zonas” principiem.

Pastāvīga neievērošana

Ja organizācija pastāvīgi neievēro principus, tā vairs nav tiesīga saņemt “drošības zonas” priekšrocības. Pastāvīga neievērošana ir tad, ja organizācija, kas ir pati apliecinājusi Tirdzniecības ministrijai (vai tās pārstāvim) principu piemērošanu, atsakās ievērot kādas pašregulatīvas vai valdības iestādes galīgo lēmumu vai ja šāda iestāde konstatē, ka organizācija bieži neievēro principus, ciktāl tās apgalvojums par ievērošanu vairs nav ticams. Šādos gadījumos organizācijai par šādiem faktiem nekavējoties jāinformē Tirdzniecības ministrija (vai tās pārstāvis). Pretējā gadījumā tai piemēro sankcijas saskaņā ar Likumu par nepatiesu ziņu sniegšanu (18 U. S. C. § 1001).

Ministrija (vai tās pārstāvis) publiskajā to organizāciju sarakstā, kas pašas ir apliecinājušas “drošības zonas” principu ievērošanu, norāda visus saņemtos paziņojumus, to, vai tie ir saņemti no pašas organizācijas, no pašpārvaldes iestādes vai no valdības iestādes, par to brīdinot trīsdesmit (30) dienas iepriekš un dodot organizācijai, kura principus neievēro, iespēju atbildēt. Tādējādi Tirdzniecības ministrijas (vai tās pārstāvja) uzturētais publiskais saraksts skaidri parādīs, kurām organizācijām ir nodrošinātas “drošības zonas” priekšrocības un kurām tādu nav.

⁽¹⁾ Strīdu izšķiršanas iestādēm nav obligāti jāievēro piemērošanas principa prasības. Tās var arī atkāpties no principiem, ja, veicot savus konkrētos uzdevumus, tās saskaras ar pretrunīgām saistībām vai skaidrām atļaujām.

⁽²⁾ Strīdu izšķiršanas iestādēm ir rīcības brīvība attiecībā uz apstākļiem, kuros tās šīs sankcijas izmanto. Attiecīgo datu sensitivitāte ir viens faktors, kas jāņem vērā, lemjot, vai dati jādzēš, kā arī vai organizācija informāciju ir ieguvusi, izmantojusi vai izpaudusi pretrunā ar principiem.

Organizācijai, kas piesakās līdzdarboties pašpārvaldes iestādē, lai atkal varētu pretendēt uz “drošības zonu”, šai iestādei jāsniedz pilnīga informācija par tās iepriekšējo līdzdalību “drošības zonā”.

FAQ 12 — Izvēle — Atteikuma laiks

Jaut.: *Vai izvēles princips ļauj individam izdarīt izvēli tikai attiecību sākumā vai jebkurā laikā?*

Atb.: Parasti izvēles principa mērķis ir nodrošināt, ka personisko informāciju izmanto un izpauž tādā veidā, kas atbilst indivīda vēlmēm un izvēlei. Tādējādi indivīdam jābūt iespējai jebkurā laikā liegt (vai izvēlēties) personisko informāciju izmantot tiešai tirgvedībai, ievērojot samērīgus ierobežojumus, ko nosaka organizācija, piemēram, dodot organizācijai laiku atteikumu īstenot. Organizācija var arī prasīt pietiekamu informāciju, lai apstiprinātu tā indivīda identitāti, kas vēlas izmantošanu liegt. Amerikas Savienotās Valstīs indivīdi šo izvēli var realizēt, izmantojot centrālu atteikuma programmu, piemēram, Tiešas tirgvedības asociācijas pasta izvēles dienests. Organizācijām, kas līdzdarbojas Tiešas tirgvedības asociācijas pasta izvēles dienestā jāveicina tā pieejamība patērētājiem, kas nevēlas saņemt komercinformāciju. Jebkurā gadījumā indivīdam šīs izvēles izdarīšanai piedāvā gatavus un viegli pieejamus mehānismus.

Līdzīgi organizācija var izmantot informāciju atsevišķiem tiešas tirgvedības mērķiem, kad nav iespējams pirms informācijas izmantošanas dot indivīdam iespēju izmantošanu liegt, ja tai pašā laikā organizācija nekavējoties (un pēc pieprasījuma vienmēr) dod indivīdam iespēju (bez maksas) atteikties no turpmākas tirgvedības paziņojumu saņemšanas un organizācija ievēro indivīda vēlmes.

FAQ 13 — Ceļojumu informācija

Jaut.: *Kad organizācijām, kas atrodas ārpus ES, var nosūtīt informāciju par aviosabiedrības pasažieru rezervāciju un citu ceļojumu informāciju, piemēram, informāciju par biežiem lidojumiem vai viesnīcas rezervēšanu, kā arī informāciju par īpašām vajadzībām, piemēram, maltītes atbilstīgi reliģiskām prasībām vai fiziska palīdzība?*

Atb.: Šādu informāciju var nosūtīt vairākos gadījumos. Saskaņā ar Direktīvas 26. pantu personas datus var nosūtīt “uz trešo valsti, kas nenodrošina pienācīgu aizsardzības līmeni 25. panta 2. punkta nozīmē”, ja 1) ir jāsniedz patērētāja prasītie pakalpojumi vai jāpilda vienošanās noteikumi, piemēram vienošanās par “biežiem lidojumiem”; vai 2) patērētājs tam ir skaidri piekritis. ASV organizācijas, kas ievēro “drošības zonu”, nodrošina personas datu pienācīgu aizsardzību un tādēļ var no ES saņemt nosūtītos datus, neievērojot šos nosacījumus vai citus nosacījumus, kuri noteikti Direktīvas 26. pantā. Tā kā “drošības zona” ietver īpašus noteikumus attiecībā uz sensitīvu informāciju, šādu informāciju (kas, iespējams, jāvāc, piemēram saistībā ar patērētāja vajadzību pēc fiziskas palīdzības) var iekļaut sūtījumos “drošības zonas” dalībniekiem. Tomēr visos gadījumos organizācijai, kas informāciju nosūta, jāievēro tās ES dalībvalsts tiesību akti, kurā tā darbojas, un tie, cita starpā, var paredzēt īpašus nosacījumus sensitīvu datu apstrādei.

FAQ 14 — Farmaceitiski preparāti un medicīnas produkti

1. Jaut.: *Ja personas datus vāc ES un nosūta uz Amerikas Savienotajām Valstīm farmaceitiskiem pētījumiem un/vai citiem mērķiem, vai ir spēkā dalībvalsts tiesību akti vai “drošības zonas” principi?*

1. Atb.: Dalībvalsts tiesību akti attiecas uz personas datu vākšanu un jebkādu apstrādi, kas notiek pirms nosūtīšanas uz Amerikas Savienotajām Valstīm. “Drošības zonas” principi attiecas uz datiem, tiklīdz tie ir nosūtīti uz Amerikas Savienotajām Valstīm. Dati, ko izmanto farmaceitiskos pētījumos un citiem mērķiem, vajadzības gadījumā jāpadara anonīmi.

2. Jaut.: *Personas dati, kas ir izstrādāti īpašos medicīnas vai farmaceitiskos pētījumos, bieži ir ļoti noderīgi turpmākajā zinātniskajā pētniecībā. Ja personas datus, kas ir iegūti vienam zinātniskam pētījumam nosūta uz “drošības zonas” ASV organizāciju, vai šī organizācija var datus izmantot jaunai zinātniskās pētniecības darbībai?*

2. Atb.: Jā, ja pirms tam ir nodrošināta informēšana un izvēle. Informējot jāsniedz ziņas par visiem turpmākiem īpašiem datu izmantošanas mērķiem, piemēram periodiskai paveiktā darba kontrolei, saistītiem pētījumiem vai tirgvedībai. Saprotams, ka nevar norādīt visus turpmākos datu izmantošanas mērķus, jo jauns pētījuma mērķis var rasties saistībā ar jaunu izpratni par sākotnējiem datiem, jauniem medicīnas atklājumiem un attīstību, kā arī izmaiņām sabiedrības veselības aizsardzībā un reglamentācijā. Tādēļ attiecīgajā gadījumā, informējot, jāsniedz paskaidrojums, ka personas datus var izmantot turpmākos medicīnas un farmaceitiskos pētījumos, kas nav paredzami. Ja izmantošanas veids neatbilst vispārīgajam pētījuma mērķim(-iem), kuram(-iem) dati sākotnēji iegūti vai kuram(-iem) indivīds pēc tam piekritis, tad jāiegūst jauna atļauja.
3. Jaut.: *Kas notiek ar indivīda datiem, ja dalībnieks brīvprātīgi vai pēc sponsora pieprasījuma nolemj pārtraukt dalību klīniskajā izpētē?*
3. Atb.: Dalībnieki var nolemt vai viņus var lūgt pārtraukt piedalīties klīniskajā izpētē jebkurā laikā. Visus datus, kas ir iegūti pirms šīs pārtraukšanas, drīkst turpināt apstrādāt kopā ar citiem datiem, kuri iegūti klīniskās izpētes laikā, tomēr, ja tas dalībniekam bijis skaidri norādīts brīdī, kad viņš piekrita piedalīties.
4. Jaut.: *Farmācijas un medicīnas ierīču uzņēmumiem ir atļauts personiskos datus no ES veiktajiem klīniskajiem pētījumiem sniegt regulatoriem Amerikas Savienotajās Valstīs reglamentējošiem un uzraudzības mērķiem. Vai līdzīga nosūtīšana ir atļauta pusēm, kas nav regulatori, piemēram, uzņēmumiem un citiem pētniekiem?*
4. Atb.: Jā, ievērojot informēšanas un izvēles principus.
5. Jaut.: *Lai nodrošinātu objektivitāti daudzajos klīniskajos pētījumos, dalībniekiem un bieži vien arī izmeklētājiem nevar piešķirt piekļuvi informācijai par to, kā katru dalībnieku ārstē. Tas apdraudētu zinātnisko pētījumu un rezultātu pamatotību. Vai šādu klīnisko pētījumu (saukti par "slēptajiem" pētījumiem) dalībniekiem pētījuma laikā ir piekļuve datiem par ārstēšanu?*
5. Atb.: Nē, šāda piekļuve dalībniekam nav jāsniedz, ja šis ierobežojums izskaidrots, kad dalībnieks iesaistījās izpētē, un ja šādas informācijas izpaušana apdraudētu veikto pētījumu integritāti. Vienošanās par dalību izpētē saskaņā ar šiem nosacījumiem ir pamatota atteikšanās no tiesībām uz piekļuvi. Pēc izpētes slēdziena saņemšanas un rezultātu analīzes dalībniekiem jābūt piekļuvei saviem datiem, ja viņi to prasa. Pirmkārt, to var mēģināt iegūt pie ārsta vai cita veselības aprūpes sniedzēja, kas viņus klīniskās izpētes laikā ārstēja, un tad no sponsorējošā uzņēmuma.
6. Jaut.: *Vai farmācijas vai medicīnas ierīču uzņēmumam ir jāpiemēro "drošības zonas" principi attiecībā uz informēšanu, tālāku nosūtīšanu un piekļuvi, veicot produktu drošības un iedarbīguma uzraudzību, tostarp ziņojot par blakusefektiem un sekojot līdz tādiem pacientiem/subjektiem, kas izmanto konkrētas zāles vai medicīnas ierīces (piem., sirdsdarbības stimulatoru)?*
6. Atb.: Nē, ciktāl principu ievērošana nav pretrunā ar reglamentējošu prasību izpildi. Tas attiecas gan, piemēram, uz veselības aprūpes sniedzēju ziņojumiem farmācijas un medicīnas ierīču uzņēmumiem, gan farmācijas un medicīnas ierīču uzņēmumu ziņojumiem tādām valdības iestādēm kā Pārtikas un zāļu iestāde.
7. Jaut.: *Galvenais izmeklētājs sākotnējos pētījumu datus vienmēr ir īpaši kodējis ar šifru tā, lai neatklātu atsevišķu datu subjektu identitāti. Farmācijas uzņēmumi, kas šādu pētījumu sponsorē, šifru nesaņem. Īpaši šifrētais kods ir tikai pētniekam, lai īpašos apstākļos (piem., ja ir pēc tam vajadzīga medicīniska uzraudzība) viņš/ viņa varētu pētījuma subjektu identificēt. Vai šādi kodētu datu nosūtīšana no ES uz Amerikas Savienotajām Valstīm ir personas datu nosūtīšana, uz kuru attiecas "drošības zonas" principi?*
7. Atb.: Nē. Tā nav tāda personas datu nosūtīšana, uz kuru attiecas principi.

FAQ 15 — Publiskie reģistri un publiski pieejama informācija

Jaut.: *Vai informēšanas, izvēles un tālākas nosūtīšanas principi ir jāpiemēro publisko reģistru informācijai vai publiski pieejamai informācijai?*

Atb.: Informēšanas, izvēles vai tālākas nosūtīšanas principi nav jāpiemēro publisko reģistru informācijai, ja tā nav kopā ar tādu reģistru informāciju, kas nav publiski, un ir ievēroti tie nosacījumu attiecībā uz to izmantošanu, kurus noteikusi attiecīgā kompetentā iestāde.

Parasti informēšanas, izvēles vai tālākas nosūtīšanas principi tāpat nav jāpiemēro publiski pieejamai informācijai, ja vien Eiropas nosūtītājs nenorāda, ka uz šādu informāciju attiecas ierobežojumi, kas prasa organizācijai piemērot principus paredzētajiem izmantošanas veidiem. Organizācijas nebūs atbildīgas par to, kā šādu informāciju izmanto tie, kuri to ir ieguvuši no publicētiem materiāliem.

Ja konstatē, ka organizācija pretrunā principiem ar nodomu ir publiskojusi personisku informāciju, lai tā vai citi varētu izmantot šos izņēmumus, tā vairāk nevarēs pretendēt uz “drošības zonas” priekšrocībām.

III PIELIKUMS

Pārskats par “drošības zonas” īstenošanu

Federālās un štatu pilnvaras attiecībā uz negodīgu un maldinošu rīcību un privātums

Šajā memorandā ir izskaidrotas *Federal Trade Commission (FTC)* pilnvaras saskaņā ar *Federal Trade Commission Act* 5. paragrāfu (15 U. S. C. §§ 41-58 ar grozījumiem), lai vērstos pret tiem, kas neaizsargā personiskās informācijas slepenību saskaņā ar viņu apgalvojumiem un/vai apņemšanos to darīt. Tajā ir arī aprakstīti izņēmumi attiecībā uz šo pilnvarojumu un citu federālo un štata iestāžu tiesības rīkoties, ja *FTC* nav tādu pilnvaru ⁽¹⁾.

FTC pilnvaras attiecībā uz negodīgu vai maldinošu rīcību

Federal Trade Commission Act 5. paragrāfā ir noteikts, ka “negodīga vai maldinoša darbība vai rīcība, ko veic tirdzniecībā vai kas to ietekmē” ir pretlikumīga. [15 U. S. C. § 45(a)(1)] Ar 5. paragrāfu *FTC* ir piešķirtas neierobežotas tiesības šādu darbību un rīcību novērst. [15 U. S. C. § 45(a)(2)] Tādējādi *FTC*, veicot formālu lietas izskatīšanu, drīkst izdot rīkojumu par pretlikumīgas darbības pārtraukšanu, lai pretlikumīgo rīcību novērstu. [15 U. S. C. § 45(b)] Ja tas ir sabiedrības interesēs, *FTC* var arī prasīt ASV apgabaltiesai izdot pagaidu ierobežojošu rīkojumu vai arī pagaidu vai pastāvīgu izpildrakstu. [15 U. S. C. § 53(b)] Ja negodīgas vai maldinošas darbības vai rīcības struktūra ir plaši izplatīta vai ja *FTC* šajā jautājumā jau ir izdevusi rīkojumus par pretlikumīgas darbības pārtraukšanu, tā var izdot administratīvu priekšrakstu, kurā noteikta attiecīgā darbība vai rīcība. [15 U. S. C. § 57a]

Visiem, kas neievēro *FTC* rīkojumu, uzliek administratīvo sodu līdz USD 11 000, un katru pārkāpuma dienu uzskata par atsevišķu pārkāpumu ⁽²⁾. [15 U. S. C. § 45(1)] Tāpat visiem, kas apzināti neievēro *FTC* priekšrakstu, jāmaksā sods USD 11 000 par katru pārkāpumu. [15 U. S. C. § 45(m)] Izpildi var veikt vai nu Tieslietu ministrija vai, ja tā atsaka, tad *FTC*. [15 U. S. C. § 56]

FTC pilnvaras un privātums

Īstenojot savas 5. paragrāfā noteiktās pilnvaras, *FTC* uzskata, ka faktu sagrozišana par to, kāpēc no patērētājiem vāc informāciju un kā informāciju izmantos, ir maldinoša rīcība ⁽³⁾. Piemēram, 1998. gadā *FTC* iesniedza prasību pret *GeoCities* par tās informācijas izpaušanu trešām personām, ko tā bija savākusi savā tīmekļa vietnē bez iepriekšējas atļaujas, lai pēc tam sūtītu savus piedāvājumus, neskatoties uz to, kā tā apgalvoja pretējo ⁽⁴⁾. *FTC* personāls arī ir apstiprinājis, ka personiskas informācijas vākšana no bērniem un šādas informācijas pārdošana un izpaušana bez vecāku piekrišanas visdrīzāk ir negodīga rīcība ⁽⁵⁾.

