EIROPAS
KOMISIJA

Briselē, 27.11.2013.
COM(2013) 847 final

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

par „drošības zonas” darbību no ES pilsoņu un uzņēmumu, kas veic uzņēmējdarbību ES, viedokļa

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

par „drošības zonas" darbību no ES pilsoņu un uzņēmumu, kas veic uzņēmējdarbību ES, viedokļa

1. IEVADS

Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvā 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (turpmāk "Datu aizsardzības direktīva") ir paredzēti noteikumi par personas datu pārsūtīšanu no ES dalībvalstīm uz citām valstīm ārpus ES[1], ciktāl uz šādu pārsūtīšanu attiecas šā instrumenta darbības joma[2].

Saskaņā ar minēto direktīvu Komisija var konstatēt, ka trešā valsts nodrošina pietiekamu aizsardzības līmeni, īstenojot tās iekšzemes tiesību aktus vai starptautiskās saistības, ko tā uzņēmusies, lai aizsargātu indivīdu tiesības; tādā gadījumā konkrētie ierobežojumi datu pārsūtīšanai uz šādu valsti nav piemērojami. Šādus lēmumus parasti sauc par "**pietiekamības lēmumiem**".

Komisija 2000. gada 26. jūlijā pieņēma Lēmumu 520/2000/EK[3] (turpmāk "**Lēmums par „drošības zonu"**"), kurā tā atzina Amerikas Savienoto Valstu Tirdzniecības ministrijas izdotos privātuma „drošības zonas" principus un biežāk uzdotos jautājumus (attiecīgi "principi" un "*FAQ*") par tādiem, kas nodrošina pietiekamu aizsardzību personas datu pārsūtīšanā no ES. Lēmums par „drošības zonu" tika pieņemts pēc 29. panta darba grupas atzinuma un 31. panta komitejas atzinuma, ko sniedza ar dalībvalstu kvalificētu vairākumu. Saskaņā ar Padomes Lēmumu 1999/468/EK Eiropas Parlaments veica Lēmuma par „drošības zonu" iepriekšēju kontroli.

Tās rezultātā ar pašreizējo Lēmumu par „drošības zonu" ir atļauta personiska rakstura informācijas brīva pārsūtīšana[4] no ES dalībvalstīm[5] uz tādiem uzņēmumiem ASV, kuri apņēmušies ievērot principus, apstākļos, kad šāda pārsūtīšana citādi neatbilstu ES standartiem par datu aizsardzības pietiekamu līmeni, ņemot vērā būtiskās privātuma tiesiskā regulējuma atšķirības abos Atlantijas okeāna krastos.

Pašreizējā „drošības zonas" shēmas darbība paļaujas uz iesaistīto uzņēmumu apņemšanos un pašsertifikāciju. Pieteikšanās šai shēmai ir brīvprātīga, bet tiem, kuri piesakās, noteikumi ir saistoši. Šīs shēmas pamatprincipi ir šādi:

(a) iesaistīto uzņēmumu slepenības [privātuma] politikas pārredzamība;

(b) „drošības zonas" principu iekļaušana uzņēmumu slepenības politikā un

---

1 Datu aizsardzības direktīvas 25. un 26. pantā ir paredzēts tiesiskais regulējums personas datu pārsūtīšanai no ES uz trešām valstīm ārpus EEZ.

2 Papildu noteikumi ir paredzēti 2008. gada 27. novembra Pamatlēmuma 2008/977/TI par tādu personas datu aizsardzību, ko apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās, 13. pantā, ciktāl šāda pārsūtīšana attiecas uz personas datiem, ko viena dalībvalsts pārsūta vai dara pieejamus citai dalībvalstij, kura ir iecerējusi šādus datus vēlāk pārsūtīt trešai valstij vai starptautiskai struktūrai noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas vai kriminālvajāšanas nolūkos vai krimināl sodu izpildes nolūkā.

3 Komisijas 2000. gada 26. jūlija Lēmums 2000/520/EK 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, OV L 215, 28.8.2000., 7. lpp.

4 Minētais neizslēdz iespēju datu apstrādei piemērot citas prasības, kādas var būt spēkā saskaņā ar valsts tiesību aktiem, ar kuriem īsteno ES Datu aizsardzības direktīvu.

5 Kopš Direktīvas 95/46/EK darbības joma tika paplašināta, aptverot arī EEZ līgumu, līdzīgi tiek ietekmēta datu pārsūtīšana no trim EEZ dalībvalstīm,; 1999. gada 25. jūnija Lēmums 83/1999, OV L 296/41, 23.11.2000.

(c) šo principu piemērošanas nodrošināšana, tostarp ar publisko iestāžu darbību.

Šis „drošības zonas" pamats ir jāpārskata, ņemot vērā **jauno kontekstu**, ko rada:

(a) to datu plūsmu eksponenciāla palielināšanās, kuras līdz šim bija palīgrakstura, bet kurām pašlaik ir galvenā nozīme digitālās ekonomikas straujajā izaugsmē un tik ļoti svarīgajās datu vākšanas, apstrādes un izmantošanas norisēs;

(b) datu plūsmu nozīmīgums, jo īpaši transatlantiskajai ekonomikai[6],

(c) to ASV uzņēmumu skaita straujā palielināšanās, kuri ir iesaistījušies „drošības zonas" shēmā; kopš 2004. gada tas ir palielinājies astoņas reizes (no 400 uzņēmumiem 2004. gadā līdz 3246 uzņēmumiem 2013. gadā);

(d) nesen publiskotā informācija par ASV novērošanas programmām, kas rada jaunus jautājumus par aizsardzības līmeni, kuru vajadzētu garantēt „drošības zonai".

Šajos apstākļos šajā paziņojumā sniegts pārskats par „drošības zonas" shēmas darbību. Tas ir **pamatots uz pierādījumiem**, ko apkopojusi Komisija, darbu, ko 2009. gadā veikusi ES un ASV kontaktgrupa privātuma jautājumos, pētījumu, ko 2008. gadā veicis neatkarīgs līgumslēdzējs[7], un informāciju, ko saņēmusi ES un ASV *ad-hoc* darba grupa ("Darba grupa"), kura izveidota pēc atklātībā nonākušās informācijas par ASV novērošanas programmām *(sk. paralēlo dokumentu)*. Šis paziņojums seko diviem **Komisijas novērtējuma ziņojumiem**, kas sniegti „drošības zonas" shēmas darbības sākumposmā, attiecīgi 2002. gadā[8] un 2004. gadā[9].