⁽¹⁾ Šeit mēs neapskatām visus dažādos federālos likumus, kas attiecas uz slepenību īpašā sakarā, štata likumus un kopējos tiesībus aktus, kurus var piemērot. Federālā līmeņa likumi, kas reglamentē personiskās informācijas vākšanu un izmantošanu, cita starpā ietver *Cable Communications Policy Act* (47 U. S. C. § 551), *Driver's Privacy Protection Act* (18 U. S. C. § 2721), *Electronic Communications Privacy Act* (18 U. S. C. § 2701 et seq.), *Electronic Funds Transfer Act* (15 U. S. C. §§ 1693, 1693 m), *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), un *Video Privacy Protection Act* (18 U. S. C. § 2710). Daudzos štatos šajās jomās ir līdzīgi tiesību akti. Skat., piem., *Mass. Gen. Laws ch. 167B, § 16* (kas fināsu iestādēm ļauj trešai personai izpaust klientu finansiāla rakstura informāciju par klientu tikai ar klienta piekrišanu vai attiecīgās tiesas atļauju), *N. Y. Pub. Health Law § 17* (kas ierobežo medicīniska rakstura vai ar garīgo veselību saistītas informācijas izmantošanu un izpaušanu un dod pacientiem tiesību tai piekļūt).

⁽²⁾ Šādas rīcības gadījumā arī Amerikas Savienoto Valstu apgabaltiesa var noteikt obligātu un taisnīgu palīdzību tās novēršanai, kas ir atbilstīga *FTC* rīkojuma izpildei. [15 U. S. C. § 45(1)]

⁽³⁾ “Maldinošu rīcību” definē kā atspoguļojumu, bezdarbību vai darbību, kas materiālā ziņā var maldināt saprātīgus patērētājus.

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

⁽⁵⁾ Skat. personāla vēstuli Mediju izglītības centrs, www.ftc.gov/os/1997/9707/cenmed.htm. Turklāt 1998. gada Likums par bērnu privātās dzīves aizsardzību tieši saistē piešķīt *FTC* īpašas tiesības reglamentēt personiskās informācijas vākšanu no bērniem, ko veic tīmekļa vietņu un tiešsaistes pakalpojumu operatori. Skat. 15 U. S. C. § 6501-6506. Jo īpaši likums prasa, lai tiešsaistes operatori informētu un iegūtu pārbaudāmu vecāku piekrišanu, pirms viņi vāc, izmanto vai izpauž personisko informāciju par bērniem. [Tas pats, § 6502(b)] Likums arī dod vecākiem piekļuves tiesības un tiesības nedot atļauju informācijas turpmākai izmantošanai. [Tas pats.]

FTC priekšsēdētājs Pitofskis (*Pitofsky*) vēstulē Eiropas Komisijas ģenerāldirektoram Džonam Mogam (*John Mogg*) norādīja FTC pilnvaru ierobežojumus, lai aizsargātu privāto dzīvi, ja nav noticis sagrozījums (vai nav nekādu apgalvojumu) par to, kā savākt informāciju izmantos. [FTC priekšsēdētāja Pitofska vēstule Džonam Mogam (1998. gada 23. septembris).] Tomēr uzņēmumiem, kas vēlas saņemt piedāvātās “drošības zonas” priekšrocības, būs jāapliecina, ka tie aizsargās informāciju, kuru tie savāc saskaņā ar noteiktajiem norādījumiem. Tātad, ja uzņēmums apliecina, ka tas aizsargās informācijas slepenību, bet to nedara, tad šāda darbība ir sagrozījums un “maldinoša rīcība” 5. paragrāfa nozīmē.

Tā kā FTC jurisdikcija attiecas arī uz negodīgu vai maldinošu darbību vai rīcību, “ko veic tirdzniecībā vai kas to ietekmē”, FTC nav jurisdikcijas pār personiskas informācijas vākšanu un izmantošanu nekomerciāliem nolūkiem, piemēram, līdzekļu vākšana labdarībai. Skat. Pitofska vēstuli, 3. lpp. Tomēr personiskas informācijas izmantošana jebkādā tirdzniecības darījumā minētajā jurisdikcijā ietilpst. Tādējādi, piemēram, ja darba devējs pārdod sava darbinieka personisko informāciju tiešam tirgotājam, 5. paragrāfs uz šādu darījumu attiecas.

5. paragrāfa izņēmumi

FTC Act 5. paragrāfā ir noteikti tie izņēmumi attiecībā uz FTC pilnvarām pār negodīgu vai maldinošu darbību vai rīcību, kas attiecas uz:

- finanšu iestādēm, to skaitā bankām, krājaizdevu sabiedrībām un kredītsabiedrībām,
- telekomunikāciju uzņēmumiem un starpstatu pārvaldītājiem,
- gaisa pārvadātājiem, un
- fasētājiem un lopu ganāmpulku pārraugiem.

Skat. 15 U. S. C. § 45(a)(2). Turpmāk apskatīsim katru izņēmumu un pašpārvaldes iestādi, kas darbojas FTC vietā.

Finanšu iestādes ⁽¹⁾

Pirmais izņēmums attiecas uz “bankām un krājaizdevu sabiedrībām, kas aprakstītas 18. paragrāfa f) punkta 3. apakšpunktā [15 U. S. C. § 57a(f)(3)]” un “federālajām kredītsabiedrībām, kuras aprakstītas 18. paragrāfa f) punkta 4. apakšpunktā [15 U. S. C. § 57a(f)(4)]” ⁽²⁾. Uz šīm finanšu iestādēm izņēmuma kārtā attiecas noteikumi, ko attiecīgi izdevusi Federālā rezervju padome, Krājaizdevu uzraudzības birojs ⁽³⁾ un Nacionālā kredītsabiedrību administratīvā padome. Skat. 15 U. S. C. § 57a(f). Šīm regulatīvajām iestādēm ir jāparedz noteikumi, kas vajadzīgi, lai novērstu norādīto finanšu iestāžu ⁽⁴⁾ negodīgu un maldinošu rīcību un jāizveido īpaša nodaļa, kura izskatītu patērētāju sūdzības. [15 U. S. C. § 57a(f)(1)]. Visbeidzot, piemērošana izriet no 8. paragrāfa Likumā par noguldījumu federālo apdrošināšanu (12 U. S. C. § 1818) attiecībā uz bankām un krājaizdevu sabiedrībām un 120. un 126. paragrāfa Federālajā kredītsabiedrību likumā — attiecībā uz federālajām kredītsabiedrībām. [15 U. S. C. § 57a(f) (2)-(4)]

Kaut gan apdrošināšanas nozare nav īpaši iekļauta 5. paragrāfa izņēmumu sarakstā, Makkarana-Fergusona likums (15 U. S. C. § 1011 *et seq.*) parasti ļauj apdrošināšanas darījumus reglamentēt katram štatam atsevišķi ⁽⁵⁾. Bez tam,

⁽¹⁾ 1999. gada 12. novembrī Prezidents Klintons parakstot pieņēma *Gramm-Leach-Bliley Act* (Pub. L. 106-102, apkopots 15 U. S. C. § 6801 *et seq.*). Likums ierobežo finanšu iestāžu iespējas izpaust personisko informāciju par saviem klientiem. Likums prasa, lai finanšu iestādes visus klientus, cita starpā, informētu par to slepenības politiku un praksi attiecībā dalīšanos ar personisko informāciju ar saistītajiem uzņēmumiem un nesaistītajiem uzņēmumiem. Likums pilnvaro FTC, federālās banku iestādes un citas iestādes izdot noteikumus, lai īstenotu likumā prasīto privātās dzīves aizsardzību. Iestādes šim nolūkam ir izvekušas ieteicamos noteikumus.

⁽²⁾ Saskaņā ar to šis izņēmums neattiecas uz vērtspapīru nozari. Tādēļ mākleri, tirdzniecības aģenti un citi vērtspapīru nozares darbinieki attiecībā uz negodīgām vai maldinošām darbībām vai rīcību atrodas sakrītošajā *Securities and Exchange Commission* un FTC jurisdikcijā.

⁽³⁾ FTC 5. paragrāfa izņēmums sākotnēji minēts *Federal Home Loan Bank Board*, ko 1989. gada augustā atcēla ar 1989. gada *Financial Institutions Reform, Recovery and Enforcement Act*. Tās funkcijas nodeva *Office of Thrift Supervision*, *Resolution Trust Corporation*, *Federal Deposit Insurance Corporation* un *Housing Finance Board*.

⁽⁴⁾ FTC 5. paragrāfs ne tikai izslēdz finanšu iestādes no FTC jurisdikcijas, bet arī nosaka, ka, ja FTC izdod noteikumus par negodīgu vai maldinošu darbību vai rīcību, 60 dienās finanšu jautājumus reglamentējošajām padomēm jāpieņem līdzīgi noteikumi. Skat. 15 U. S. C. § 57a(f)(1).

⁽⁵⁾ “Uz apdrošināšanas darījumiem un visām tajā iesaistītajām personām attiecas vairāku štatu likumi par šādu darījumu reglamentēšanu vai aplikšanu ar nodokli.” [15 U. S. C. § 1012(a)]

atbilstīgi Makkarana-Fergusona likuma 2. paragrāfa b) punktam, neviens federālais tiesību akts nevar atzīt štata noteikumus par spēkā neesošiem, tos ietekmēt vai aizstāt, "ja vien šāds likums īpaši neattiecas uz apdrošināšanas darījumiem." [15 U. S. C. § 1012(b)] Tomēr *FTC* likuma noteikumi attiecas uz apdrošināšanas nozari, "ja štata tiesību akti šādus darījumus nereglamentē." [Tas pats.] Jāpiebilst, ka Makkarana-Fergusona likums uz štatiem attiecas tikai saistībā ar "apdrošināšanas darījumiem". Tādēļ *FTC* saglabā pārējās pilnvaras attiecībā uz apdrošināšanas sabiedrību negodīgu vai maldinošu rīcību, ja tās nav iesaistītas apdrošināšanas darījumos. Tas, piemēram, var ietvert gadījumu, kad apdrošinātāji pārdod personisko informāciju par saviem apdrošinājuma ņēmējiem tādiem tiešajiem tirgotājiem, kas nepārdod apdrošināšanas pakalpojumus ⁽¹⁾.

Pārvadātāji

Otrais 5. paragrāfa izņēmums attiecas uz tiem pārvadātājiem, uz kuriem "attiecas likumi, kas reglamentē tirdzniecību." [15 U. S. C. § 45(a)(2)] Šajā gadījumā "likumi, kas reglamentē tirdzniecību" attiecas uz *United States Code* 49. sadaļas IV apakšsadaļu un uz 1934. gada *Communications Act* (47 U. S. C. § 151 *et seq.*) (*Communications Act*). Skat. 15 U. S. C. § 44.

U. S. C. 49. sadaļas IV apakšsadaļa (Starpstatu transports) attiecas uz dzelzceļa pārvadātājiem, autopārvadātājiem, jūras pārvadātājiem, mākleriem, kravu ekspeditoriem un piegādātājiem pa cauruļvadiem. [49 U. S. C. § 10101 *et seq.*] Uz šiem dažādajiem pārvadātājiem attiecas *Surface Transportation Board* noteikumi, kas ir Transporta ministrijas neatkarīga iestāde. [49 U. S. C. §§ 10501, 13501, un 15301]. Jebkurā gadījumā pārvadātājam ir aizliegts izpaust informāciju par kravas raksturu, galamērķi un citiem aspektiem, ko varētu izmantot, lai kaitētu nosūtītājam. Skat. 49 U. S. C. §§ 11904, 14908, un 16103. Var konstatēt, ka šie noteikumi attiecas uz informāciju par nosūtītāja kravu un tādējādi neattiecas uz personisko informāciju par nosūtītāju, kas nav saistīta ar attiecīgo sūtījumu.

Kas attiecas uz *Communications Act*, tas paredz, ka "starpstatu un ārzemju vadu un radio sakaru darījumus" reglamentē *Federal Communications Commission* (FCC) Skat. 47 U. S. C. §§ 151 un 152. *Communications Act* attiecas ne tikai uz telekomunikāciju uzņēmumiem, bet arī uz tādiem uzņēmumiem kā televīzijas un radio raidorganizācijām un kabelpakalpojumu sniedzēji, kas nav pārvadātāji. Tādēļ uz šiem uzņēmumiem *FTC Act* 5. paragrāfs neattiecas. Tādējādi *FTC* jurisdikcijā ietilpst šo uzņēmumu pārbaude attiecībā uz negodīgu un maldinošu rīcību, bet FCC atbilstīgajā jurisdikcijā ietilpst tās neatkarīgo pilnvaru izpilde šajā jomā, kā aprakstīts turpmāk.

Saskaņā ar *Communications Act* "katra telekomunikāciju uzņēmuma", tostarp vietējās telefoncentrāles, pienākums ir aizsargāt klientu savrupo datu slepenību ⁽²⁾. [47 U. S. C. § 222(a)]. Papildus šīm vispārīgajām privātās dzīves aizsardzības pilnvarām *Communications Act* tika grozīts ar 1984. gada *Cable Communications Policy Act* (*Cable Act*, 47 U. S. C. § 521 *et seq.*), lai īpaši noteiktu, ka kabeļu operatori aizsargā kabeļsakaru abonentu "personiski identificējamās informācijas" slepenību. [47 U. S. C. § 551 ⁽³⁾] *Cable Act* ierobežo kabeļu operatoru vāktu personisko informāciju un prasa kabeļu operatoram informēt abonentu par savāktās informācijas raksturu un to, kā šo informāciju izmantos. *Cable Act* dod abonentiem tiesības piekļūt informācijai par viņiem un prasa, lai kabeļu operatori šo informāciju iznīcinātu, kad tā vairs nav vajadzīga.

Communications Act pilnvaro FCC šos divus slepenības noteikumus piemērot vai nu pēc savas iniciatīvas vai, atbildot uz ārēju sūdzību ⁽⁴⁾. [47 U. S. C. §§ 205, 403; id. § 208]. Ja FCC konstatē, ka telekomunikāciju uzņēmums (tostarp kabeļu operators) ir pārkāpis 222. vai 551. paragrāfa slepenības noteikumus, tā var veikt trīs

⁽¹⁾ *FTC* jurisdikciju pār apdrošināšanas sabiedrībām ir izmantojusi dažādos gadījumos. Vienā gadījumā *FTC* veica pasākumus pret uzņēmumu par maldinošu reklāmu štatā, kurā tam nebija atļauts veikt darījumus. *FTC* jurisdikciju izmantoja, pamatojoties uz to, ka štata noteikumi nebija spēkā, jo uzņēmums štatam nebija pieejams. Skat. *FTC v. Travelers Health Association*, 362 U. S. 293 (1960).

Kas attiecas uz štatiem, 17 štati ir pieņēmuši *National Association of Insurance Commissioners* (NAIC) sagatavoto "Insurance Information and Privacy Protection Act" paraugu. Likumā ir iekļauti noteikumi par informēšanu, izmantošanu, izpaušanu un piekļuvi. Tāpat gandrīz visi štati ir pieņēmuši NAIC paraugu "Unfair Insurance Practices Act", kas ir īpaši mērķēts uz negodīgu tirdzniecības rīcību apdrošināšanas nozarē.