2. „DROŠĪBAS ZONAS" STRUKTŪRA UN DARBĪBA

2.1. „Drošības zonas" struktūra

ASV uzņēmumam, kas vēlas iesaistīties „drošības zonā", a) savā publiski pieejamā slepenības politikā jānorāda, ka tas ievēro un faktiski piemēro principus, kā arī b) jāveic pašsertifikācija, t. i., jāpaziņo ASV Tirdzniecības ministrijai, ka tas ievēro principus. Pašsertifikācijas pieteikums jāiesniedz atkārtoti katru gadu. Privātuma „drošības zonas" principos, kas iekļauti Lēmuma par „drošības zonu" I pielikumā, ir ietvertas prasības attiecībā uz personas datu materiāltiesisko aizsardzību (datu integritātes, drošības, izvēles un tālākas pārsūtīšanas principi) un datu subjektu procesuālajām tiesībām (informēšanas, piekļuves un piemērošanas principi).

Attiecībā uz „drošības zonas" shēmas piemērošanas nodrošināšanu ASV svarīga nozīme ir divām ASV iestādēm — ASV Tirdzniecības ministrijai un ASV Federālajai tirdzniecības komisijai.

Tirdzniecības ministrija izskata katru no uzņēmumiem saņemto „drošības zonas" pašsertifikācijas un katru atkārtotas gada sertifikācijas iesniegumu, lai pārliecinātos, ka tajos ir

---

6 Saskaņā ar dažiem pētījumiem, ja pakalpojumi un pārrobežu datu plūsmas būtu jāpārtrauc, jo tiktu pārtraukta uzņēmumu saistošo noteikumu, līgumu noteikumu paraugu un „drošības zonas" piemērošana, negatīvā ietekme uz ES IKP varētu sasniegt no –0,8 % līdz –1,3% ,un ES pakalpojumu eksports uz ASV samazinātos par –6,7 % konkurētspējas zaudēšanas dēļ. Sk. Eiropas Starptautiskās politiskās ekonomikas centra (*European Centre for International Political Economy*) pētījumu ASV Tirdzniecības ministrijai "*The Economic Importance of Getting Data Protection Right*", 2013. gada marts.

7 Ietekmes novērtējums, ko Eiropas Komisijai 2008. gadā sagatavoja Namīras Universitātes *Centre de Recherche Informatique et Droit* ("*CRID*").

8 Komisijas dienestu darba dokuments "Komisijas 2000. gada 26. jūlija Lēmuma 2000/520/EK atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK par personas datu pienācīgu aizsardzību, kas noteikta ar privātuma „drošības zonas" principiem un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija, piemērošana", SEC(2002)196, 13.12.2002.

9 Komisijas dienestu darba dokuments " Komisijas Lēmuma 520/2000/EK par personas datu pienācīgu aizsardzību, kas noteikta ar privātuma „drošības zonas" principiem un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija, īstenošana", SEC(2004)1323, 20.10.2004.

ietverti visi elementi, kas nepieciešami, lai varētu piedalīties shēmā[10]. Tā atjaunina to uzņēmumu sarakstu, kuri iesnieguši pašsertifikācijas vēstules, un sarakstu un vēstules publicē savā tīmekļa vietnē. Tā arī uzrauga "drošības zonas" darbību un no saraksta svītro tos uzņēmumus, kuri neievēro principus.

Federālā tirdzniecības komisija atbilstoši savām pilnvarām patērētāju tiesību aizsardzības jomā vēršas pret negodīgu vai maldinošu rīcību saskaņā ar Federālās tirdzniecības komisijas likuma 5. pantu. Federālās tirdzniecības komisijas īstenotie piemērošanas nodrošināšanas pasākumi ietver izmeklēšanu saistībā ar nepatiesiem apgalvojumiem par „drošības zonas" ievērošanu un saistībā ar neatbilstību šiem principiem uzņēmumos, kas ir shēmas dalībnieki. Gadījumos, kad „drošības zonas" principu piemērošanas nodrošināšanas pasākumi ir vērsti pret gaisa pārvadātājiem, kompetentā iestāde ir ASV Satiksmes ministrija[11].

Pašreizējais Lēmums par „drošības zonu" ir daļa no ES tiesiskā regulējuma, kas dalībvalstu iestādēm ir jāpiemēro. Saskaņā ar minēto lēmumu ES valstu **datu aizsardzības iestādēm** (DAI) konkrētos gadījumos ir tiesības pārtraukt datu pārsūtīšanu sertificētajiem „drošības zonas" uzņēmumiem[12]. Komisijai nav informācijas par kādas valsts datu aizsardzības iestādes veiktas pārtraukšanas gadījumiem kopš „drošības zonas" izveides 2000. gadā. Neatkarīgi no pilnvarām, kas ES valstu datu aizsardzības iestādēm piešķirtas ar Lēmumu par „drošības zonu", tās ir kompetentas iejaukties, tostarp starptautiskas datu pārsūtīšanas gadījumos, lai nodrošinātu 1995. gada Datu aizsardzības direktīvā noteikto vispārējo principu ievērošanu.

Kā atgādināts pašreiz spēkā esošajā Lēmumā par „drošības zonu", **Komisija ir kompetenta** saskaņā ar Regulā (ES) Nr. 182/2011 paredzēto pārbaudes procedūru jebkurā laikā pielāgot lēmumu, to apturēt vai ierobežot lēmuma darbības jomu, ņemot vērā pieredzi tā īstenošanā. Tas īpaši ir paredzēts gadījumā, ja ASV to sistemātiski neizpilda, piemēram, ja struktūra, kas atbildīga par privātuma „drošības zonas" principu ievērošanas nodrošināšanu Amerikas Savienotajās Valstīs, savu pienākumu nepilda efektīvi vai ja ASV tiesību aktu prasības tiek uzskatītas par svarīgākām nekā aizsardzības līmenis, ko nodrošina „drošības zonas" principi. Šo lēmumu tāpat kā jebkuru citu Komisijas lēmumu var arī grozīt citu iemeslu dēļ vai pat atcelt.

2.2. „Drošības zonas" darbība

Starp **3246[13] sertificētajiem uzņēmumiem** ir gan mazi, gan lieli uzņēmumi[14]. Lai gan uz finanšu pakalpojumu un telesakaru nozarēm neattiecas Federālās tirdzniecības komisijas pilnvaras nodrošināt piemērošanu, un tāpēc tās nav iekļautas „drošības zonā", sertificēto uzņēmumu vidū ir daudzas rūpniecības un pakalpojumu nozares, tostarp labi zināmi interneta uzņēmumi un nozares, sākot no informācijas un datoru pakalpojumiem, līdz farmācijai, ceļojumu un tūrisma pakalpojumiem, veselības aprūpes vai kredītkaršu pakalpojumiem[15]. Tie

---

10 Ja uzņēmuma sertifikācija vai pašsertifikācija neatbilst „drošības zonas" prasībām, Tirdzniecības ministrija informē uzņēmumu, pieprasot, lai pirms uzņēmuma sertifikācijas pabeigšanas tiktu veikti noteikti pasākumi (piemēram, precizējumi, grozījumi politikas aprakstā).

11 Saskaņā ar ASV Kodeksa 41712. sadaļas 49. iedaļu.

12 Konkrētāk, pārsūtīšanas pārtraukšanu var pieprasīt divās situācijās:
a) kad ASV valdības iestāde ir noteikusi, ka uzņēmums neievēro privātuma „drošības zonas" principus, vai
b) kad ir liela iespējamība, ka privātuma „drošības zonas" principi nav ievēroti; ir pamats uzskatīt, ka attiecīgais piemērošanas mehānisms neietver vai neietvers piemērotus un savlaicīgus pasākumus, lai attiecīgo gadījumu atrisinātu; pārsūtīšanas 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.

13 To „drošības zonas" organizāciju skaits, kuras iekļautas „drošības zonas" sarakstā kā "**aktuālas**", 2013. gada 26. septembrī bija **3246,** bet "**neaktuālo**" organizāciju skaits bija **935.**

14 "Drošības zonas" organizācijas ar 250 vai mazāk darbiniekiem — 60 **%** (1925 no 3246). "Drošības zonas" organizācijas ar 251 vai vairāk darbiniekiem — **40 %** (1295 no 3246).

15 Piemēram, *MasterCard* veic darījumus ar tūkstošiem banku, un šis uzņēmums ir uzskatāms piemērs gadījumam, kad „drošības zonu" nevar aizstāt ar citiem personas datu pārsūtīšanas juridiskiem instrumentiem, piemēram, uzņēmumu saistošiem noteikumiem vai līgumu noteikumiem.

ir pārsvarā ASV uzņēmumi, kas sniedz pakalpojumus ES iekšējā tirgū. To vidū ir arī dažu ES uzņēmumu, piemēram, *Nokia* vai *Bayer*, filiāles. No tām 51 % ir uzņēmumi, kas Eiropā apstrādā darbinieku datus, kurus pārsūta uz ASV cilvēkresursu pārvaldes vajadzībām[16].

Ir **palielinājušās** dažu ES datu aizsardzības iestāžu **bažas** par datu pārsūtīšanu saskaņā ar pašreizējo „drošības zonas" shēmu. Dažu dalībvalstu datu aizsardzības iestādes ir kritizējušas principu ļoti vispārīgo formulējumu un lielo paļaušanos uz pašsertifikāciju un pašregulāciju. Līdzīgas bažas ir paudusi rūpniecības nozare, kas atsaucas uz konkurences izkropļojumiem, ko rada nepietiekamā piemērošana.

Pašreizējās „drošības zonas" shēmas pamatā ir principu brīvprātīga ievērošana uzņēmumos, principus ievērojošo uzņēmumu pašsertifikācija un publisko iestāžu nodrošinātā pašsertifikācijas saistību piemērošana. Šajā saistībā ikviens pārredzamības trūkums un jebkādi piemērošanas trūkumi grauj „drošības zonas" shēmas pamatus.

Jebkādi ASV puses trūkumi pārredzamības vai piemērošanas nodrošināšanas jomā noved pie tā, ka atbildība tiek novirzīta uz Eiropas datu aizsardzības iestādēm un uzņēmumiem, kas izmanto shēmu. Vācijas datu aizsardzības iestādes 2010. gada 29. aprīlī pieņēma lēmumu, pieprasot uzņēmumiem, kas pārsūta datus no Eiropas uz ASV, aktīvi pārbaudīt, vai uzņēmumi ASV, kas importē datus, faktiski ievēro privātuma „drošības zonas" principus, un iesakot, ka "vismaz eksportētājam uzņēmumam ir jānosaka, vai importētāja „drošības zonas" sertifikācija joprojām ir spēkā"[17].

Vācijas DAI pēc atklātībā nonākušās informācijas par ASV novērošanas programmām 2013. gada 24. jūlijā turklāt izteica bažas, ka "pastāv liela iespējamība, ka Komisijas lēmumos noteiktie principi nav ievēroti"[18]. Dažas DAI (piemēram, Brēmenes DAI) ir pieprasījušas, lai uzņēmums, kas pārsūta personas datus ASV pakalpojumu sniedzējiem, informētu DAI par to, vai un kā attiecīgie pakalpojumu sniedzēji novērš Valsts drošības aģentūras piekļuvi. Īrijas DAI ir ziņojusi, ka tā nesen, pēc atklātībā nonākušās informācijas par ASV izlūkdienestu programmām, saņēmusi divas sūdzības, kas attiecas uz „drošības zonas" programmu, bet atteikusies tās izskatīt, pamatojoties uz to, ka personas datu pārsūtīšana trešai valstij atbilst Īrijas datu aizsardzības tiesību aktiem. Pēc līdzīgas sūdzības saņemšanas Luksemburgas DAI konstatēja, ka *Microsoft* un *Skype* datu pārsūtīšanā uz ASV ievēro Luksemburgas Datu aizsardzības likumu[19]. Tomēr Īrijas Augstā tiesa kopš tā laika ir pieņēmusi izskatīšanai tiesā prasību, saskaņā ar kuru tā izvērtēs Īrijas datu aizsardzības komisāra bezdarbību attiecībā uz ASV novērošanas programmām. Vienu no šīm divām sūdzībām iesniedza studentu grupa *Europe v Facebook* (*EvF*), kas līdzīgu sūdzību pret *Yahoo* iesniedza Vācijā, un to izskata attiecīgās datu aizsardzības iestādes.

Šī datu aizsardzības iestāžu atšķirīgā reakcija uz atklātībā nonākušo informāciju par novērošanu liecina par reālu „drošības zonas" shēmas sadrumstalotības risku un rada jautājumus par to, ciktāl tiek nodrošināta shēmas piemērošana.

---

16 „Drošības zonas" organizācijas, kuru „drošības zonas" sertifikācija ietver organizācijas cilvēkresursu datus (un kuras tādējādi ir piekritušas sadarboties ar ES datu aizsardzības iestādēm un ievērot to noteikumus): **51 %** (1671 no 3246).

17 Sk. *Düsseldorfer Kreis* 2010. gada 28./29. aprīļa lēmumu. Sk. *Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover*: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile Tomēr Eiropas Datu aizsardzības uzraudzītājs (EDAU) *Peter Hustinx* Eiropas Parlamenta *LIBE* komitejas izmeklēšanas ietvaros 2013. gada 7. oktobrī pauda nostāju, ka attiecībā uz „drošības zonu" "ir panākti būtiski uzlabojumi un ir atrisināta lielākā daļa jautājumu": https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf

18 Sk. Vācijas datu aizsardzības komisāru konferences rezolūciju, kurā norādīts, ka izlūkdienesti rada būtiskus draudus datu plūsmām starp Vāciju un valstīm ārpus Eiropas: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870

19 Sk. Luksemburgas DAI sniegto paziņojumu presei 2013. gada 18. novembrī.

3. PRINCIPUS IEVĒROJOŠO UZŅĒMUMU SLEPENĪBAS POLITIKAS PĀRREDZAMĪBA

Saskaņā ar *FAQ* 6, kas pievienots Lēmumam par „drošības zonu" (II pielikums), uzņēmumiem, kuri ir ieinteresēti sertifikācijā „drošības zonas" ietvaros, jāiesniedz Tirdzniecības ministrijai un jāpublisko sava slepenības politika. Tajā jāiekļauj apņemšanās ievērot privātuma principus. Prasība **nodrošināt** pašsertificētu uzņēmumu **slepenības politikas publisku pieejamību** un to apņemšanās ievērot privātuma principus ir būtiska shēmas darbībai.