⁽²⁾ Termins "klienta savrupie dati par tīkla lietojumu" nozīmē klienta informāciju, kas attiecas uz "telekomunikāciju pakalpojumu daudzumu, tehnisko konfigurāciju, veidu, galamērķi un izmantošanas daudzumu" un informāciju par telefona rēķiniem. [47 U. S. C. § 222(f)(1)] Tomēr termins neietver abonentu sarakstu informāciju. [Tas pats]

⁽³⁾ Tiesību aktos "personiski identificējama informācija" nav skaidri definēta.

⁽⁴⁾ Šīs pilnvaras ietver tiesības saņemt kompensāciju par privātuma pārkāpumiem gan saskaņā ar 222. paragrāfu *Communications Act*, kas grozīts ar *Cable Act*, gan — attiecībā uz kabeļsakaru abonentiem — ar *Cable Act* 551. paragrāfu. Skat. arī 47 U. S. C. § 551(f)(3) (civilprasības iesniegšana federālajai apgabaltiesai ir parasts aizsardzības līdzeklis, ko pievādā "papildus citiem likumiem aizsardzības līdzekļiem, kuri kabeļsakaru abonentam ir pieejami").

pamatpasākumus. Pirmkārt, pēc uzklaušanās un pārkāpuma noteikšanas Komisija var pieprasīt uzņēmumam segt finanšu zaudējumus ⁽¹⁾. [47 U. S. C. § 209]. Tad FCC var uzņēmumam izdot rīkojumu nelikumīgo darbību vai bezdarbību pārtraukt. [47 U. S. C. § 205(a)] Tad Komisija var arī pavēlēt uzņēmumam, kas pārkāpj likumu, “nodrošināt atbilstību un ievērot noteikumus vai praksi”, kuru FCC var noteikt. [Tas pats.]

Privātpersonas, kas uzskata, ka telekomunikāciju uzņēmums vai kabeļu operators ir pārkāpis attiecīgos *Communications Act* vai *Cable Act* noteikumus, var vai nu iesniegt sūdzību FCC, vai celt prasību federālajā apgabaltiesā. [47 U. S. C. § 207] Sūdzības iesniedzējam, kas uzvar feredārālā tiesas prāvā pret telekomunikāciju uzņēmumu par klienta savrupo datu neaizsargāšanu saskaņā ar *Communications Act* 222. paragrāfu, var atlīdzināt faktiskos zaudējumus un maksu par advokāta pakalpojumiem. [47 U. S. C. § 206] Sūdzības iesniedzējam, kas cēl prasību, apgalvojot, ka ir noticis privātuma pārkāpums saskaņā ar *Cable Act* 551. paragrāfu, kurš attiecas uz kabeļiem, var atlīdzināt ne tikai faktiskos zaudējumus un maksu par advokāta pakalpojumiem, bet arī zaudējumus ar mērķi sodīt un ar tiesāšanos saistītos izdevumus. [47 U. S. C. § 551(f)]

FCC ir pieņēmusi sīki izstrādātus noteikumus, lai īstenotu 222. paragrāfu. Skat. 47 CFR 64.2001-2009. Noteikumos ir paredzēti īpaši aizsardzības pasākumi, lai novērstu neatļautu piekļuvi klienta savrupiem datiem par tīkla lietojumu. Šie noteikumi prasa telekomunikāciju uzņēmumiem:

- izstrādāt un īstenot programmatūras sistēmas, kas automātiski parāda klienta informēšanas/apstiprinājuma statusu, kad klientu pakalpojumu reģistrs pirmo reizi parādās uz ekrāna;
- uzturēt elektronisku “audita posmu izsekojamību”, lai izsekotu piekļuvi klienta rēķinam, ieskaitot, kad klienta ieraksts ir uzsākts, kurš to ir veicis un kādam nolūkam;
- apmācīt personālu par klientu savrupo datu izmantošanu un izveidot attiecīgās disciplinārlietu izskatīšanas procedūras;
- izveidot uzraudzības un kontroles procedūru, lai nodrošinātu atbilstību, veicot ārēju tirdzniecību; un
- katru gadu apliecināt FCC, kā tie šos noteikumus ievēro.

Gaisa pārvadātāji

FTC Act 5. paragrāfa noteikumi neattiecas arī uz ASV un ārzemju gaisa pārvadātājiem, uz kuriem attiecas 1958. gada *Federal Aviation Act* [Federālais aviācijas likums]. Skat. 15 U. S. C. § 45(a)(2). Tas ietver visus, kas veic starpstatu vai ārzemju preču, pasažieru vai pasta pārvadājumus ar lidmašīnu. Skat. 49 U. S. C. § 40102. Gaisa pārvadātāji ir Transporta ministrijas pakļautībā. Šajā sakarā transporta ministrs ir pilnvarots veikt pasākumus, lai “novērstu negodīgu, kaitniecisku vai konkurenci traucējošu rīcību gaisa transporta jomā.” [49 U. S. C. § 40101(a)(9)] Ja tas ir sabiedrības interesēs, transporta ministrs var pārbaudīt, vai ASV vai ārzemju gaisa pārvadātājs vai biļešu pārdevējs ir iesaistīts negodīgā vai maldinošā rīcībā. [49 U. S. C. § 41712] Pēc uzklaušanās transporta ministrs var izdot rīkojumu pretlikumīgo darbību pārtraukt. [Tas pats] Cik zināms, transporta ministrs šo pilnvarojumu nav izmantojis jautājumā par aviosabiedrību klientu personiskās informācijas slepenības aizsardzību ⁽²⁾.

Ir divi noteikumi, kas aizsargā personiskās informācijas slepenību un kas atsevišķos gadījumos attiecas uz gaisa pārvadātājiem. Pirmkārt, *Federal Aviation Act* aizsargā pilota amata kandidātu privāto dzīvi. Skat. 49 U. S. C. § 44936(f). Lai gan tas ļauj gaisa pārvadātājiem iegūt informāciju par kandidāta nodarbinātību, likums dod kandidātam tiesības būt informētam, ka šāda informācija ir pieprasīta, dot piekrišanu pieprasījumam, labot neprecizātes un informāciju atklāt tikai tiem, kas pieņem lēmumu par pieņemšanu darbā. Otrkārt, Transporta ministrijas noteikumi prasa, lai informāciju par pasažieriem, kas savāktas valdības vajadzībām, gaisa katastrofas gadījumā “turētu slepenībā un izpaustu tikai ASV Valsts Departamentam, *National Transportation Board* (pēc NTSB pieprasījuma) un ASV Transporta ministrijai.” [14 CFR 243. daļa, § 243.9(c) (pievienots ar 63 FR 8258)]

⁽¹⁾ Tomēr tas, ka sūdzības iesniedzējam nav nodarīts tiešs kaitējums, nav pamats sūdzības noraidīšanai. [47 U. S. C. § 208(a)]

⁽²⁾ Ir saprotams, ka pašlaik nozarē tiek daudz darīts, lai risinātu jautājumu par privātās dzīves aizsardzību. Nozares pārstāvji ir apsprieduši ierosinātos “drošības zonas” principus un to iespējamo piemērošanu gaisa pārvadātājiem. Apspriedē bija iekļauts priekšlikums pieņemt nozares slepenības politiku, un lai uzņēmumi, kas to ievēro, pakļautos Transporta ministrijas pilnvarām.

Fasētāji un lopu ganāmpulku pārraugi

Ņemot vērā 1921. gada *Packers and Stockyards Act* (7 U. S. C. § 181 *et seq.*), likums aizliedz “fasētājiem, kas strādā ar lauksaimniecības dzīvniekiem, gaļu, gaļas pārtikas produktiem vai negataviem lauksaimniecības dzīvnieku produktiem, un dzīvu mājputnu tirgotājiem attiecībā uz dzīvīm mājputniem iesaistīties vai izmantot negodīgu, nepamatoti diskriminējošu vai maldinošu rīcību vai paņēmieni.” [7 U. S. C. § 192(a); skat. arī 7 U. S. C. § 213(a) (kas aizliedz “negodīgu, nepamatoti diskriminējošu vai maldinošu rīcību vai paņēmienus” saistībā ar lauksaimniecības dzīvniekiem)] Lauksaimniecības ministra galvenais pienākums ir panākt šo noteikumu izpildi, bet FTC jurisdikcijā paliek mazumtirdzniecības darījumi un darījumi saistībā ar mājputnu nozari. [7 U. S. C. § 227(b)(2)]

Nav skaidrs, vai lauksaimniecības ministrs to, ka fasētājs vai lopu ganāmpulku pārraugš neaizsargā personu privāto dzīvi saskaņā ar norādīto politiku, interpretēs kā “maldinošu” darbību saskaņā ar *Packers and Stockyards Act*. Tomēr 5. paragrāfa izņēmumi attiecas uz personām, personālsabiedrībām vai korporācijām tikai tad, ja “uz tiem attiecas *Packers and Stockyards Act*.” Tādēļ, ja jautājums par personu privātās dzīves aizsardzību nav iekļauts *Packers and Stockyards Act*, 5. paragrāfa izņēmumu var arī nepiemērot, un šajā ziņā fasētāji un lopu ganāmpulku pārraugi būtu FTC pakļautībā.

Štatu pilnvaras attiecībā uz “negodīgu un maldinošu rīcību”

Saskaņā ar FTC personāla sagatavoto analīzi “lai novērstu negodīgu vai maldinošu rīcību tirdzniecībā, visi 50 štati, kā arī Kolumbijas, Agaņas, Puertoriko apgabali un ASV Virdžīnu salas ir ieviesuši likumus, kas ir aptuveni līdzīgi *Federal Trade Commission Act* (“FTCA”). [FTC informatīvā lapa, publicēta “*Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation*”, 59 Tul. L. Rev. 427 (1984).] Jebkurā gadījumā izpildiestādei ir tiesības “veikt izmeklēšanu, izmantojot tiesas pavēstes jeb uzaicinājumus ierasties tiesā, iegūt pierādījumus par brīvprātīgu atbilstību, izdot rīkojumus par pretlikumīgas darbības aizliegšanu vai iegūt tiesas izpildrakstus, ar kuriem novērš negodīgu, ļaunprātīgu vai maldinošu rīcību tirdzniecībā. [Tas pats.] 46 jurisdikcijās ar likumu ir atļauts iesniegt privātas prasības par faktisku, dubultu, trīskāršu zaudējumu atlīdzināšanu vai par zaudējumu atlīdzināšanu ar mērķi sodīt un dažos gadījumos — prasības atlīdzināt samaksu par advokāta pakalpojumiem. [Tas pats].”

Piemēram, Floridas *Deceptive and Unfair Trade Practices Act* ļauj ģenrālprokuroram izmeklēt un iesniegt civilprasības par “negodīgiem konkurences paņēmieniem, negodīgu, ļaunprātīgu vai maldinošu rīcību tirdzniecībā”, ieskaitot nepatiesu vai maldinošu reklāmu, maldinošas franšīzes vai uzņēmējdarbības iespējas, krāpniecisku tirdzniecību pa telefonu un piramīdshēmas. Skat. arī N. Y. *General Business Law* § 349 (kas aizliedz negodīgu darbību un maldinošu rīcību uzņēmējdarbībā).

National Association of Attorneys General (NAAG) veiktā izpēte šos rezultātus apstiprina. No 43 štatiem, kas atbildēja, visos ir tā sauktie “mini-FTC” likumi vai citi likumi, kas paredz pielīdzināmu aizsardzību. Tāpat saskaņā ar NAAG pētījumu 39 štati norādīja, ka tiem ir pilnvaras uzklaut nerezidentu sūdzības. Attiecībā tieši uz klientu privātās dzīves aizsardzību 37 štati no 41, kas atbildēja, norādīja, ka tie atbild uz sūdzībām, kurās apgalvots, ka to jurisdikcijā esošs uzņēmums neievēro slepenības politiku, ko tas pats ir izsludinājis.

IV PIELIKUMS

Kaitējuma atlīdzināšana par privātās dzīves aizskārumiem, tiesiskas atļaujas, apvienošanās un pārņemšana ASV tiesību aktos

Šī ir atbilde uz Eiropas Komisijas pieprasījumu izskaidrot ASV tiesību aktus attiecībā uz a) prasībām atlīdzināt zaudējumus par privātās dzīves aizskārumiem, b) ASV tiesību aktos dotām “skaidrām atļaujām” izmantot personisko informāciju tādā veidā, kas ir pretrunā ar “drošības zonas” principiem, un c) to, kā apvienošanās un pārņemšana ietekmē atbilstīgi “drošības zonai” uzņemtās saistības.

A. Kaitējuma atlīdzināšana par privātās dzīves aizskārumiem

Atkarībā no attiecīgajiem apstākļiem, “drošības zonas” principu neievērošana varētu izraisīt vairāku civilprasību iesniegšanu. Jo īpaši “drošības zonas” organizācijas varētu saukt pie atbildības par sagrozījumu vai pašu noteiktās slepenības politikas neievērošanu. Saskaņā ar kopējiem tiesību aktiem ir iespējami arī privāti iemesli iesniegt prasību atlīdzināt kaitējumu par privātās dzīves aizskārumiem. Daudzos federālajos vai štatu likumos par privātās dzīves aizsardzību ir arī noteikta atbildība par kaitējumu, ko izraisījuši privātpersonu pārkāpumi.

Tiesības uz kaitējuma atlīdzināšanu par personu privātās dzīves aizskārumiem ASV paražu tiesībās ir vispārārtītas.

Personiskās informācijas izmantošana tādā veidā, kas ir pretrunā ar “drošības zonas” principiem, saskaņā ar dažādām tiesību teorijām var būt par pamatu juridiskajai atbildībai. Piemēram, gan atbildīgais par datu apstrādi nosūtītājvalstī, gan individuāli, kurus tas skar, var iesūdzēt “drošības zonas” organizāciju, kas nepilda savas “drošības zonas” saistības, par sagrozījumu. Saskaņā ar *Restatement of the Law, Second, Torts* ⁽¹⁾:

To, kurš krāpnieciski sagroza faktus, viedokli, nodomu vai likumu, lai liktu kādam citam, uzskatot šo informāciju par patiesu, rīkoties vai atturēties no kādas darbības, ir saucams pie atbildības par finansiālajiem zaudējumiem, ko tas nodarījis sakarā ar atvainojamu maldību.

[*Restatement*, § 525] Sagrozījums ir “krāpniecisks”, ja tas ir veikts, zinot vai pieļaujot, ka kas ir nepatiess. [Tas pats, § 526] Parasti visi, ko tas, kurš ir veicis krāpniecisku sagrozījumu, ir paredzējis apkrāpt vai kas pēc viņa domām varētu šim sagrozījumam ticēt, var saukt viņu pie atbildības par finansiālajiem zaudējumiem, kuri viņiem tā rezultātā var rasties. [Tas pats, 531] Bez tam to pusi, kas otrai pusei ir veikusi krāpniecisku sagrozījumu, var saukt pie atbildības trešā puse, ja civiltiesību pārkāpējs ir paredzējis vai domā, ka sagrozījumu varētu veikt atkārtoti attiecībā pret trešo personu. [Tas pats, § 533]

Saistībā ar “drošības zonu” attiecīgais atspoguļojums ir organizācijas publiskais apliecinājums, ka tā stingri ievēros “drošības zonas” principus. Pēc šādu saistību uzņemšanās apzināta principu neievērošana var būt par pamatu prasībai par sagrozījumu tiem, kas šādu sagrozījumu uzskatījuši par patiesu. Tā kā apņemšanās stingri ievērot principus ir izteikta plašai sabiedrībai, indivīdiem, kas ir šīs informācijas subjekti, un atbildīgajam par datu apstrādi Eiropā, kurš personisko informāciju nosūta uz ASV organizāciju, var būt visas iespējas iesūdzēt ASV organizāciju par sagrozījumu ⁽²⁾. Turklāt ASV organizācija viņu priekšā ir atbildīga par “ilgstošu sagrozīšanu” tikmēr, kamēr viņi faktu sagrozījumu uzskata par patiesu, radot sev kaitējumu. [*Restatement*, § 535]

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

⁽²⁾ Tā tas varētu būt, piemēram, ja indivīdi, dodot atbildīgajam par datu apstrādi piekrišanu nosūtīt viņu personisko informāciju uz Amerikas Savienotajām Valstīm, ir palāvušies uz ASV organizācijas “drošības zonas” apņemšanos.

Tiem, kuri krāpniecisku sagrozījumu ir uzskatījuši par patiesu, ir tiesības saņemt kaitējuma atlīdzību. [Saskaņā ar *Restatement*.]

Krāpnieciska sagrozījuma subjekts ir tiesīgs saņemt atlīdzību par kaitējumu, kas viņam ir radies krāpšanas darbības dēļ un kas ir finansiāli zaudējumi, un ja krāpšanas juridiskais pamats ir sagrozījums.

[*Restatement*, § 549]. Pieļaujamā kaitējuma atlīdzināšana ietver faktiskus finansiālus zaudējumus, kā arī “neiegūto peļņu” no komercdarbības. [Tas pats]; skat., piem., *Boling v. Tennessee State Bank*, 890 S. W.2d 32 (1994) (bankai bija jāmaksā aizdevumaņēmējiem USD 14 825, lai atlīdzinātu zaudējumus par aizdevumaņēmēju personiskās informācijas un uzņēmējdarbības plānu izpaušanu bankas prezidentam, kuram bijis interešu konflikts).]

Tā kā krāpnieciska sagrozījuma priekšnoteikums ir vai nu zināšana, vai vismaz uzskats, ka sagrozījums ir nepatiess, var saukt pie atbildības arī par sagrozījumu aiz neuzmanības. Saskaņā ar *Restatement*, visus, kas uzņēmējdarbības, profesionālās darbības vai darba attiecību vai finanšu darījuma laikā ir izteikuši nepatiesu apgalvojumu, var saukt pie atbildības, ja “nav veiktas samērīgas pūles vai nav īstenota kompetence, lai informāciju iegūtu vai paziņotu.” [*Restatement*, § 552(1)] Pretēji krāpnieciskiem sagrozījumiem par sagrozījumu aiz neuzmanības atlīdzina finansiālus zaudējumus. [Tas pats, § 552B (1)]

Piemēram, kādā nesenā lietā Konektikukas Augstākā Tiesa nolēma, ka ir tas, ka kāds elektroapgādes uzņēmums nepareizi izpaušis ziņas par klientu maksājumu datiem valsts kredītiestādēm, ir pietiekams pamats iesniegt prasību par sagrozījumu. Skat. *Brouillard v. United Illuminating Co.*, 1999 Conn. Super. LEXIS 1754. Šajā lietā prasītājam atteica izsniegt kredītu, jo atbildētājs paziņoja, ka maksājumi, kas nav saņemti trīsdesmit dienās pēc rēķina izsniegšanas, ir novēloti. Prasītājs apgalvoja, ka viņš nav bijis informēts par šādu politiku, kad viņš pie atbildētāja atvēra iedzīvotāju elektropakalpojumu rēķinu. Tiesa nolēma, ka “prasība par nolaidīgu sagrozījumu var būt balstīta uz atbildētāja klusēšanu, kad viņa pienākums ir runāt.” Šī lieta parāda arī, ka “krāpniecisks nodoms” nav vienmēr pamatojums prasībai par sagrozījumu aiz neuzmanības. Tādējādi ASV organizāciju, kas aiz neuzmanības pilnībā neizpauž, kā tā izmantos personisko informāciju, kura saņemta saskaņā ar “drošības zonu”, var saukt pie atbildības par sagrozījumu.

Ciktāl “drošības zonas” principu neievērošana ietver personiskās informācijas nepareizu izmantošanu, tā var būt par pamatu datu subjekta prasībai, lai privātās dzīves aizsākumu novērstu saskaņā ar paražu tiesībām civiltiesību jomā. Amerikas tiesībās jau sen ir ietverti zināmi iemesli, kāpēc var iesniegt prasību par privātās dzīves aizskaršanu. 1905. gada lietā ⁽¹⁾ Džordžijas Augstākā Tiesa atzina tiesības uz privāto dzīvi, pamatojoties uz to, ka dabiskās tiesības un paražu tiesības paredz apmierināt tās privātpersonas prasību, kuras fotogrāfiju dzīvības apdrošināšanas sabiedrība, bez viņa piekrišanas vai ziņas bija izmantojusi reklāmā. Uzsverot tagad jau pazīstamās tēmas Amerikas tiesu praksē par privātās dzīves aizsardzību, tiesa atzina, ka fotogrāfijas izmantošana bija “jaunprātīga”, “negodīga” un varēja “prasītāju padarīt par izsmieklu visas pasaules priekšā.” ⁽²⁾ Lēmuma pamatojums Peivsiča lietā ar nelielām izmaiņām ir kļuvis par pamatprincipu Amerikas tiesu praksei šajā jautājumā. Štatu tiesas ir konsekventi atzinušas prasības privātās dzīves aizsākumu jomā par pamatotām, un vismaz 48 štati pašreiz juridiski atzīst atsevišķus šādu prasību pamatojumus. ⁽³⁾ Turklāt vismaz 12 štatos ir konstitucionāli noteikumi, kuri aizsargā pilsoņu tiesības uz neuzmāksanos ⁽⁴⁾, kas dažos gadījumos var attiekties arī uz aizsardzību pret nevalstisku struktūrvienību uzmāksanos. Skat., piem., *Hill v. NCAA*, 865 P.2d 633 (Ca. 1994); skat. arī *S. Ginder, Lost and Found in Cyberspace: Informational Privacy in the age of the Internet*, 34 S. D. L. Rev. 1153 (1997) (“Dažu štatu konstitūcija ietver privātās dzīves aizsardzības pasākumus, kas pārsniedz ASV Konstitūcijā noteikto privātās dzīves aizsardzību. Aļaskas, Arizonas, Kalifornijas, Floridas, Havaju salu, Ilinoisas, Luiziānas, Montanas, Dienvidkarolīnas un Vašingtonas štatā ir plašāka privātās dzīves aizsardzība.”)

Second Restatement of Torts ir dots oficiāls pārskats par tiesībām šajā jomā. Atspoguļojot parasto tiesu praksi, *Restatement* ir paskaidrots, ka “tiesības uz privāto dzīvi” ietver četrus skaidrus iemeslus prasības iesniegšanai par civiltiesību pārkāpumu. Skat. *Restatement*, § 652A. Pirmkārt, prasību par “vienatnības traucēšanu” var vērst pret atbildētāju, kas ar nodomu fiziski vai kā citādi traucē cita nošķirtību vai vienatnību, vai arī viņa privātās lietas ⁽⁵⁾. Otrkārt, var ierosināt

⁽¹⁾ *Pavesich v. New England Life Ins. Co.*, 50 S. E. 68 (Ga. 1905).

⁽²⁾ Tas pats, 69.

⁽³⁾ Elektroniskas meklēšanas rezultātā *Westlaw* datu bāzē, sākot ar 1995. gadu, tika atrasti 2 703 paziņoti tādi civilprasību iesniegšanas gadījumi štatu tiesās, kuri attiecas uz “privātumu”.

⁽⁴⁾ Skat., piem., Aļaskas štata konstitūcijas 1. panta 22. paragrāfu; Arizonas štata konstitūcijas 2. panta 8. paragrāfu; Kalifornijas štata konstitūcijas 1. panta 1. paragrāfu; Floridas štata konstitūcijas 1. panta 23. paragrāfu; Havaju salu konstitūcijas 1. panta 5. paragrāfu; Ilinoisas štata konstitūcijas 1. panta 6. paragrāfu; Luiziānas štata konstitūcijas 1. panta, 5. paragrāfu; Montanas štata konstitūcijas 2. panta, 10. paragrāfu; Ņujorkas štata konstitūcijas 1. panta 12. paragrāfu; Pensilvānijas štata konstitūcijas 1. panta 1. paragrāfu; Dienvidkarolīnas štata konstitūcijas 1. panta 10. paragrāfu un Vašingtonas štata konstitūcijas 1. panta 7. paragrāfu.

⁽⁵⁾ Tas pats, 28. nodaļa, 652. B paragrāfs.

lietu par “nelikumīgu tiesību piesavināšanos”, ja kāds pieņem cita vārdu vai līdzību, lai to izmantotu savām vajadzībām vai lai gūtu labumu ⁽¹⁾. Treškārt, var iesūdzēt tiesā par “privātu fakta publicēšanu”, ja publicētā materiāla raksturs attiecīgajai personai ir ļoti aizskarošs un būtiski neskar sabiedrību ⁽²⁾. Visbeidzot, prasība par “publisku goda un cieņas aizskaršanu” ir pamatota, ja atbildētājs apzināti vai aiz neuzmanības kādu publiski apmelo, kas attiecīgajai personai var būt ļoti aizskaroši ⁽³⁾.

Saistībā ar “drošības zonu” “vienatnības traucēšana” varētu ietvert neatļautu personiskās informācijas vākšanu, bet personiskās informācijas neatļautu izmantošana varētu būt pamats prasībai par “nelikumīgu tiesību piesavināšanos”. Līdzīgi neprecīzas personiskās informācijas izpaušana varētu būt pamats civilprasībai par “publisku goda un cieņas aizskaršanu”, ja informācija attiecīgo personu ir ļoti aizskaroša. Visbeidzot, privātās dzīves aizskaršana saistībā ar sensitīvas personiskās informācijas publicēšanu vai izpaušanu varētu būt pamats prasībai par “privātu fakta publicēšanu”. (Ilustratīvu lietu piemērus skatīt turpmāk).

Saistībā ar kaitējuma atlīdzināšanu privātās dzīves aizskaršanas gadījumā aizskartajai pusei ir tiesības saņemt atlīdzību par:

- a) kaitējumu, kas nodarīts viņa privātajai dzīvei aizskārums dēļ;
- b) pierādītu morālo kaitējumu, kas parasti rodas šāda aizskārums dēļ; un
- c) īpašiem zaudējumiem, kuru juridiskais pamats ir aizskārums.

[*Restatement*, § 652H] Ņemot vērā deliktu tiesību parasto piemērojamību un daudzos prasību pamatojumus, kas ietver dažādus privātās dzīves aspektus, tiem, kuru privātā dzīve ir aizskarta sakarā ar “drošības zonas” principu neievērošanu, varētu atlīdzināt finansiālus zaudējumus.

Štatu tiesās ir ļoti daudz lietu, kuras ir par privātās dzīves aizskaršanu līdzīgās situācijās. Piemēram, lietā *Ex Parte AmSouth Bancorporation et al.*, 717 So.2d 357 bija kolektīva sūdzība, kurā apgalvots, ka atbildētājs “ļauņprātīgi izmantoja noguldītāju uzticēšanos bankai, izpaužot konfidencialu informāciju par bankas noguldītājiem un viņu rēķiniem”, lai saistīta banka varētu pārdot kopfondus un citus ieguldījumus. Šādos gadījumos bieži vien nosaka kaitējumu atlīdzību. Lietā *Vassiliades v. Garfinckel's, Brooks Bros.*, 492 A.2d 580 (D. C. App. 1985) apelācijas tiesa atcēla zemākas tiesas spriedumu un apmierināja prasību, ka prasītāja fotogrāfijas “pirms” un “pēc” plastiskās operācijas izmantošana demonstrācijai lielveikalā ir privātās dzīves aizskaršana, publicējot privātus faktus. Lietā *Candebat v. Flanagan*, 487 So.2d 207 (Miss. 1986) atbildētājs — apdrošināšanas sabiedrība bija reklāmas kampaņā izmantojusi negadījumu, kurā prasītāja sieva bija guvusi smagus miesas bojājumus. Prasītājs iesniedza prasību par privātās dzīves aizskaršanu. Tiesa nolēma, ka prasītājam jāatlīdzina kaitējums par emocionālajām ciešanām un nelikumīgu tiesību piesavināšanos. Prasības par nelikumīgu tiesību piesavināšanos var iesniegt pat tad, ja prasītājs pats nav slavens. Skat., piem., *Staruski v. Continental Telephone Co.*, 154 Vt. 568 (1990) (atbildētājs guva komerciālu labumu, izmantotot darbinieka vārdu un fotogrāfiju laikraksta reklamā). Lietā *Pulla v. Amoco Oil Co.*, 882 F. Supp. 836 (S. D. Iowa 1995) darba devējs aizskāra prasītāja — darbinieka nošķirtību, liekot citam darbiniekam izpētīt viņa kredītkartes informāciju, lai pārbaudītu viņa neierašanos darbā slimības dēļ. Tiesa atbalstīja zvērināto tiesas lēmumu piešķirt USD 2 par faktiskajiem zaudējumiem un USD 500 000, lai atlīdzinātu zaudējumus ar mērķi sodīt. Kādu citu darba devēju sauca pie atbildības par raksta publicēšanu uzņēmuma laikrakstā par kādu darbinieku, ko atlaida no darba par savu nodarbinātības datu iespējamu falsifikāciju. Skat. *Zinda v. Louisiana-Pacific Corp.*, 140 Wis.2d 277 (Wis. App. 1987). Privāta jautājuma publicēšana rakstā aizskāra prasītāja privāto dzīvi, jo laikraksts bija pieejams visā apdzīvotajā vietā. Visbeidzot, kādu koledžu, kas studentiem veica HIV testu, bet apgalvoja, ka asins analīze ir masaliņu pārbaudei, sauca pie atbildības par nošķirtības aizskaršanu. Skat. *Doe v. High-Tech Institute, Inc.*, 972 P.2d 1060 (Colo. App. 1998). (Par citām ziņotām lietām skatīt *Restatement*, § 652H, Appendix.)

Amerikas Savienotās Valstis bieži kritizē par pārmērīgu tiesāšanos, bet tas arī nozīmē, ka indivīdi ne tikai var, bet arī tiešām izmanto tiesisku aizsardzību, ja viņi uzskata, ka pret viņiem ir izdarīts pārkāpums. Daudzi ASV tiesību sistēmas

⁽¹⁾ Tas pats, 28. nodaļa, 652. C paragrāfs.

⁽²⁾ Tas pats, 28. nodaļa, 652. D paragrāfs.

⁽³⁾ Tas pats, 28. nodaļa, 652. E paragrāfs.

aspekti gan individuālajiem, gan kolektīvajiem prasītājiem vienkāršo prasības celšanu. Juristu apvienība, kas ir salīdzinoši lielāka nekā citās valstīs, padara profesionālu pārstāvniecību viegli pieejamu. Prasītāja aizstāvis, kas pārstāv indivīdus civilprasībās, parasti strādā par samaksu atkarībā no gadījuma, un tas ļauj vērsties pēc palīdzības pat nabadzīgiem vai maznodrošinātiem prasītājiem. Tas norāda uz svarīgu faktu — Amerikas Savienotajās Valstīs parasti katra puse sedz izmaksas par savu advokātu un citas izmaksas. Turpretim Eiropā parasti zaudētājam pusei jāatlīdzina otras puses izmaksas. Nesalīdzinot abu sistēmu priekšrocības un trūkumus, ASV sistēmā ir mazāka iespējamība, ka indivīdi, kas zaudējuma gadījumā nevarētu segt abu pušu izmaksas, neiesniegs pamatotas prasības.

Indivīdi var iesniegt prasību par zaudējumu atlīdzību arī tad, ja prasība ir salīdzinoši neliela. Lielākajā daļā, vai pat visās ASV jurisdikcijās ir tiesas nelielām prasībām, kas nodrošina vienkāršotas un lētākas procedūras attiecībā uz strīdiem, kuru apjoms nesasniedz likumos noteiktos apmērus⁽¹⁾. Iespējamā zaudējumu atlīdzība ar mērķi sodīt sniedz indivīdiem, kuriem ir nodarīts neliels tiešs kaitējums, finansiālu atlīdzību prasības iesniegšanai par nelikumīgu rīcību. Visbeidzot indivīdi, kuru tiesības ir aizskartas vienādā veidā, var apvienot savus resursus un prasības, lai iesniegtu tiesai kolektīvu prasību.

Labs piemērs tam, ka indivīdi var iesniegt prasību tiesā, lai saņemtu zaudējumu atlīdzību, ir vēl neizlemtā tiesas prāva pret *Amazon.com* par privātās dzīves aizskaršanu. Pret *Amazon.com*, kas ir liels tiešsaistes mazumtirgotājs, ir iesniegta kolektīva prasība, kurā prasītāji apgalvo, ka viņus neinformēja un ka viņi nav devuši savu piekrišanu personiskās informācijas vākšanai par viņiem, kad viņi izmantoja datorprogrammu, kas pieder *Amazon*, ar nosaukumu "*Alexa*". Šajā lietā prasītāji apgalvo, ka ir pārkāpts *Computer Fraud and Abuse Act*, nelikumīgi piekļūstot viņu glabātajiem ziņojumiem, un *Electronic Communications Privacy Act*, nelikumīgi pārtverot viņu elektroniskos un vada ziņojumus. Viņi apgalvo arī, ka saskaņā ar paražu tiesībām ir noticis privātās dzīves aizskārums. Tas izriet no prasības pieteikuma, ko decembrī ir iesniedzis Interneta drošības eksperts. Prasība ir par zaudējumu atlīdzību USD 1 000 apmērā katram prasītājam, kā arī advokāta izmaksu segšanu un likumpārkāpumu rezultātā iegūtas peļņas atmaksāšanu. Ņemot vērā to, ka prasītāju skaits var būt miljonos, zaudējumu kopējais apmērs varētu būt miljoni dolāru. Arī *FTC* izmeklē šīs sūdzības.