Šādu uzņēmumu slepenības politikas nepietiekama pieejamība kaitē indivīdiem, kuru personas dati tiek vākti un apstrādāti, un var būt **informēšanas principa pārkāpums**. Tādos gadījumos indivīdi, kuru dati tiek pārsūtīti no ES, var nebūt informēti par viņu tiesībām un pienākumiem, kas ir saistoši pašsertificētam uzņēmumam.

Turklāt uzņēmumu apņemšanās ievērot privātuma principus **ļauj Federālajai tirdzniecības komisijai** neatbilstības gadījumos attiecībā uz uzņēmumiem **īstenot tās pilnvaras nodrošināt šo principu piemērošanu** , neatbilstību kvalificējot kā negodīgu vai maldinošu rīcību. Pārredzamības trūkums, ko pieļauj uzņēmumi ASV, sarežģī Federālās tirdzniecības komisijas īstenoto uzraudzību un grauj piemērošanas nodrošināšanas efektivitāti.

Gadu gaitā ievērojams skaits pašsertificētu uzņēmumu nav publiskojis savu slepenības politiku un/vai nav sniedzis publisku paziņojumu par privātuma principu ievērošanu. 2004. gada ziņojumā par „drošības zonu" ir norādīts uz vajadzību Tirdzniecības ministrijai **īstenot aktīvāku nostāju** šīs prasības **izpildes pārbaudīšanā**.

Kopš 2004. gada Tirdzniecības ministrija ir izstrādājusi **jaunus informācijas rīkus**, lai palīdzētu uzņēmumiem izpildīt to saistības pārredzamības jomā. Attiecīgā informācija par shēmu ir pieejama Tirdzniecības ministrijas specializētajā „drošības zonas" vietnē[20], kurā uzņēmumi var arī augšupielādēt savu slepenības politiku. Tirdzniecības ministrija ir ziņojusi, ka uzņēmumi izmanto šo iespēju un publicē savu slepenības politiku Tirdzniecības ministrijas tīmekļa vietnē, kad tie piesakās dalībai „drošības zonā"[21]. Tirdzniecības ministrija no 2009. gada līdz 2013. gadam turklāt publicēja vairākas pamatnostādnes uzņēmumiem, kuri vēlas pievienoties „drošības zonai", piemēram, "Pašsertifikācijas rokasgrāmatu" un "Noderīgus padomus par atbilstību pašsertifikāciju principiem"[22].

Tas, ciktāl uzņēmumi izpilda pārredzamības saistības, atšķiras. Daži uzņēmumi tikai dara zināmu Tirdzniecības ministrijai savas slepenības politikas aprakstu kā daļu no pašsertifikācijas procesa, bet lielākā daļa uzņēmumu šo politiku publisko savā tīmekļa vietnē un to arī augšupielādē Tirdzniecības ministrijas tīmekļa vietnē. Tomēr šī **politika ne vienmēr ir noformēta patērētājiem draudzīgā un viegli uztveramā veidā**. Hipersaites uz slepenības politiku ne vienmēr pietiekami labi darbojas un ne vienmēr norāda uz pareizajām tīmekļa vietnēm.

No lēmuma un tā pielikumiem izriet, ka prasība uzņēmumiem publiskot savu slepenības politiku **ietver ne tikai** Tirdzniecības ministrijas **informēšanu** par pašsertifikāciju. *FAQ* noteiktajās sertifikācijas prasībās ir ietverta prasība sniegt slepenības politikas aprakstu un pārredzamu informāciju par to, kur politika ir pieejama publiskai aplūkošanai[23]. Paziņojumiem par slepenības politiku jābūt skaidri saprotamiem un viegli pieejamiem

---

20 http://www.export.gov/SafeHarbour/

21 https://SafeHarbour.export.gov/list.aspx

22 Rokasgrāmata ir pieejama shēmas tīmekļa vietnē http://export.gov/SafeHarbour/, un noderīgie padomi ir pieejami tīmekļa vietnē http://export.gov/SafeHarbour/eu/eg_main_018495.asp

23 Tirdzniecības ministrija 2013. gada 12. novembrī apstiprināja, ka "mūsdienās uzņēmumiem, kam ir publiskas tīmekļa vietnes un kas strādā ar patērētāju/klientu/apmeklētāju datiem, savā tīmekļa vietnē jāpublicē „drošības zonai" atbilstoša slepenības politika" (dokuments "*U.S.-EU Cooperation to Implement the Safe Harbor Framework*", 2013. gada 12. novembris).

sabiedrībai. Tajos jāiekļauj hipersaite uz Tirdzniecības ministrijas „drošības zonas" tīmekļa vietni, kurā uzskaitīti visi shēmas "aktuālie" dalībnieki, un saite uz strīdu alternatīvas izšķiršanas pakalpojumu sniedzēju. Tomēr vairāki shēmā iesaistītie uzņēmumi laikposmā no 2000. gada līdz 2013. gadam šīs prasības neizpildīja. Darba saziņā ar Komisiju 2013. gada februārī Tirdzniecības ministrija apliecināja, ka līdz 10 % sertificēto uzņēmumu, iespējams, faktiski nav savā tīmekļa vietnē publicējuši slepenības politiku, kurā ietverts apstiprinošs paziņojums par „drošības zonu".

Neseni statistikas dati liecina arī par pastāvīgu problēmu, ka tiek sniegti **nepatiesi apgalvojumi par „drošības zonas" principu ievērošanu**. Aptuveni 10 % uzņēmumu, kas norādījuši, ka tie esot „drošības zonas" dalībnieki, nav iekļauti Tirdzniecības ministrijas sarakstā kā shēmas aktuālie dalībnieki[24]. Šādus nepatiesus apgalvojumus izsaka gan uzņēmumi, kas nekad nav bijuši „drošības zonas" dalībnieki, gan uzņēmumi, kas reiz ir pievienojušies šai shēmai, bet vēlāk nav Tirdzniecības ministrijā veikuši atkārtotu ikgadējo pašsertifikāciju. Tādā gadījumā tie joprojām ir norādīti „drošības zonas" tīmekļa vietnē, tikai ar sertifikācijas statusu "neaktuāls", kas nozīmē, ka uzņēmums ir bijis shēmas dalībnieks un tāpēc tam ir pienākums turpināt nodrošināt jau apstrādāto datu aizsardzību. Federālā tirdzniecības komisija ir kompetenta iejaukties maldinošas rīcības gadījumos un gadījumos, kad netiek ievēroti „drošības zonas" principi (sk. 5.1. sadaļu). Neskaidrība par "nepatiesiem apgalvojumiem" ietekmē shēmas ticamību.