Federālie un štata tiesību akti attiecībā uz privātās dzīves aizsardzību bieži ļauj iesniegt privātas prasības par finansiālu zaudējumu atlīdzību.

Par "drošības zonas" principu neievērošanu var ne tikai saukt pie atbildības saskaņā ar deliktu tiesībām, bet tas var arī būt pārkāpums saskaņā ar kādu no daudzajiem federālajiem un štata likumiem par privāto dzīvi. Daudzi no šiem likumiem, kas attiecas uz personiskās informācijas apstrādi gan valsts, gan privātajā sektorā, ļauj indivīdiem iesniegt prasību, ja notiek pārkāpumi. Piemēram,

1986. gada Electronic Communications Privacy Act, *ECPA* aizliedz neatļautu mobilo telefonu zvanu un sūtījumu no datora un datoru savstarpēju pārtveršanu. Pārkāpumi var izraisīt civiltiesisko atbildību ne mazāk kā USD 100 apmērā par katru pārkāpuma dienu. *ECPA* aizsardzība attiecas arī uz neatļautu piekļuvi uzglabātiem elektroniskiem paziņojumiem un to izpaušanu. Likumpārkāpējiem ir jāatlīdzina nodarītais kaitējums vai viņiem atsavina peļņu, kas gūta pārkāpuma rezultātā.

1996. gada Telecommunications Act. Saskaņā ar 702. paragrāfu klienta savrupos datus par tīkla lietojumu drīkst izmantot tikai, lai sniegtu telekomunikāciju pakalpojumus. Pakalpojuma abonenti var vai nu iesniegt prasību *Federal Communications Commission*, vai iesniegt prasību federālajā apgabaltiesā, lai panāktu kaitējuma un advokāta maksu atlīdzināšanu.

1996. gada Consumer Credit Reporting Reform Act. 1996. gada likums grozīja 1970. gada *Fair Credit Reporting Act* (*FCRA*), lai noteiktu kredītu uzraudzības subjektu labāku informēšanu un piekļuves tiesības. *Reform Act* noteica arī jaunus ierobežojumus attiecībā uz patērētāja kredītinformācijas tālākajiem pārdevējiem. Patērētāji, pret kuriem noticis pārkāpums, var panākt kaitējuma un advokāta maksu atlīdzināšanu.

⁽¹⁾ Mēs jau agrāk esam snieguši Komisijai informāciju par maza apmēra prasībām.

Arī štatu likumi daudzās dažādās situācijās aizsargā personas privāto dzīvi. Jomas, kur štati nav veikuši nekādus pasākumus, ietver banku informāciju, kabeļtelevīzijas abonementus, kredītinformāciju, nodarbinātības datus, valdības informāciju, ģenētisko un medicīnas informāciju, informāciju par apdrošināšanu, izglītību, elektroniskos paziņojumus un video nomu ⁽¹⁾.

B. Likumā skaidri noteiktas atļaujas

“Drošības zonas” principos ir iekļauts izņēmums, ja likums, noteikumi vai tiesu prakse rada “pretrunīgus pienākumus vai skaidri izteiktas atļaujas, ja izmantojot šādu atļauju, organizācija var pierādīt, ka principu neievērošana ir ierobežota, ciktāl tas vajadzīgs, lai ievērotu primārās likumīgās intereses, kuras izriet no šādas atļaujas.” Ir skaidrs, ka, ja ASV tiesību akti uzliek pretrunīgas saistības, ASV organizācijām, neatkarīgi no tā, vai tās ir “drošības zonā” vai ne, tie ir jāievēro. Lai gan “drošības zonas” principi ir paredzēti, lai pārvarētu ASV un Eiropas sistēmu atšķirības attiecībā uz privātās dzīves aizsardzību, attiecībā uz skaidrām atļaujām mēs pievēršsimies mūsu ievēlēto likumdevēju likumdošanas prerogatīvām. Ierobežotais izņēmumu skaits, kad var atkāpties no “drošības zonas” principu stingras ievērošanas, ir noteikts, lai ievērotu abu pušu likumīgās intereses.

Izņēmums attiecas tikai uz tiem gadījumiem, kad ir skaidra atļauja. Tādēļ neskaidrās situācijās attiecīgajam likumam, noteikumiem vai tiesas lēmumam ir skaidri jāatļauj “drošības zonas” organizācijām konkrēta rīcība ⁽²⁾. Citiem vārdiem, izņēmumu nepiemēro, ja tas nav noteikts likumā. Turklāt izņēmumu piemēro tikai tad, ja skaidra atļauja ir pretrunā ar “drošības zonas” principu ievērošanu. Pat tad izņēmums “ir ierobežots, ciktāl tas ir vajadzīgs, lai ievērotu primārās likumīgās intereses, kuras izriet no šādas atļaujas.” Piemēram, ja likums vienkārši atļauj uzņēmumam sniegt personisko informāciju valdības iestādēm, izņēmumu nepiemēro. Turpretim, ja likums īpaši atļauj uzņēmumam sniegt personisko informāciju valdības iestādēm bez indivīda piekrišanas, tā ir “skaidra atļauja” rīkoties tādā veidā, kas ir pretrunā “drošības zonas” principiem. Arī īpaši izņēmumi no prasībām par informēšanu un piekrišanu attiektos uz izņēmumu (jo tas būtu līdzvērtīgs īpaši atļaujai izpaust informāciju bez informēšanas un piekrišanas). Piemēram, saskaņā ar likumu, kas ļauj ārstiem sniegt viņu pacientu medicīnas datus veselības iestāžu ierēdņiem bez pacienta iepriekšējas piekrišanas, var atļaut izņēmumu no informēšanas un izvēles principiem. Šī atļauja neļautu ārstam šos pašus medicīnas datus sniegt veselības aprūpes organizācijām vai komerciālām farmācijas pētījumu laboratorijām, jo tas neatbilstu ar likumu atļautajiem mērķiem un nebūtu izņēmums ⁽³⁾. Attiecīgais likumīgais pamats var būt vienreizēja atļauja veikt noteiktas darbības ar personisko informāciju, bet, kā rāda turpmākie piemēri, tas drīzāk būs izņēmums no plašāka likuma, kas reglamentē personiskās informācijas vākšanu, izmantošanu vai izpaušanu.

1996. gada Telecommunications Act

Daudzos gadījumos atļauti izmantošanas veidi vai nu atbilst Direktīvas un principu prasībām, vai ir pieļaujami saskaņā ar kādu no citiem atļautajiem izņēmumiem. Piemēram, *Telecommunications Act* 702. paragrāfā (kodificēts 47 U. S. C. § 222) telekomunikāciju uzņēmumiem uzliek pienākumu saglabāt tās personiskās informācijas konfidencialitāti, ko tie iegūst, sniedzot klientiem savus pakalpojumus. Šis noteikums īpaši atļauj telekomunikāciju uzņēmumiem:

- 1) izmantot klientu informāciju, lai sniegtu telekomunikāciju pakalpojumus, to skaitā publicēt abonentu katalogus;
- 2) sniegt klienta informāciju citiem pēc klienta rakstiska pieprasījuma; un
- 3) sniegt klientu informāciju apkopotā veidā.

⁽¹⁾ Nesenas elektroniskas meklēšanas rezultātā *Westlaw* datu bāzē tika atrastas 994 zināmas lietas štata līmenī, kuras attiecās uz kaitējuma atļidzināšanu un privātās dzīves aizskārumiem.

⁽²⁾ Skaidrības labad jānorāda, ka attiecīgajai tiesu iestādei nav īpaši jāatsaucas uz “drošības zonas” principiem.

⁽³⁾ Līdzīgi ārsts šajā piemērā nevarēja pamatot to, ka nebija ievērotas indivīda tiesības atteikties no tiesas tirgvedības, kas noteikta FAQ 12, ar likumā noteiktajām pilnvarām.

Skat. 47 U. S. C. § 222(a)(1)-(3). Likums arī atļauj telekomunikāciju uzņēmumiem izņēmuma kārtā izmantot klientu informāciju:

- 1) lai uzsāktu, sniegtu, izsniegtu rēķinus un iekasētu samaksu par saviem pakalpojumiem;
- 2) lai aizsargātu pret krāpniecisku, aizskarošu vai nelikumīgu rīcību; un
- 3) lai veiktu tirdzniecību pa telefonu, sniegtu izziņas vai administratīvus pakalpojumus klienta zvana laikā ⁽¹⁾.

[Tas pats, § 222(d)(1)-(3)] Visbeidzot, telekomunikāciju uzņēmumiem ir jāsniedz abonentu katalogu izdevējiem abonentu saraksta informācija, kurā var būt tikai vārdi, adreses, telefona numuri un uzņēmējdarbības joma attiecībā uz klientiem, kas ir juridiskās personas. [Tas pats, § 222(e)]

Izņēmumu attiecībā uz "skaidrām atļaujām" var piemērot, ja telekomunikāciju uzņēmumi izmanto CPNI, lai novērstu krāpšanu vai citu nelikumīgu rīcību. Pat tad var uzskatīt, ka šādas darbības ir sabiedrības interesēs, un šā iemesla dēļ tās saskaņā ar principiem var atļaut.

Veselības ministrijas [Department of Health and Human Services] ierosinātie noteikumi

Veselības ministrija (HHS) ir ierosinājusi noteikumus attiecībā uz individuāli identificējamās veselības informācijas slepenības standartu. Skat. 64 Fed. Reg. 59.918 (1999. gada 2. novembris) (tiks kodificēts kā 45 C. F. R. pts. 160-164). Ar noteikumiem īstenotu 1996. gada *Health Insurance Portability and Accountability Act*, Pub. L. 104-191 [Likums par veselības apdrošināšanas pārnēsāmību un atbildību] prasības attiecībā uz privātās dzīves aizsardzību. Skat. ierosinājumus 45 C. F. R. § 164.506. Ierosinātie noteikumi prasītu izpaust aizsargājamu veselības informāciju tikai diviem mērķiem: 1) lai ļautu indivīdiem apskatīt un nokopēt veselības informāciju par viņiem, skat. to pašu § 164.514; un 2) lai izpildītu noteikumus, skat. to pašu § 164.522.

Ierosinātie noteikumi atļautu izmantot vai izpaust aizsargājamu veselības informāciju bez īpašas indivīda atļautas atsevišķos apstākļos. Piemēram, to var darīt pārskatā par veselības aprūpes sistēmu, likuma izpildei un ārkārtējās situācijās. Skat. to pašu § 164.510. Ierosinātajos noteikumos ir sīki izklāstīti šo izmantošanas veidu izpaušanas robežas. Turklāt atļauti izmantojot un izpaužot aizsargājamu veselības informāciju, jārikojas tikai ar minimālo vajadzīgo informācijas daudzumu. Skat. to pašu § 164.506.

Ierosinātajos noteikumus skaidri atļautie izmantošanas veidi parasti atbilst "drošības zonas" principiem, vai arī tie ir citādi atļauti saskaņā ar citu izņēmumu. Piemēram, ir atļauta likuma izpilde, tiesiska administrēšana un medicīniski pētījumi. Citi izmantošanas veidi, piemēram, pārskats par veselības aprūpes sistēmu, sabiedrības veselības aizsardzības funkcija un valdības veselības datu sistēmas kalpo sabiedrības interesēm. Informācijas izpaušana, lai apstrādātu veselības aprūpes maksājumus un prēmijas, ir vajadzīga veselības aprūpes sniegšanai. Izmantošana ārkārtējos gadījumos, lai apspriestos ar tuvāko radnieku par ārstēšanu, kas pacienta piekrišanu "faktiski vai pienācīgi nevar iegūt", vai lai noteiktu mirušā cilvēka identitāti vai nāves cēloni, aizsargā datu subjektu un citu personu īpaši svarīgās intereses. Izmantošana, lai pārzinātu iesauamos karadienestā un citas īpašas indivīdu grupas, palīdz pienācīgi izpildīt militāro misiju vai līdzīga neatliekamas situācijas; jebkurā gadījumā parasti šie izmantošanas veidi maz attiecas uz patērētājiem vai arī uz tiem neattiecas vispār.

Paliek vienīgi gadījums, kad veselības aprūpes iestādes izmanto personisko informāciju, lai veidotu pacientu reģistrus. Kaut gan tas var neskart "īpaši svarīgās intereses", no šiem reģistriem gūst labumu gan pacienti, gan viņu draugi un radnieki. Tātad šī atļautā izmantošanas veida darbības joma ir ierobežota rakstura. Tādēļ tas, ka šim mērķim piemēro

⁽¹⁾ Šī izņēmuma piemērošanas joma ir ļoti ierobežota. Saskaņā ar tā noteikumiem, telekomunikāciju uzņēmums var izmantot CPNI tikai klienta zvana laikā. Bez tam FCC ir ieteikusi, ka telekomunikāciju uzņēmums nedrīkst izmantot CPNI, lai tirgotu pakalpojumus, par kuriem klients nepieprasa informāciju. Visbeidzot, tā kā klientam ir jāatļauj CPNI izmantošana šim mērķim, šis noteikums nav "izņēmums".

izņēmumu attiecībā uz likumā noteiktu "skaidru atļauju" izmantošanas veidiem, pacientu privāto dzīvi apdraud minimāli.

Fair Credit Reporting Act

Eiropas Komisija ir izteikusi bažas, ka izņēmumi attiecībā uz "skaidrām atļaujām" "efektīvi radītu atbilstības atzinumu" par *Fair Credit Reporting Act* (FCRA). Taču tas tā nav. Ja nav īpaša atbilstības atzinuma par FCRA, tām ASV organizācijām, kas citādi paļautos uz šādu atzinumu, jāapsola stingri ievērot "drošības zonas" principus visos jautājumos. Tas nozīmē, ka tad, ja FCRA prasības pārsniedz principu prasības, ASV organizācijām jāpakļaujas tikai FCRA. Turpretim, ja FCRA prasības ir mazākas, tad šīm organizācijām sava darbība ir jāsaskaņo ar principiem. Izņēmums šo pamatnovērtējumu nemainītu. Saskaņā ar tā noteikumiem, izņēmumu piemēro tikai tad, ja attiecīgajā likumā ir atļauta rīcība, kas būtu pretrunā ar "drošības zonas" principiem. Izņēmumu nepiemēro, ja FCRA prasības vienkārši neatbilst "drošības zonas" principiem ⁽¹⁾.

Citiem vārdiem sakot, nav paredzēts, ka izņēmums nozīmē to, ka tas, kas nav vajadzīgs, tādēļ ir "skaidri atļauts". Bez tam izņēmumu piemēro tikai tad, ja tas, ko atļauj ASV tiesību akti, ir pretrunā "drošības zonas" principiem. Lai dotu atļauju neievērot principus, attiecīgajam tiesību aktam jāatbilst abiem šiem kritērijiem.

Piemēram, FCRA 604. paragrāfā ir skaidri atļauts patērētāju kredītu uzraudzības iestādēm izdot ziņojumus par patērētājiem vairākos konkrētos gadījumos. Skat. FCRA, § 604. Ja to darot, 604. paragrāfā ir atļauts kredītu uzraudzības iestādēm rīkoties pretrunā "drošības zonas" principiem, tām jābalstās uz šo izņēmumu (protams, izņemot, ja nav spēkā kādi citi izņēmumi). Kredītu uzraudzības iestādēm jāpilda tiesas nolēmumi un iepriekšējas izmeklēšanas zvērināto tiesas pavēstes, un kredītinformācijas izmantošana valdības licencēšanas iestādēm, sociālā un bērnu pabalstu izpildiestādēm atbilst sabiedrības interesēm. [Tas pats, § 604(a)(1), (3)(D) un (4).] Tātad kredītu uzraudzības iestādei šiem mērķiem nevajadzētu pamatoties uz izņēmumu attiecībā uz "skaidru atļauju". Ja tā rīkojas atbilstīgi patērētāja rakstiskiem norādījumiem, patērētāju kredītu uzraudzības iestāde pilnībā ievēro "drošības zonas" principus. [Tas pats, § 604(a)(2)] Līdzīgi ziņas par patērētājiem var iegūt nodarbinātības mērķiem tikai ar patērētāja rakstisku atļauju (tas pats, §§ 604(a)(3)(B) un (b)(2)(A)(iii)) un kredīta vai apdrošināšanas darījumiem, ko patērētājs neveic, tikai tad, ja patērētājs nav šādu iespēju atteicis (tas pats, § 604(c)(1)(B)). Turklāt FCRA aizliedz kredītu uzraudzības iestādēm sniegt medicīnas informāciju nodarbinātības mērķiem bez patērētāja piekrišanas. [Tas pats, § 604(g)] Attiecībā uz šādiem izmantošanas veidiem jāievēro informēšanas un izvēles principi. Citi mērķi, kas ir atļauti saskaņā ar 604. paragrāfu, ir darījumi, kurā patērētājs ir iesaistīts, un šā iemesla dēļ principi tos atļauj. Skat. to pašu, § 604(a)(3)(A) un (F).

Pēdējais izmantošanas veids, kas saskaņā ar 604. paragrāfu, ir atļauts, attiecas uz sekundārajiem kredītu tirgiem. [Tas pats, § 604(a)(3)(E)] Nav pretrunu starp patērētāju kredītinformācijas izmantošanu šim mērķim un "drošības zonas" principiem *per se*. Ir taisnība, ka FCRA neprasa, lai kredītu uzraudzības iestādes, piemēram, informētu patērētājus un saņemtu viņu piekrišanu, kad tās izdod ziņojumus šim mērķim. Tomēr vēlreiz atkārtojam, ka tas, kas nav prasības, nenozīmē, ka "skaidra atļauja" ļauj rīkoties citādi nekā prasīts. Līdzīgi 608. paragrāfs ļauj kredītu uzraudzības iestādēm sniegt daļu personiskās informācijas valdības iestādēm. Šī "atļauja" neattaisnotu to, ka kredītu uzraudzības iestāde ignorētu savu apņemšanos stingri ievērot "drošības zonas" principus. Taču pārējos piemēros izņēmumi attiecībā uz prasību par informēšanu un izvēli darbojas, lai skaidri atļautu personiskās informācijas izmantošanu, nepiemērojot informēšanas un izvēles principus.

Secinājumi

Pat no šiem nedaudzajiem likumu piemēriem rodas priekšstats par struktūru.

— Likumā noteikta "skaidra atļauja" parasti ļauj personisko informāciju izmantot vai izpaust bez indivīda iepriekšējas piekrišanas; tādējādi izņēmums attiecas tikai uz informēšanas un izvēles principu.

⁽¹⁾ Šo apspriešanu nevajadzētu uztvert kā pieņēmumu, ka FCRA nenodrošina "pienācīgu" aizsardzību. Vērtējot FCRA, jāņem vērā aizsardzība, kas kopumā noteikta likumā, un nevajadzētu visu uzmanību pievērst tikai izņēmumiem, kā darīts šeit.

- Lielākajā daļā gadījumu likumā atļautie izņēmumi ir noteikti, lai tos izmantotu tikai īpašās situācijās īpašiem mērķiem. Visos gadījumos, kas nav iepriekšminētie gadījumi, likums citādi aizliedz personiskās informācijas neatļautu izmantošanu vai izpaušanu.
- Lielākajā daļā gadījumu, ņemot vērā to juridisko raksturu, atļauta izmantošana vai izpaušana ir sabiedrības interesēs.
- Gandrīz visos gadījumos atļautie izmantošanas veidi vai nu pilnībā atbilst “drošības zonas” principiem, vai attiecas uz vienu no abiem izņēmumiem.

Tātad, ņemot vērā to izņēmumu raksturu, kas attiecas uz likumā noteiktām “skaidrām atļaujām”, tie visdrīzāk būs diezgan ierobežoti.

C. Apvienošanās un pārņemšana

Direktīvas 29. pantā minēta darba grupa ir izteikusi bažas par situācijām, kad kādu “drošības zonas” organizāciju pārņem vai apvieno ar uzņēmumu, kas nav apņēmis ievērot “drošības zonas” principus. Tomēr šķiet, ka darba grupa ir pieņēmusi, ka jaunajam uzņēmumam nebūtu obligāti jāievēro “drošības zonas” principi attiecībā uz personisko informāciju, kas ir pārņemtā uzņēmuma rīcībā. Saskaņā ar ASV tiesību aktiem pieņem, ka jaunais uzņēmums pilda pārņemtā uzņēmuma saistības un uzņemas tā atbildību. Skat. 15 *Fletcher Cyclopedia of the Law of Private Corporations* § 7117 (1990); skat. arī *Model Bus. Corp. Act* § 11.06(3) (1979) (“jaunajam uzņēmumam paliek visi pārņemto uzņēmumu pienākumi”). Citiem vārdiem sakot, saskaņā ar šo metodi, jaunajam uzņēmumam, kas rodas, apvienojoties ar “drošības zonas” organizāciju vai to pārņemot, šīs “drošības zonas” organizācijas pienākumi ir saistoši.

Turklāt pat tad, ja apvienošanās vai pārņemšana būtu notikusi, iegādājoties aktīvus, iegūtā uzņēmuma saistības iegūstošajam uzņēmumam vienlīdz atsevišķos apstākļos būtu jāpilda. [15 *Fletcher*, § 7122] Pat tad, ja saistības pēc apvienošanās nav jāpilda, tomēr ir vērts norādīt, ka tās pēc apvienošanās nebūtu jāpilda arī tad, ja dati būtu nosūtīti no Eiropas atbilstīgi līgumam, kas ir vienīgā alternatīva “drošības zonai” attiecībā uz datu nosūtīšanu uz Amerikas Savienotajām Valstīm. Turklāt pārskatītie “drošības zonas” dokumenti tagad prasa, lai “drošības zonas” organizācijas paziņotu Tirdzniecības ministrijai par pārņemšanu un ļautu datus turpināt nosūtīt pārņemtajai organizācijai tikai tad, ja tā pievienojas “drošības zonai”. Skat. FAQ 6. Amerikas Savienotās Valstis tiešām ir tagad pārskatījušas “drošības zonas” sistēmu, prasot, lai ASV organizācijas šādā situācijā dzēstu informāciju, ko tās ir saņēmušas saskaņā ar “drošības zonas” sistēmu, ja to saistības vairs nebūs spēkā vai arī ja nav ieviesti citi piemēroti aizsardzības pasākumi.

V PIELIKUMS

2000. gada 14. jūlijs

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

Godātais Moga kungs!

Saprotu, ka saistībā ar manu 2000. gada 29. marta vēstuli ir radušies vairāki jautājumi. Sūtu šo vēstuli, lai precizētu mūsu pilnvaras jomās, par kurām ir radušies jautājumi, un tā papildinās un rezumēs iepriekšējo vēstuli.

Jūsu vizīšu laikā uz mūsu birojiem un jūsu sarakstē Jūs esat izteicis vairākus jautājumus par Amerikas Savienoto Valstu *Federal Trade Commission* pilnvarām tiešsaistes privātuma jomā. Domāju, ka būtu lietderīgi apkopot manas iepriekš sniegtās atbildes attiecībā uz FTC darbību šajā jomā un sniegt papildu informāciju par iestādes jurisdikciju patērētāju privātuma jautājumos, kas skarti Jūsu pēdējā vēstulē. Jūs īpaši jautājat, vai 1) FTC jurisdikcijā ir ar nodarbinātību saistītu datu nosūtīšana, ja tā ir veikta, pārkāpjot ASV "drošības zonas" principus; 2) FTC jurisdikcijā ir bezpeļņas programmas ar slepenības statusu; 3) FTC Act attiecas gan uz tiešsaistes darbībām, gan arī uz darbībām, kuras nenotiek Internetā; un 4) kas notiek tad, ja FTC jurisdikcija daļēji sakrīt ar citu tiesībaizsardzības iestāžu jurisdikciju.

FTC Act piemērošana privātumam

Kā Jūs zināt, pēdējos piecos gados FTC ir uzņēmusies vadošu lomu, sekmējot šīs ASV nozares un patērētāju grupu centienus izstrādāt vispusīgu sistēmu attiecībā uz patērētāju privātās dzīves aizsardzības jautājumiem, to skaitā personiskās informācijas vākšanu un izmantošanu Internetā. Publiskos semināros un ilgstošās apspriedēs ar nozares locekļiem, patērētāju pārstāvjiem un kolēģiem no Tirdzniecības ministrijas, kā arī ar ASV valdības palīdzību esam palīdzējuši noteikt galvenos politikas jautājumus un izstrādāt pieņemamus risinājumus.

Federal Trade Commission likumīgās pilnvaras šajā jomā ir noteiktas *Federal Trade Commission Act* ("FTC Act") 5. paragrāfā, kas aizliedz "negodīgu un maldinošu darbību vai rīcību", ko veic tirdzniecībā vai kas to ietekmē ⁽¹⁾. Maldinošu rīcību definē kā atspoguļojumu, bezdarbību vai darbību, kas materiālā ziņā var maldināt saprātīgus patērētājus. Rīcība ir negodīga, ja tā rada vai var radīt būtisku kaitējumu patērētājiem, kas nav novēršams un ko neatsver labums, kuru patērētājs gūst vai kurš ietekmē konkurenci ⁽²⁾.

Atsevišķa informācijas vākšanas prakse visdrīzāk pārkāpj FTC Act. Piemēram, ja tīmekļa vietne nepatiesi apgalvo, ka tā ievēro noteikto slepenības politiku vai pašregulatīvu pamatnostādņu kopumu, FTC Act 5. paragrāfs ir juridiskais pamats, lai šādu sagrozījumu apstrīdētu kā maldinošu. Mēs tiešām esam veiksmīgi piemērojuši likumu, lai noteiktu šo principu ⁽³⁾. Turklāt Komisija ir nolēmusi, ka tā īpaši apstrīdēs nelikumīgu rīcību attiecībā uz privātumu kā negodīgu saskaņā ar 5. paragrāfu, ja šāda rīcība attiecas uz bērniem vai tajā ir izmantota ļoti sensitīva informācija, piemēram, finanšu informācija ⁽⁴⁾ un medicīnas dati. *Federal Trade Commission* ir veikusi un turpinās veikt šādu tiesību aizsardzību, īstenojot aktīvu uzraudzību un izmeklēšanu, arī uz to lietu pamata, ko mēs saņemam no pašregulatīvām organizācijām un citiem, to skaitā no Eiropas Savienības dalībvalstīm.

⁽¹⁾ 15 U. S. C. § 45. *Fair Credit Reporting Act* attiecas arī uz datu vākšanu un tirdzniecību Internetā, kas atbilst likumā noteiktajām terminu "patērētāju kredītinformācija" un "patērētāju kredītu uzraudzības iestāde" definīcijām.

⁽²⁾ 15 U. S. C. § 45(n).

⁽³⁾ Skat. *GeoCities*, lieta Nr. C-3849 (1999. gada 12. februāra galīgais spriedums) (pieejams Interneta adresē www.ftc.gov/os/1999/9902/9823015d%26o.htm); *Liberty Financial Cos.*, lieta Nr. C-3891 (1999. gada 12. augusta galīgais spriedums) (pieejams Interneta adresē www.ftc.gov/os/1999/9905/younginvestor.htm). Skat. arī *Children's Online Privacy Protection Act Rule (COPPA)*, 16 C. F. R. 312. daļa (pieejams Interneta adresē www.ftc.gov/opa/1999/9910/childfinal.htm). COPPA Rule, kas stājas spēkā pāgājušajā mēnesī, prasa, lai tādu tīmekļa vietņu operatori, kuras ir domātas bērniem, kas ir jaunāki par 13 gadiem un kurās apzināti vāc personisko informāciju no bērniem, kas ir jaunāki par 13 gadiem, īstenotu godīgas informēšanas prakses standartus, kuri likumā ir skaidri noteikti.

⁽⁴⁾ Skat. *FTC v. Touch Tone, Inc.*, civilprasība Nr. 99-WM-783 (D. Co.) (iesniegta 1999. gada 21. aprīlī), pieejama Interneta adresē www.ftc.gov/opa/1999/9904/touchtone.htm. 1997. gada 17. jūlija personāla vēstule ar atzinumu, kas sniegts, atbildot uz *Center for Media Education* iesniegto lūgumrakstu, pieejams Interneta adresē www.ftc.gov/os/1997/9707/cenmed.htm.

FTC pašregulēšanās atbalsts

FTC jau ilgi ir atbalstījusi nozares centienus izstrādāt efektīvas pašregulatīvas programmas, lai nodrošinātu patērētāju privātās dzīves aizsardzību Internetā. Lai šie centieni būtu veiksmīgi, jābūt arī plašai to personu līdzdalībai, kas šajā nozarē darbojas. Tai pašā laikā pašregulēšanās jāapvieno ar tiesībaizsardzību. Šo iemeslu dēļ FTC pirmkārt izskatīs lietas par tādu organizāciju kā BBBOnline un TRUSTe pašregulatīvu pamatnostādņu neievērošanu. Šī pieeja būtu savienojama ar mūsu ilgstošajām attiecībām ar Better Business Bureau [Uzņēmējdarbības veicināšanas birojs] National Advertising Review Board [Valsts reklāmas uzraudzības padome] (NARB), kas FTC iesniedz sūdzības attiecībā uz reklāmu. NARB National Advertising Division [Valsts reklāmas nodaļa] (NAD) risina sūdzības attiecībā uz valsts reklāmu, izmantojot iztiesāšanas procedūru. Ja puse atsakās ievērot NAD lēmumu, lietu iesniedz FTC. FTC personāls pirmkārt pārbauda apstrīdēto reklāmu, lai noteiktu, vai tā pārkāpj FTC Act, un tam bieži izdodas apstrīdēto rīcību pārtraukt vai pārliecināt pusi atgriezties pie NARB procedūras.

Līdzīgi FTC pirmkārt izskatīs lietas par "drošības zonas" principu neievērošanu no ES dalībvalstīm. Tāpat kā gadījumā ar lietām, ko iesniedz ASV pašregulatīvas organizācijas, mūsu personāls izskatīs visu informāciju, lai pārbaudītu vai rīcība, par kuru ir iesniegta sūdzība, pārkāpj FTC Act 5. paragrāfu. Šī apņemšanās ir arī atrodama "drošības zonas" princips pie visbiežāk uzdotā jautājuma (FAQ 11) par izpildi.

Geo Cities: FTC pirmā lieta par tiešsaistes privātumu

Federal Trade Commission pirmā lieta par privātās dzīves aizsardzību Internetā pret GeoCities pamatojās uz Komisijas pilnvarām saskaņā ar 5. paragrāfu ⁽¹⁾. Šajā lietā FTC apgalvoja, ka GeoCities maldināja gan pieaugušos, gan bērnus par to, kā tiks izmantota viņu personiskā informācija. Federal Trade Commission sūdzībā bija apgalvots, ka GeoCities skaidroja, ka atsevišķu personisko informāciju, ko tā vāca savā tīmekļa vietnē, izmantos tikai iekšējiem mērķiem vai lai sniegtu patērētājiem īpašus reklāmas piedāvājumus, produktus vai pakalpojumus, kurus viņi pieprasa, un ka atsevišķu papildu "izvēles" informāciju tā nevienam neizpauž bez patērētāja atļaujas. Taču patiesībā šo informāciju izpauž trešai personai, kas to izmantoja, lai izteiktu piedāvājumus, kuriem personas nebija devušas savu piekrišanu. Sūdzībā arī bija apgalvots, ka GeoCities ir iesaistījies maldinošā rīcībā saistībā ar informācijas vākšanu no bērniem. Saskaņā ar FTC sūdzību GeoCities apgalvoja, ka tā tīmekļa vietnē darbojas zona bērniem un ka tur savāko informāciju pārzina GeoCities. Patiesībā šīs tīmekļa vietnes zonas darbināja trešās personas, kas informāciju arī vāca un pārzināja.