Eiropas Komisija 2012. un 2013. gadā regulārā saziņā brīdināja Tirdzniecības ministriju, ka, lai izpildītu pārredzamības saistības, nepietiek tikai ar to, ka uzņēmumi Tirdzniecības ministrijai iesniedz savas slepenības politikas aprakstu. Paziņojumiem par slepenības politiku jābūt publiski pieejamiem. Tirdzniecības ministrijai arī tika prasīts **pastiprināt savu periodisko kontroli attiecībā uz uzņēmumu tīmekļa vietnēm**, pirms tam veicot pārbaudes procedūru saistībā ar pirmo pašsertifikācijas procesu vai tās ikgadējo atjaunošanu, un vērsties pret uzņēmumiem, kuri neizpilda pārredzamības prasības.

Atbildot uz ES bažām, **Tirdzniecības ministrija** vispirms **2013. gada martā noteica**, ka „drošības zonas" uzņēmumiem, kam ir publiska tīmekļa vietne, ir pienākums tajā viegli pieejamā veidā publiskot savu slepenības politiku attiecībā uz patērētāju/lietotāju datiem. Vienlaikus Tirdzniecības ministrija sāka informēt visus uzņēmumus, kuru slepenības politikā vēl nebija ietverta saite uz Tirdzniecības ministrijas tīmekļa vietni, ka tāda ir jāiekļauj, nodrošinot oficiālā „drošības zonas" saraksta un tīmekļa vietnes tiešu pieejamību patērētājiem, kuri apmeklē uzņēmuma tīmekļa vietni. Tas ļaus Eiropas datu subjektiem nekavējoties, bez papildu meklēšanas tīmeklī pārliecināties par uzņēmuma saistībām, par kuru uzņemšanos tas informējis Tirdzniecības ministrijai. Turklāt Tirdzniecības ministrija sāka informēt uzņēmumus, ka to publicētajā slepenības politikā jāiekļauj kontaktinformācija par uzņēmumu izmantoto neatkarīgo pakalpojumu sniedzēju strīdu izšķiršanai[25].

Šis process ir jāpaātrina, lai nodrošinātu, ka visi sertificētie uzņēmumi pilnībā izpilda „drošības zonas" prasības ne vēlāk kā līdz 2014. gada martam (t. i., līdz uzņēmumu ikgadējās atkārtotās sertifikācijas termiņam, skaitot no jauno prasību ieviešanas 2013. gada martā).

---

24 Austrālijas konsultāciju uzņēmums *Galexia* 2013. gada septembrī salīdzināja 2008. un 2013. gadā sniegtos nepatiesos apgalvojumus par dalību „drošības zonā". Tā galvenais konstatējums bija tāds, ka vienlaikus ar dalības paplašināšanos drošības zonā laikā no 2008. gada līdz 2013. gadam (no 1109 līdz 3246 dalībniekiem) nepatiesu apgalvojumu skaits palielinājies no 206 līdz 427. http://www.galexia.com/public/about/news/about_news-id225.html

25 Laikposmā no 2013. gada marta līdz septembrim Tirdzniecības ministrija:
• informēja 101 uzņēmumu, kas jau bija drošības zonas tīmekļa vietnē augšupielādējis savu privātuma „drošības zonai" atbilstošo slepenības politiku, ka tiem šī slepenības politika jāpublicē arī savā tīmekļa vietnē;
• informēja 154 uzņēmumus, kuri vēl to nebija izdarījuši, ka tiem savā slepenības politikā jāiekļauj saite uz „drošības zonas" tīmekļa vietni;
• informēja vairāk nekā 600 uzņēmumu, ka tiem savā slepenības politikā jāiekļauj sava neatkarīgā strīdu izšķiršanas pakalpojumu sniedzēja kontaktinformācija.

Tomēr turpina pastāvēt bažas par to, vai visi pašsertificētie uzņēmumi pilnībā izpilda pārredzamības prasības. Tirdzniecības ministrijai ir jāuzrauga un stingrāk jāpārbauda to saistību izpilde, kuras uzņēmumi uzņēmušies sākotnējās pašsertifikācijas un ikgadējās atjaunošanas brīdī.

4. „DROŠĪBAS ZONAS" PRIVĀTUMA PRINCIPU IEKĻAUŠANA UZŅĒMUMU SLEPENĪBAS POLITIKĀ

Lai iegūtu un saglabātu „drošības zonas" sniegtās priekšrocības, pašsertificētiem uzņēmumiem ir jāievēro privātuma principi, kas ir izklāstīti lēmuma I pielikumā.

Komisija 2004. gada ziņojumā konstatēja, ka ievērojams skaits **uzņēmumu** savā datu apstrādes politikā **nav pareizi iekļāvuši privātuma „drošības zonas" principus**. Piemēram, indivīdiem ne vienmēr tika sniegta skaidra un pārredzama informācija par to, kādiem mērķiem veikta viņu datu apstrāde, vai arī viņiem netika sniegta iespēja atteikties, kad to datus bija paredzēts izpaust trešai personai vai izmantot mērķim, kas nav saderīgs ar mērķiem, kādiem dati sākotnēji savākti. Komisijas 2004. gada ziņojumā tika atzīts, ka Tirdzniecības ministrijai *"vajadzētu būt aktīvākai attiecībā uz „drošības zonas" pieejamību un informētības veicināšanu par principiem"*[26].

Šajā ziņā ir panākts neliels progress. Kopš 2009. gada 1. janvāra Tirdzniecības ministrija izvērtē slepenības politiku katram uzņēmumam, kurš vēlas atjaunot sertifikācijas statusu attiecībā uz „drošības zonu" — un statuss ir jāatjauno katru gadu —, pirms tā atjauno šo statusu. Tomēr izvērtējuma tvērums ir ierobežots. **Netiek pilnībā izvērtēta faktiskā prakse** pašsertificētos uzņēmumos — ja tas tiktu veikts, tiktu būtiski palielināta pašsertifikācijas procesa ticamība.

Ņemot vērā Komisijas pieprasījumus Tirdzniecības ministrijai veikt pašsertificēto uzņēmumu stingrāku un sistemātiskāku pārraudzību, **pašlaik vairāk uzmanības tiek pievērsts jauniem iesniegumiem**. To jauno iesniegumu skaits, kuri nav pieņemti, bet ir nosūtīti atpakaļ uzņēmumiem uzlabojumu veikšanai slepenības politikā, laikposmā no 2010. gada līdz 2013. gadam būtiski palielinājās — tas divkāršojās attiecībā uz atkārtoti sertificējamiem uzņēmumiem un trīskāršojās attiecībā uz jauniem „drošības zonas" dalībniekiem[27]. Tirdzniecības ministrija ir Komisijai apliecinājusi, ka ikvienu sertifikāciju vai atkārtotu sertifikāciju iespējams pabeigt tikai tad, ja uzņēmuma slepenības politika atbilst visām prasībām, proti, ja tajā ir ietverta apstiprinoša apņemšanās ievērot attiecīgo privātuma „drošības zonas" principu kopumu un tā ir publiski pieejama. Uzņēmumiem savā „drošības zonas" saraksta uzskaitē jānorāda vieta, kur attiecīgā politika ir atrodama. Uzņēmumiem ir arī pienākums savā tīmekļa vietnē skaidri norādīt strīdu alternatīvas izšķiršanas pakalpojumu sniedzēju un ietvert saiti uz „drošības zonas" sertifikāciju Tirdzniecības ministrijas tīmekļa vietnē. Tomēr ir aplēsts, ka vairāk nekā 30 % „drošības zonas" dalībnieku savā tīmekļa vietnē pieejamajā slepenības politikā nenorāda informāciju par strīdu izšķiršanu[28].

Lielākā daļa uzņēmumu, kurus Tirdzniecības ministrija svītrojusi no „drošības zonas" saraksta, tika svītroti pēc attiecīgo uzņēmumu skaidri izteikta pieprasījuma (piemēram, tie ir uzņēmumi, kas apvienojušies vai tikuši pārņemti, mainījuši savu uzņēmējdarbības veidu vai

---

26 Sk. 2004. gada ziņojuma (SEC(2004)1323) 8. lappusi.

27 Saskaņā ar statistikas datiem, ko Tirdzniecības ministrija iesniedza 2013. gada septembrī, tā 2010. gadā informēja 18 % (93) no 512 pirmreizēji sertificējamiem uzņēmumiem un 16 % (231) no 1417 atkārtoti sertificējamiem uzņēmumiem, ka tiem jāievieš uzlabojumi privātuma politikā un/vai „drošības zonas" principu piemērošanā. Tomēr, ņemot vērā Komisijas pieprasījumus veikt visu iesniegumu pamatīgu, rūpīgu un sistemātisku izvērtēšanu, Tirdzniecības ministrija līdz 2013. gada septembrim bija informējusi 56 % (340) no 602 pirmreizēji sertificējamiem uzņēmumiem un 27 % (493) no 1809 atkārtoti sertificējamiem uzņēmumiem, ka tiem jāievieš uzlabojumi savā slepenības politikā.

28 *Chris Connolly* (*Galexia*) uzstāšanās Eiropas Parlamenta *LIBE* komitejas izmeklēšanā 2013. gada 7. oktobrī.

izbeiguši uzņēmējdarbību). Mazāks skaits prasībām neatbilstošu uzņēmumu no saraksta svītrots, kad konstatēts, ka sarakstā norādītās tīmekļa vietnes nedarbojas un ka uzņēmumu sertifikācijas statuss jau vairākus gadus ir bijis "neaktuāls"[29]. Svarīgi ir tas, ka neviens no svītrošanas gadījumiem nav noticis tāpēc, ka Tirdzniecības ministrijas pārbaudē būtu konstatētas atbilstības problēmas.

„Drošības zonas" saraksts ir izmantojams kā publisks paziņojums un kā uzņēmuma „drošības zonas" apņemšanos apkopojums. **Apņemšanās ievērot „drošības zonas" principus nav ierobežota laikā** attiecībā uz datiem, kas saņemti laikposmā, kurā uzņēmums izmanto „drošības zonas" sniegtās priekšrocības, un uzņēmumam jāturpina piemērot principus šādiem datiem, kamēr vien tas šādus datus uzglabā, izmanto vai izpaužu, pat ja tas jebkāda iemesla dēļ izstājas no „drošības zonas".

To „drošības zonas" **pretendentu skaits, kuri nav izturējuši** Tirdzniecības ministrijas veikto **administratīvo izvērtēšanu** un tāpēc nav nekad bijuši iekļauti „drošības zonas" sarakstā, ir šāds: **2010. gadā** tikai **6 %** (33) no 513 pirmreizēji sertificējamiem uzņēmumiem nekad nebija iekļauti „drošības zonas" sarakstā, jo tie neatbilda Tirdzniecības ministrijas noteiktajiem pašsertifikācijas standartiem. **2013. gadā 12 %** (75) no 605 pirmreizēji sertificējamiem uzņēmumiem nekad nebija iekļauti „drošības zonas" sarakstā, jo tie neatbilda Tirdzniecības ministrijas noteiktajiem pašsertifikācijas standartiem.

Lai uzlabotu uzraudzības pārredzamību, Tirdzniecības ministrijai būtu vismaz jāveic šādi pasākumi: savā tīmekļa vietnē jāuzskaita visi uzņēmumi, kas svītroti no „drošības zonas" saraksta, un jānorāda iemesli, kuru dēļ sertifikācija nav atjaunota. Norāde "neaktuāls" Tirdzniecības ministrijas sarakstā ar „drošības zonā" iesaistītajiem uzņēmumiem nav uzskatāma tikai par informatīvu — tā būtu jāpapildina ar **skaidru brīdinājumu** (gan vārdisku, gan grafisku), ka uzņēmums konkrētajā brīdī neatbilst „drošības zonas" prasībām.

Turklāt daži uzņēmumi joprojām nepilnīgi ievēro visus „drošības zonas" principus. Papildus pārredzamības jautājumam, kas aplūkots 3. sadaļā, pašsertificēto uzņēmumu slepenības politikā bieži vien nav skaidri norādīts, kādiem mērķiem dati tiek vākti, un nav skaidrības par tiesībām izvēlēties, vai datus var izpaust trešām personām, tādējādi radot jautājumus par privātuma principu "informēšana" un "izvēle" ievērošanu. Informēšanai un izvēlei ir ļoti svarīga nozīme, lai datu subjektiem nodrošinātu kontroli pār to, kas notiek ar viņu personiska rakstura informāciju.

Pietiekamā apjomā nav nodrošināts pirmais svarīgais atbilstības procesa posms, proti, privātuma „drošības zonas" principu iekļaušana uzņēmumu slepenības politikā. Tirdzniecības ministrijai šis jautājums būtu jārisina prioritārā kārtā, izstrādājot atbilstības metodoloģiju uzņēmumu darbības praksei un to saskarsmei ar klientiem. **Tirdzniecības ministrijai aktīvi jāseko līdzi tam, vai „drošības zonas" principi tiek faktiski iekļauti uzņēmumu slepenības politikā**, nevis piemērošanas nodrošināšanas pasākumi jāīsteno tikai tad, kad saņemtas indivīdu sūdzības.