Nolēmums aizliedz GeoCities maldināt attiecībā uz mērķi, kuram tā vāc vai izmanto personisko informāciju no patērētājiem, ieskaitot bērnus, vai par tiem. Rīkojums prasa uzņēmumam savā tīmekļa vietnē ievietot skaidru un pamanāmu paziņojumu par privātumu, kurā patērētājiem ir izskaidrots, kāda informācija tiek vākta un kādam mērķim to dara, kam to izpauž un kā patērētāji var informācijai piekļūt un to dzēst. Lai nodrošinātu vecāku kontroli, nolēmums prasa arī, lai GeoCities iegūtu vecāku atļauju pirms personiskas informācijas vākšanas no bērniem, kas ir jaunāki par 13 gadiem. Saskaņā ar rīkojumu, GeoCities jāinformē savi biedri un jāsniedz viņiem iespēja savu informāciju izdzēst no GeoCities un trešo personu datu bāzēm. Nolēmums īpaši prasa, lai GeoCities informētu to bērnu vecākus, kas ir jaunāki par 13 gadiem, un dzēstu viņu informāciju, ja vien vecāki nav piekrituši tās atstāšanai un izmantošanai. Visbeidzot, GeoCities ir jāsaazinās ar trešām personām, kurām tas pirms tam ir izpaužis informāciju un jāpieprasa, lai arī šīs personas šādu informāciju dzēstu ⁽²⁾.

ReverseAuction.com

Pavisam nesen kāds cits tiešsaistes uzņēmums iesniedza sūdzību, kurā apgalvoja, ka minētais uzņēmums pārkāpj privātumu. 2000. gada janvārī Komisija apstiprināja un piekrita izsoles tīmekļa vietnes sūdzībai par ReverseAuction.com, ko apsūdzēja par patērētāju personiskās informācijas iegūšanu no konkurējošās vietnes (eBay.com) un sekojošu maldinošu un neprasītu e-pasta ziņojumu sūtīšanu šiem patērētājiem, kuri bija ieinteresēti šajos darījumos ⁽³⁾. Sūdzības iesniedzējs apgalvoja, ka ReverseAuction pārkāpj FTC Act 5. paragrāfu, iegūstot personiski

⁽¹⁾ GeoCities, lieta Nr. C-3849 (1999. gada 12. februāra galīgais spriedums) (pieejams Interneta adresē www.ftc.gov/os/1999/9902/9823015d%26o.htm).

⁽²⁾ Komisija vēlāk atrisināja vēl vienu lietu saistībā ar personiskas informācijas vākšanu no bērniem Internetā. Liberty Financial Companies, Inc., darbināja tīmekļa vietni Young Investor, kas bija paredzēta bērniem un pusaudžiem un bija saistīta ar finanšu un ieguldījumu jautājumiem. Komisija apgalvoja, ka tur bija maldinoši izskaidrots, ka personisko informāciju, kas ir iegūta no bērniem aptaujā, glabās anonīmi un ka dalībniekiem nosūtīs e-pasta apkārtakstu, kā arī balvas. Patiesībā personisko informāciju par bērnu un ģimenes finansēm glabāja identificējamā veidā, un netika izsūtīti ne apkārtaksti, ne balvas. Konsensuālā vienošanās aizliedz turpmākus sagrozījumus un prasa, lai Liberty Financial savās bērniem paredzētajās tīmekļa vietnēs ievietotu paziņojumu par privātās dzīves aizsardzību un pirms personiski identificējamās informācijas vākšanas no bērniem iegūtu pārbaudāmu atļauju no viņu vecākiem. Liberty Financial Cos., lieta Nr. C-3891 (1999. gada 12. augusta galīgais spriedums) (pieejams Interneta adresē www.ftc.gov/os/1999/9905/younginvestor.htm).

⁽³⁾ Skat. ReverseAuction.com, Inc., civiltiesas Nr. 000032 (D. D. C.) (iesniegta 2000. gada 6. janvārī) (paziņojums presei un pieejami pieejami Interneta adresē www.ftc.gov/opa/2000/01/reverse4.htm).

identificējamu informāciju, kas ietvēra *eBay* lietotāju e-pasta adreses un personalizētus lietotāju identifikācijas vārdus ("lietotāja ID"), un izsūtīt maldinošus e-pasta ziņojumus.

Sūdzībā aprakstīts, ka *ReverseAuction* pirms informācijas iegūšanas reģistrējās kā *eBay* lietotājs un apņēmas ievērot *eBay* lietotāja līgumu un slepenības politiku. Līgums un politika aizsargā patērētāju privāto dzīvi, aizliedzot *eBay* lietotājiem vākt un izmantot personisko informāciju neatļautiem mērķiem, kā piemēram, sūtīt neprasītus e-pasta ziņojumus. Tādējādi sūdzībā, pirmkārt, bija apgalvots, ka *ReverseAuction* maldināja, ka tas ievēros *eBay* lietotāja līgumu un slepenības politiku, kas saskaņā ar 5. paragrāfu ir maldinoša rīcība. Turklāt sūdzībā bija apgalvots, ka tas, ka *ReverseAuction* izmantoja informāciju, lai sūtītu neprasītas komerciāla rakstura elektroniskās vēstules, pārkāpjot lietotāja līguma un slepenības politiku, saskaņā ar 5. paragrāfu ir negodīga rīcība tirdzniecībā.

Otrkārt, sūdzībā bija apgalvots, ka e-pasta ziņojumos patērētājiem bija iekļauta maldinoša temata rindiņa, kurā bija teikts, ka viņu *eBay* lietotāja ID "drīz beigsies termiņš". Visbeidzot sūdzībā bija apgalvots, ka e-pasta ziņojumos bija nepatiesi apgalvots, ka *eBay* ir tieši vai netieši sniedzis *ReverseAuction* *eBay* lietotāju personiski identificējamu informāciju vai citādi piedalījies neprasītu elektronisko vēstuļu izplatīšanā.

FTC panāktais nolēmums aizliedz *ReverseAuction* turpmāk izdarīt šādus pārkāpumus. Tas arī prasa, lai *ReverseAuction* sniegtu paziņojumu patērētājiem, kas pēc *ReverseAuction* elektroniskās vēstules saņemšanas ir reģistrējušies vai reģistrēsies *ReverseAuction*. Paziņojumā šie patērētāji jāinformē, ka viņu *eBay* lietotāja ID tūlīt nebeigsies termiņš un ka *eBay* nezina par to, ka *ReverseAuction* izplatīja neprasītas elektroniskās vēstules, un to neatļāva. Paziņojumā šiem patērētājiem jāsniedz arī iespēja anulēt *ReverseAuction* reģistrāciju un izdzēst savu personiski identificējamu informāciju no *ReverseAuction* datu bāzes. Turklāt rīkojums prasa, lai *ReverseAuction* dzēstu to *eBay* lietotāju personiski identificējamu informāciju, kas saņēma *ReverseAuction* elektronisko vēstuli, bet *ReverseAuction* nav reģistrējušies, un atturētos no šādas informācijas izmantošanas vai izpaušanas. Visbeidzot, saskaņā ar šim uzņēmumam agrāk izsniegtajiem rīkojumiem attiecībā uz privātumu, nolēmums prasa, lai *ReverseAuction* savā tīmekļa vietnē publiskotu savu slepenības politiku, un tajā būtu iekļauti vispārēji noteikumi attiecībā uz uzskaites veikšanu, lai FTC varētu uzraudzīt atbilstību.

ReverseAuction lieta parāda, ka FTC ir apņēmusies izmantot izpildes pasākumus, lai atbalstītu nozares pašregulatīvus centienus patērētāju tiesaistes privātuma jomā. Šī lieta tieši apstrīdēja rīcību, kura pārkāpa slepenības politiku un lietotāja līgumu, kas aizsargā patērētāja privāto dzīvi, un kura varētu sagraut patērētāju uzticību privātās dzīves aizsardzības pasākumiem, ko veic tiesaistes uzņēmumi. Tā kā šajā lietā viens uzņēmums bija nelikumīgi piesavinājis tiesības uz patērētāju informāciju, kas bija aizsargāta saskaņā ar cita uzņēmuma slepenības politiku, tā var arī jo īpaši attiekties uz jautājumu par privātumu saistībā ar datu nosūtīšanu starp uzņēmumiem, kuri atrodas dažādās valstīs.

Neatkarīgi no *Federal Trade Commission* veiktās tiesībsaistības saistībā ar *GeoCities*, *Liberty Financial Cos.* un *ReverseAuction*, iestādes pilnvaras dažās tiesaistes privātuma jomās ir ierobežotākas. Kā norādīts iepriekš, lai varētu piemērot FTC Act, personiskās informācijas vākšanai vai izmantošanai bez piekrišanas jābūt maldinošai vai negodīgai rīcībai tirdzniecībā. Tādējādi FTC Act visdrīzāk neattieksies uz tīmekļa vietnē veiktu personiski identificējamās informācijas vākšanu no patērētājiem, ja vākšanas mērķis ir izskaidrots pareizi un informācija ir izmantota vai izpausta tādā veidā, ka tā, visdrīzāk, patērētājiem būtiski nekaitē. Tāpat FTC pilnvarās neietilpst vispārīgi prasīt, lai uzņēmumi, kas Internetā vāc informāciju, stingri ievērotu slepenības politiku vai kādu īpašu slepenības politiku⁽¹⁾. Tomēr, kā norādīts iepriekš, uzņēmuma noteiktās slepenības politikas neievērošana visdrīzāk būs maldinoša rīcība.

⁽¹⁾ Šā iemesla dēļ *Federal Trade Commission* savā ziņojumā Kongresam apgalvoja, ka, iespējams, ir vajadzīgi papildu tiesību akti, lai noteiktu, ka visās ASV komerciāla rakstura tīmekļa vietnēs, kas ir paredzētas patērētājiem, jāievēro noteiktā godīgas informēšanas prakse. "Consumer Privacy on the World Wide Web", iesniegts 1998. gada 21. jūlijā Amerikas Savienoto Valstu Pārštāvju palātas Tirdzniecības komisijas Telekomunikāciju, tirdzniecības un patērētāju tiesību aizsardzības apakškomisijai (ziņojums atrodams Interneta adresē www.ftc.gov/os/9807/privac98.htm). FTC atturējās ierosināt šādus tiesību aktus, lai dotu pašregulatīviem uzņēmumiem iespēju savās tīmekļa vietnēs parādīt, ka tie ir pieņēmuši godīgas informēšanas praksi. *Federal Trade Commission* savā ziņojumā Kongresam par tiesaistes privātumu, "Tiesaistes privātums: Ziņojums Kongresam" 1998. gada jūnijā (ziņojumu var atrast Internetā www.ftc.gov/reports/privacy3/toc.htm), FTC ieteica likumdošanu, kas liktu komerciālām tīmekļa vietnēm iegūt vecāku atļauju, pirms ievākt personiski identificējamu informāciju no bērniem, kas jaunāki par 13 gadiem. Skat. zemsvītras 3. (supra) piezīmi. Pagājušgad Komisijas ziņojums "Pašnoteikšanās un tiesaistes privātums: *Federal Trade Commission* Ziņojums Kongresam" 1999. gada jūlijā (ziņojumu var atrast Internetā www.ftc.gov/os/1999/9907/index.htm#13) atklāja pietiekami progresu pašnoteikšanās jomā un tajā brīdī nolēma neieteikt likumdošanu. Komisija tuvākajās nedēļās ziņos Kongresam par pašnoteikšanās attīstību vēlreiz.

Bez tam *FTC* jurisdikcija šajā jomā attiecas uz negodīgu vai maldinošu darbību vai rīcību tikai tad, ja to veic tirdzniecībā vai ja tā to ietekmē. Informācija, ko vāc komercuzņēmumi, kas reklamē produktus vai pakalpojumus, to skaitā vāc un izmanto informāciju komerciāliem mērķiem, visdrīzāk atbilstu šim nosacījumam par tirdzniecību. No otras puses, daudzi indivīdi vai uzņēmumi var vākt informāciju Internetā bez jebkāda komerciāla mērķa, un tādējādi tas var nebūt *Federal Trade Commission* jurisdikcijā. Šī ierobežojuma piemērs ir “virtuālās tērzēšanas telpas”, ja tās pārvalda nekomerciāli uzņēmumi, piem., labdarības organizācija.

Visbeidzot, uz *FTC* pamata jurisdikciju tirdzniecībā attiecas vairāki pilnīgi vai daļēji likumā noteikti izņēmumi, kas ierobežo *FTC* spēju vispusīgi risināt Interneta privātuma jautājumus. Šie izņēmumi attiecas uz daudziem tādiem intensīvas informācijas patērētāju uzņēmumiem, kā bankas, apdrošināšanas sabiedrības un aviosabiedrības. Kā Jūs jau zināt, šādi uzņēmumi atrodas citu federālo vai štata iestāžu jurisdikcijā, kā piemēram, federālās banku iestādes vai Transporta ministrija.

Gadījumos, kas ir tās jurisdikcijā, *FTC* pieņem, un ja to atļauj resursi, izskata patērētāju sūdzības, ko saņem pa e-pastu un telefonu savā Patērētāju informācijas centrā [*Consumer Response Center*] (“*CRC*”), kā arī pavisam nesen — savā tīmekļa vietnē ⁽¹⁾. *CRC* pieņem sūdzības no visiem patērētājiem, tostarp no tiem, kas dzīvo Eiropas Savienības dalībvalstīs. *FTC Act* piešķir *Federal Trade Commission* vienlīdzīgas pilnvaras ar rīkojumu saņemt palīdzību, lai novērstu turpmākus *FTC Act* pārkāpumus, kā arī par sniegtu kompensāciju skartajiem patērētājiem. Taču mēs izskatītu, vai uzņēmums ir iesaistījies noteiktā nelikumīgā rīcībā, jo nerisinām atsevišķu patērētāju domstarpības. *Federal Trade Commission* ir sniegusi kompensācijas gan Amerikas Savienoto Valstu, gan citu valstu pilsoņiem ⁽²⁾. *FTC* turpinās attiecīgos gadījumos īstenot savas pilnvaras, lai sniegtu kompensācijas citu valstu pilsoņiem, kurus ir skārusi tās jurisdikcijā veikta maldinoša rīcība.

Nodarbinātības dati

Savā pēdējā vēstulē Jūs lūdzāt papildus izskaidrot *FTC* jurisdikciju nodarbinātības datu jomā. Pirmkārt, Jūs uzdevāt jautājumu, vai *FTC* saskaņā ar 5. paragrāfu varētu vērsties pret uzņēmumu, kurš apgalvo, ka tas ievēro ASV “drošības zonas” principus, bet nosūta vai izmanto ar nodarbinātību saistītus datus tāda veidā, kas šiem principiem neatbilst. Mēs vēlamies Jums apliecināt, ka esam rūpīgi izskatījuši *FTC* pilnvarojošos tiesību aktus, saistītos dokumentus un attiecīgo tiesu praksi, un esam secinājuši, ka *FTC* ir tādi pati jurisdikcija attiecībā uz nodarbinātības datiem kā parasti saskaņā ar *FTC Act* 5. paragrāfu ⁽³⁾. Tātad, pieņemot, ka lieta atbilst mūsu pašreizējiem kritērijiem (negodīgums vai maldināšana) attiecībā uz privātuma aizsardzību, mēs varētu rīkoties situācijā, kas saistīta ar nodarbinātības datiem.

Mēs gribētu arī kļiedēt uzskatu, ka *FTC* var veikt privātuma aizsardzību tikai situācijās, kad uzņēmums ir krāpis atsevišķus patērētājus. Patiesībā, kā to skaidri parāda Komisijas nesenā rīcība *ReverseAuction* ⁽⁴⁾ lietā, *FTC* veiks privātuma aizsardzību attiecībā uz datu nosūtīšanu starp uzņēmumiem, kad viens uzņēmums ir rīkojies nelikumīgi attiecībā pret citu uzņēmumu, un tas, iespējams, ir radījis kaitējumu gan patērētājiem, gan uzņēmumiem. Mēs domājam, ka tieši šajā situācijā visdrīzāk radīsies jautājums par nodarbinātību, jo Eiropas uzņēmumi nosūta eiropiešu nodarbinātības datus Amerikas uzņēmumiem, kas ir apņēmušies ievērot “drošības zonas” principus.