5. PUBLISKO IESTĀŽU ĪSTENOTĀ PIEMĒROŠANAS NODROŠINĀŠANA

Ir pieejami vairāki mehānismi, lai nodrošinātu „drošības zonas" shēmas efektīvu piemērošanu un paredzētu indivīdu tiesību aizsardzību gadījumos, kad viņu personiskās informācijas aizsardzību ietekmē neatbilstība privātuma principiem.

[29] Kopš 2011. gada decembra ASV Tirdzniecības ministrija no „drošības zonas" saraksta svītrojusi 323 uzņēmumus — 94 uzņēmumi svītroti, jo tie vairs neveica uzņēmējdarbību, 88 uzņēmumi svītroti pārņemšanas vai apvienošanās dēļ, 95 uzņēmumi svītroti pēc mātesuzņēmuma pieprasījuma, 41 uzņēmums svītrots, jo nav pieprasījis atkārtotu sertifikāciju, un 5 uzņēmumi svītroti dažādu citu iemeslu dēļ.

Saskaņā ar "piemērošanas" principu pašsertificēto organizāciju slepenības politikā jābūt iekļautiem efektīviem atbilstības mehānismiem. Atbilstoši privātuma principam "piemērošana", kā sīkāk izskaidrots *FAQ* 11, *FAQ* 5 un *FAQ* 6, šo prasību var izpildīt, pievienojoties **neatkarīgiem tiesību aizsardzības mehānismiem**, kas ir publiski apliecinājuši savu kompetenci izskatīt individuālas sūdzības par principu neievērošanu. Alternatīvi to var nodrošināt, organizācijai apņemoties sadarboties ar **ES Datu aizsardzības komisiju**[30]**.** Turklāt pašsertificētiem uzņēmumiem ir piemērojama Federālās tirdzniecības komisijas jurisdikcija saskaņā ar Federālās tirdzniecības likuma 5. pantu, ar ko aizliedz negodīgu vai maldinošu rīcību vai praksi, kuru veic tirdzniecībā vai kura to ietekmē[31].

Iepriekš minētajā 2004. gada ziņojumā ir paustas bažas par „drošības zonas" shēmas piemērošanas nodrošināšanu, proti, Federālajai tirdzniecības komisijai vajadzētu būt aktīvākai, sākot izmeklēšanu un veicinot indivīdu informētību par viņu tiesībām. Vēl viena problēmjoma ir skaidrības trūkums saistībā ar Federālās tirdzniecības komisijas kompetenci nodrošināt principu piemērošanu attiecībā uz cilvēkresursu datiem.

Tiesību aizsardzības struktūra, kas ir atbildīga par cilvēkresursu datiem, — ES Datu aizsardzības komisija — ir saņēmusi vienu sūdzību par cilvēkresursu datiem[32]. Tomēr sūdzību neesamība neļauj izdarīt secinājumus par shēmas vispārējo darbību. Būtu jāievieš uzņēmumu atbilstības *ex-officio* pārbaudes, lai pārliecinātos par datu aizsardzības saistību faktisko īstenošanu. Arī ES datu aizsardzības iestādēm būtu jāveic darbības, lai uzlabotu informētību par šādas komisijas pastāvēšanu.

Ir uzsvērtas problēmas attiecībā uz to, kādā veidā alternatīvi tiesību aizsardzības mehānismi darbojas kā piemērošanas nodrošināšanas struktūras. Vairākām no šīm struktūrām trūkst atbilstošu līdzekļu, lai rīkotos principu neievērošanas gadījumos. Šis trūkums ir jānovērš.

5.1. Federālā tirdzniecības komisija

Federālā tirdzniecības komisija var veikt piemērošanas nodrošināšanas pasākumus, ja tiek pārkāptas „drošības zonas" saistības, ko uzņēmušies uzņēmumi. Kad tika izveidota „drošības zona", Federālā tirdzniecības komisija apņēmās prioritārā kārtā izskatīt visus pieprasījumus no ES dalībvalstu iestādēm[33]. Tā kā pirmos desmit gadus pēc shēmas izveides sūdzības netika saņemtas, Federālā tirdzniecības komisija nolēma, ka tā centīsies identificēt visus „drošības zonas" pārkāpumus ikvienā privātuma un datu drošības izmeklēšanā, ko tā veic. Kopš 2009. gada Federālā tirdzniecības komisija, pamatojoties uz „drošības zonas" pārkāpumiem, ir cēlusi pret uzņēmumiem 10 prasības par piemērošanu. Pēc šādu prasību izskatīšanas tika pieņemti izlīguma rīkojumi ar būtiskām sankcijām, aizliedzot maldinošus apgalvojumus par privātumu, tostarp saistībā ar „drošības zonas" ievērošanu, un piemērojot uzņēmumiem visaptverošas privātuma programmas un revīzijas 20 gadu laikposmā. Uzņēmumiem ir jāļauj veikts to privātuma programmu neatkarīgus novērtējumus pēc Federālās tirdzniecības komisijas pieprasījuma. Par šādiem novērtējumiem regulāri ziņo Federālajai tirdzniecības komisijai. Federālās tirdzniecības komisijas rīkojumi arī aizliedz šādiem uzņēmumiem izteikt

---

30 ES Datu aizsardzības komisija ir struktūra, kas ir kompetenta izvērtēt un atrisināt indivīdu iesniegtās sūdzības par iespējamiem „drošības zonas" principu pārkāpumiem, kurus pieļāvuši „drošības zonā" iesaistīti uzņēmumi no ASV. Uzņēmumiem, kas apliecina, ka tie ievēro „drošības zonas" principus, jāizvēlas ievērot neatkarīgu tiesību aizsardzības mehānismu vai sadarboties ar ES Datu aizsardzības komisiju, lai atrisinātu problēmas, ko rada „drošības zonas" principu neievērošana. Tomēr sadarbība ar ES Datu aizsardzības komisiju ir obligāta, kad ASV uzņēmums apstrādā cilvēkresursu personas datus, kuri tiek pārsūtīti no ES saistībā ar darba attiecībām. Ja uzņēmums pats apņemas sadarboties ar ES komisiju, tam arī jāapņemas izpildīt visus ieteikumus, ko sniedz ES komisija, ja tā uzskata, ka uzņēmumam ir jāveic īpaši pasākumi, lai ievērotu „drošības zonas" principus, tostarp korektīvi vai kompensējoši pasākumi.