Tomēr mēs vēlamies norādīt uz vienu apstākli, kad *FTC* darbība būtu ierobežota. Tas notiktu tad, ja lietu jau skata saistībā ar parasto kārtību strīdu izšķiršanā par darba tiesiskajām attiecībām, visdrīzāk kā prasību šķērējtiesā vai sūdzību par negodīgu rīcību nodarbinātības jomā *National Labor Relations Board*. Tas notiktu, piemēram, ja darba

⁽¹⁾ *Federal Trade Commission* tiešsaistes sūdzību veidlapa ir pieejama Interneta adresē <http://www.ftc.gov/ftc/complaint.htm>.

⁽²⁾ Piemēram, kādā nesenā lietā, kas bija saistīta ar Interneta piramīdveida shēmu, Komisija ieguva kompensāciju 15 622 patērētājiem, kas kopā bija aptuveni USD 5,5 miljoni. Patērētāji dzīvoja Amerikas Savienotajās Valstīs un 70 dažādās ārvalstīs. Skat. www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftcrefund01.htm.

⁽³⁾ Izņemot, ja to īpaši izslēdz *FTC* pilnvarojošais likums, *FTC* jurisdikcija saskaņā ar *FTC Act* attiecībā uz darbību, “ko veic tirdzniecībā vai kas to ietekmē, atbilst Kongresa konstitucionālajām pilnvarām saskaņā ar *Commerce Clause*”, *United States v. American Building Maintenance Industries*, 422 U.S. 271, 277 n. 6 (1975). Tādējādi *FTC* jurisdikcijā ir uzņēmumu un nozaru rīcība tirdzniecībā, kas ir saistīta ar nodarbinātību.”

⁽⁴⁾ Skat. “*Online Auction Site Settles FTC Privacy Charges*”, *FTC* ziņu izlaidums (2000. gada 6. janvāris), pieejams Interneta adresē <http://www.ftc.gov/opa/2000/01/reverse4.htm>.

devējs saistībā ar kolektīvo līgumu būtu uzņēmies saistības attiecībā uz personas datu izmantošanu un darbinieks vai arodbiedrība apgalvotu, ka darba devējs šo līgumu ir pārkāpis. Komisija visdrīzāk šādu lietu noraidītu ⁽¹⁾.

Jurisdikcija pār programmām ar slepenības statusu

Otrkārt, Jūs jautājat, vai *FTC* jurisdikcijā ir programmas ar slepenības statusu, kas reglamentē strīdu izšķiršanas mehānismus Amerikas Savienotajās Valstīs un kas nebija izpratušas savu lomu “drošības zonas” principu izpildē un izskatītā atsevišķas sūdzības, neskatoties uz to, ka šādi uzņēmumi tehniski bija “bezpeļņas”. Nosakot, vai mūsu jurisdikcijā ir uzņēmums, kas sevi uzskata par bezpeļņas uzņēmumu, Komisija rūpīgi analizē to, vai šāds uzņēmums, kura mērķis nav gūt peļņu sev, nedod peļņu saviem dalībniekiem. Komisijai ir izdevies apstiprināt savu jurisdikciju pār šādiem uzņēmumiem, un 1999. gada 24. maijā Amerikas Savienoto Valstu Augstākā tiesa lietā *California Dental Association v. Federal Trade Commission* vienprātīgi apstiprināja, ka pretmonopola jautājumā vietējo zobārstu apvienību brīvprātīgās bezpeļņas asociācijas ir Komisijas jurisdikcijā. Tiesa nosprieda:

FTC Act attiecas ne tikai uz uzņēmumiem, kas “ir izveidoti, lai veiktu darījumus nolūkā gūt sev peļņu” [15 U. S. C. § 44], bet arī uz tādiem uzņēmumiem, kuri veic darījumus, lai peļņu gūtu “tā dalībnieki”. Diez vai var pieņemt, ka Kongress ir paredzējis šādu ierobežotu atbalsta organizāciju jēdziena lietojumu, jo tas radītu iespēju izvairīties no jurisdikcijas, kad *FTC Act* mērķi neapšaubāmi to apstiprina.

Tātad, nosakot, vai apstiprināt jurisdikciju pār kādu konkrētu “bezpeļņas” organizāciju, kas pārvalda programmas ar slepenības statusu, faktiski jāpārbauda tas, cik lielā mērā uzņēmums ir sniedzis ekonomisku labumu saviem dalībniekiem. Ja šāds uzņēmums ir īstenojis savu programmu ar slepenības statusu tādā veidā, ka tā ir sniegusi dalībniekiem ekonomisku labumu, *FTC* jurisdikcija visdrīzāk būtu atzīstama. Kā atsevišķs punkts jāmin, ka *FTC* jurisdikcijā visdrīzāk būtu maldinošas programmas ar slepenības statusu, kuras statuss ir maldinoši norādīts kā bezpeļņas.

Privātās dzīves aizsardzība attiecībā uz darbībām, kas nenotiek Internetā

Treškārt, Jūs norādījāt, ka mūsu līdzšinējā sarakste ir bijusi galvenokārt par privātās dzīves aizsardzību Internetā. Privātās dzīves aizsardzība Internetā ir bijusi galvenais jautājums, kas *FTC* ir jārisina, jo tā ir svarīga elektroniskās tirdzniecības attīstības sastāvdaļa, taču *FTC Act* ir datējams ar 1914. gadu un tikpat lielā mērā attiecas arī uz darbībām, kas nenotiek Internetā. Tādējādi mēs varam celt prasības pret uzņēmumiem, kas nedarbojas Internetā un kas saistībā ar patērētāju privātās dzīves aizsardzību ir iesaistīti negodīgā vai maldinošā rīcībā attiecībā uz tirdzniecību ⁽²⁾. Pagājušajā gadā Komisijas iesniegtajā lietā *FTC v. TouchTone Information, Inc.* ⁽³⁾ kādu “informācijas mākleri” apsūdzēja par nelegālu patērētāju privātās finanšu informācijas iegūšanu un pārdošanu. Komisija apgalvoja, ka *TouchTone* ieguva patērētāju informāciju ar “aizbaidināšanos”, kas ir tehnisks termins, ko izmanto privātdetekktīvi, lai aprakstītu to, ka personisku informāciju par citiem iegūst ar uzdodoties par citu personu, parasti pa telefonu. Lietā, kas 1999. gada 21. aprīlī iesniegta Kolorado federālajā tiesā, tiek prasīts izdot izpildrakstu un atmaksāt visu nelikumīgi gūto peļņu.

Sakrītoša jurisdikcija

Visbeidzot, Jūs uzdevāt jautājumu par *FTC* jurisdikcijas mijiedarbību ar citu tiesību aizsardzības iestāžu jurisdikciju, jo īpaši gadījumos, kad jurisdikcijas, iespējams, sakrīt. Mums ir izveidojušās ciešas darba attiecības ar vairākām citām

⁽¹⁾ Lēmums par to, vai rīcībā ir “negodīga rīcība nodarbinātības jomā” vai kolektīvā līguma pārkāpums ir tehnisks jautājums, ko parasti izskata kompetentas darba tiesas, piemēram, šķīrējtiesas un *NRLB*, kuras izskatīs sūdzības.

⁽²⁾ Kā Jums ir zināms no iepriekšējām debatēm, *Fair Credit Reporting Act* arī pilnvaro *FTC* aizsargāt patērētāju finanšu privātumu tā darbības jomā, un Komisija nesen izdeva lēmumu, kas attiecas uz šo jautājumu. Skat. *In the Matter of Trans Union*, lieta Nr. 9255 (2000. gada 1. marts) (paziņojums preseī un atzinums ir pieejams Interneta adresē www.ftc.gov/os/2000/03/index.htm#1).

⁽³⁾ Civilprasība 99-WM-783 (*D. Colo.*) (pieejama Interneta adresē <http://www.ftc.gov/opa/1999/9904/touchtone.htm>) (nosacītās piekrišanas spriedums nav pieņemts).

tiesību aizsardzības iestādēm, ieskaitot federālās banku iestādes un valsts ģenerālprokurorus. Mēs ļoti bieži koordinējam izmeklēšanas, lai maksimāli izmantotu mūsu resursus gadījumos, kad jurisdikcijas sakrīt. Mēs arī bieži iesniedzam lietas izskatīšanai attiecīgajā federālajā vai valsts iestādē.

Es ceru, ka šis pārskats būs noderīgs. Lūdzu, dariet man zināmu, ja Jums ir vajadzīga papildu informācija.

Ar cieņu,

Robert Pitofsky

VI PIELIKUMS

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

Godātais ģenerāldirektor Moga kungs!

Sūtu Jums šo vēstuli pēc ASV Tirdzniecības ministrijas pieprasījuma, lai izskaidrotu Tirdzniecības ministrijas nozīmi patērētāju privātās dzīves aizsardzībā attiecībā uz informāciju, ko tai sniedz aviosabiedrības.

Tirdzniecības ministrija atbalsta pašregulēšanos kā neuzbāzīgāko un efektīvāko veidu, kā nodrošināt tās informācijas privātumu, kuru patērētāji sniedz aviosabiedrībām, un attiecīgi atbalsta "drošības zonas" režīma izvedi, kas ļautu aviosabiedrībām ievērot Eiropas Savienības privātuma direktīvas prasības attiecībā uz datu nosūtīšanu ārpus ES. Tomēr ministrija atzīst, ka, lai pašregulatīvi centieni būtu veiksmīgi, ir svarīgi, lai aviosabiedrības, kas apņemas ievērot "drošības zonas" režīmā noteiktos privātuma principus, tiešām to arī darītu. Šajā sakarā pašregulēšanās jāapvieno ar tiesībaizsardzību. Tādēļ, izmantojot savas pašreizējās pilnvaras attiecībā uz patērētāju aizsardzību, ministrija publiskos aviosabiedrību apņemšanos ievērot privātumu un izskatīs lietas par iespējamām pārkāpumiem, ko mēs saņemam no pašregulatīvām organizācijām un citām personām, tostarp Eiropas Savienības dalībvalstīm.

Ministrijas pilnvaras veikt izpildes darbību šajā jomā balstās uz U. S. C. 49. sadaļas 41712. paragrāfu, kurš aizliedz pārvadātājam, pārdodot gaisa transporta pakalpojumus, iesaistīties "negodīgā vai maldinošā rīcībā vai negodīgā konkurences veidā", kas rada vai var radīt kaitējumu patērētājiem. Sadaļas 41712. paragrāfs ir formulēts pēc *Federal Trade Commission Act* 5. paragrāfa parauga (15 U. S. C. 45). Tomēr saskaņā ar 15 U. S. C. 45(a)(2) *Federal Trade Commission* ir atbrīvojusi gaisa pārvadātājus no 5. paragrāfa noteikumu ievērošanas.

Mans birojs izmeklē un ierosina lietas saskaņā ar U. S. C. 49. sadaļas 41712. paragrāfu. (Skat. Transporta ministrijas rīkojumus 99-11-5, 1999. gada 9. novembris; 99-8-23, 1999. gada 26. augusts; 99-6-1, 1999. gada 1. jūnijs; 98-6-24, 1998. gada 22. jūnijs; 98-6-21, 1998. gada 19. jūnijs; 98-5-31, 1998. gada 22. maijs un 97-12-23, 1997. gada 18. decembris.) Mēs šādas lietas ierosinām, pamatojoties uz mūsu veikto izmeklēšanu, kā arī formālām un neformālām sūdzībām, ko saņemam no indivīdiem, ceļojumu aģentiem, aviosabiedrībām, kā arī ASV un ārzemju valdības iestādēm.

Vēlētos norādīt, ka tas, pārvadātājs neievēro no pasažieriem saņemtās informācijas slepenību, *per se* nav 41712. paragrāfa pārkāpums. Tomēr, ja pārvadātājs ir formāli un publiski apņēmis ievērot "drošības zonas" principu, kas paredz neizpaust iegūto patērētāju informāciju, ministrija būtu tiesīga izmantot 41712. paragrāfā noteiktās pilnvaras, lai panāktu šo principu ievērošanu. Tādēļ, ja pasažieris ir sniedzis informāciju pārvadātājam, kas ir apņēmis ievērot "drošības zonas" principus, neizpilde visticamāk nodarītu patērētājiem kaitējumu, un tas būtu 41712. paragrāfa pārkāpums. Mans birojs piešķirtu augstu prioritātes pakāpi visu šādu iespējamu darbību izmeklēšanai un lietu ierosināšanai. Mēs arī sniegsim Tirdzniecības ministrijai informāciju par šādu lietu iznākumu.

Sadaļas 41712. pārkāpumu rezultātā var izdot rīkojumus par nelikumīgas darbības aizliegšanu un saukt pie civiltiesiskās atbildības par šo rīkojumu neievērošanu. Kaut gan mūsu pilnvarās neietilpst kaitējuma atlīdzināšana vai finansiālas kompensācijas sniegšana individuāliem prasību iesniedzējiem, mūsu pilnvarās ietilpst to nolēmumu apstiprināšana, ko izdod saistībā ar izmeklēšanu, un lietas, kuras iesniegusi ministrija un kuras sniedz patērētājiem zināmu kompensāciju, vai nu samazinot sodu vai sedzot maksājamo sodu. Mēs to jau esam darījuši agrāk, un mēs varam to darīt un darīsim saistībā ar "drošības zonas" principiem, kad apstākļi to prasa. Jebkuras ASV aviosabiedrības atkārtoti 41712. paragrāfa pārkāpumi radītu arī jautājumu par aviosabiedrības spēju ievērot atbilstību, un tā rezultātā ārkārtējās situācijās varētu atzīt, ka aviosabiedrība vairs nespēj darboties un tādēļ zaudē savas ekonomiskās tiesības darboties. (Skat. Transporta ministrijas rīkojumus 93-6-34, 1993. gada 23. jūnijs, un 93-6-11, 1993. gada 9. jūnijs.

Kaut gan šie procesi neattiecas uz 41712. paragrāfu, to rezultātā pārvadātājam par pilnīgu *Federal Aviation Act* noteikumu, divpusējā līguma un ministrijas noteikumu neievērošanu atpēma tiesības darboties.)

Es ceru, ka šī informācija būs noderīga. Ja Jums ir kādi jautājumi vai ir vajadzīga papildu informācija, lūdzu nekavējieties ar mani sazināties.

Ar cieņu,

Samuel Podberesky

Galvenā juriskonsulta vietnieks aviācijas
tiesībaizsardzības un procesuālajos jautājumos

VII PIELIKUMS

Atsaucoties uz 1. panta 2. punkta b) apakšpunktu, ja nav ievēroti saskaņā ar FAQ īstenotie principi, šādas Amerikas Savienoto Valstu valdības iestādes ir pilnvarotas izmeklēt sūdzības un panākt palīdzību negodīgas vai maldinošas rīcības novēršanai, kā arī iegūt kompensācijas indivīdiem, neatkarīgi no viņi mītnes valsts vai valstiskās piederības:

1. *Federal Trade Commission* un
2. ASV Tirdzniecības ministrija.

Federal Trade Commission rīkojas, pamatojoties uz pilnvarām, kas noteiktas *Federal Trade Commission Act* 5. paragrāfā. Saskaņā ar 5. paragrāfu *Federal Trade Commission* jurisdikcija neattiecas uz bankām, krājaizdevu sabiedrībām un kredītsabiedrībām; telekomunikāciju uzņēmumiem, starpstatu pārvadātājiem, gaisa pārvadātājiem, fasētājiem un lopu ganāmpulku pārraugiem. Kaut gan apdrošināšanas nozare nav īpaši iekļauta 5. paragrāfa izņēmumu sarakstā, *McCarran-Ferguson Act* ⁽¹⁾ parasti ļauj apdrošināšanas darījumus reglamentēt katram štatam atsevišķi. Tomēr *FTC Act* noteikumi attiecas uz apdrošināšanas nozari, ja valsts tiesību akti šādus darījumus nereglamentē. *FTC* saglabā pārējās pilnvaras attiecībā uz apdrošināšanas sabiedrību negodīgu vai maldinošu rīcību, ja tās nedarbojas apdrošināšanas nozarē.

ASV Tirdzniecības ministrija darbojas, pamatojoties uz pilnvarām, kas noteiktas *United States Code* 49. sadaļas 41712. paragrāfā. ASV Tirdzniecības ministrija ierosina lietas, pamatojoties uz savu veikto izmeklēšanu, kā arī formālām un neformālām sūdzībām, ko tā saņem no indivīdiem, ceļojumu aģentiem, aviosabiedrībām, kā arī ASV un ārzemju valdības iestādēm.

⁽¹⁾ U. S. C. § 1011 et seq.