31 Transporta ministrija īsteno līdzīgu jurisdikciju attiecībā uz gaisa pārvadātājiem saskaņā ar Amerikas Savienoto Valstu Kodeksa 41712. sadaļas 49. iedaļu.

32 Sūdzību iesniedza Šveices pilsonis, un tāpēc ES Datu aizsardzības komisija to nosūtīja Šveices datu aizsardzības iestādei (ASV ir atsevišķa „drošības zonas" shēma attiecībā uz Šveici).

33 Sk. Komisijas 2000. gada 26. jūlija Lēmuma 2000/520/EK V pielikumu.

maldinošus apgalvojumus par to privātuma praksi un dalību „drošības zonā" vai līdzīgās privātuma shēmās. Kā piemēru var minēt Federālās tirdzniecības komisijas veikto izmeklēšanu pret *Google*, *Facebook* un *Myspace*[34]. *Google* 2012. gadā piekrita samaksāt naudas sodu USD 22,5 miljonu apmērā, lai nokārtotu konfliktu saistībā ar apgalvojumiem, ka tā nav izpildījusi piekrišanas rīkojumu. Visos privātuma izmeklēšanas gadījumos Federālā tirdzniecības komisija *ex officio* pārbauda, vai ir noticis „drošības zonas" pārkāpums.

Federālā tirdzniecības komisija nesen ir atkārtoti apliecinājusi savus paziņojumus un apņemšanos prioritārā kārtā izskatīt visus pieprasījumus, kuri saņemti no privātumu pašregulējošiem uzņēmumiem un ES dalībvalstīm un kuros norādīts, ka uzņēmums neievēro privātuma principus[35]. Pēdējo trīs gadu laikā Federālā tirdzniecības komisija ir saņēmusi tikai dažus pieprasījumus no Eiropas datu aizsardzības iestādēm.

Transatlantiskā sadarbība starp datu aizsardzības iestādēm sāka attīstīties pēdējo mēnešu laikā. Piemēram, 2013. gada 26. jūnijā Federālā tirdzniecības komisija ar Īrijas Datu aizsardzības komisāra biroju parakstīja saprašanās memorandu par savstarpējo palīdzību to tiesību aktu piemērošanā, kuri aizsargā personisko informāciju privātajā sektorā. Memorands nosaka satvaru intensīvākai, racionalizētākai un efektīvākai sadarbībai privātuma tiesību aktu piemērošanas nodrošināšanā[36].

Federālā tirdzniecības komisija 2013. gada augustā paziņoja, ka turpinās pastiprināt to uzņēmumu pārbaudes, kuru kontrolē ir lielas personiskās informācijas datubāzes. Tā ir arī izveidojusi portālu, kurā patērētāji var iesniegt par ASV uzņēmumiem sūdzības saistībā ar privātuma jautājumiem[37].

Federālajai tirdzniecības komisijai arī vajadzētu intensīvāk izmeklēt nepatiesus apgalvojumus par „drošības zonas" ievērošanu. Uzņēmums, kas savā tīmekļa vietnē norāda, ka tas ievēro „drošības zonas" prasības, bet nav iekļauts Tirdzniecības ministrijas sarakstā kā "aktuāls" shēmas dalībnieks, maldina patērētājus un ļaunprātīgi izmanto viņu uzticību. Nepatiesi apgalvojumi grauj sistēmas uzticamību kopumā, un tāpēc būtu nekavējoties jāizņem no uzņēmumu tīmekļa vietnēm. Uzņēmumiem būtu jāizņemas izpildāms pienākums nemaldināt patērētājus. Federālajai tirdzniecības komisijai būtu jāturpina apzināt maldinošus apgalvojumus par „drošības zonu", piemēram, tādus kā *Karnani* lietā, kurā Federālā tirdzniecības komisija slēdza kādu Kalifornijas tīmekļa vietni, jo tajā bija maldinoši apgalvojumi par reģistrēšanos „drošības zonā" un tā bija iesaistīta krāpnieciskā e-komercijā, kas vērsta pret Eiropas patērētājiem[38].

Federālā tirdzniecības komisija 2013. gada 29. oktobrī paziņoja, ka tā ir sākusi "vairākas izmeklēšanas par „drošības zonas" ievērošanu pēdējo mēnešu laikā" un ka "nākamajos mēnešos" ir vēl gaidāmas vairākas piemērošanas nodrošināšanas darbības šajā jomā. Federālā tirdzniecības komisija arī apstiprināja, ka tā ir "apņēmusies meklēt veidus, kā uzlabot savas darbības efektivitāti" un ka tā "arī turpmāk labprāt saņems būtiskas norādes, tādas kā sūdzība,

---

34 Laikposmā no 2009. gada līdz 2012. gadam Federālā tirdzniecības komisija pabeidza desmit piemērošanas nodrošināšanas prasības par „drošības zonas" saistībām: *FTC* pret *Javian Karnani* un *Balls of Kryptonite, LLC* (2009. gads), *World Innovators, Inc*. (2009 gads), *Expat Edge Partners, LLC* (2009. gads), *Onyx Graphics, Inc.* (2009. gads), *Directors Desk LLC* (2009. gads), *Progressive Gaitways LLC* (2009. gads), *Collectify LLC* (2009. gads), *Google Inc.* (2011. gads), *Facebook*, *Inc.* (2011. gads), *Myspace LLC* (2012. gads). Sk. "*Federal Trade Commission of Safe Harbour Commitments*": http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf. Sk. arī: "*Case Highlights*": http://business.ftc.gov/us-eu-Safe-Harbour-framework. Lielākā daļa šo lietu attiecās uz problēmām ar uzņēmumiem, kas pievienojās „drošības zonai", bet pēc tam turpināja uzdoties par dalībniekiem, neatjaunojot ikgadējo sertifikāciju.

35 Šī apņemšanās tika atkārtoti izteikta sanāksmē 2013. gada 17. aprīlī Briselē, kuras laikā Federālās tirdzniecības komisijas komisāre *Julie Brill* tikās ar ES datu aizsardzības iestādēm (29. panta darba grupu).

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n

37 Patērētāji var iesniegt sūdzības, izmantojot Federālās tirdzniecības komisijas "Sūdzību asistentu" (https://www.ftccomplaintassistant.gov/), un starptautiskie patērētāji var iesniegt sūdzības, izmantojot vietni (http://www.econsumer.gov).

38 http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf

kas saņemta iepriekšējā mēnesī no Eiropā mītoša patērētāju advokāta, kurš norādīja uz lielu skaitu ar „drošības zonu" saistītu pārkāpumu"[39]. Aģentūra arī apņēmās "sistemātiski uzraudzīt „drošības zonas" rīkojumu izpildi, kā tas tiek darīts attiecībā uz visiem mūsu rīkojumiem"[40].

Federālā tirdzniecības komisija 2013. gada 12. novembrī informēja Eiropa Komisiju, ka, "**ja uzņēmuma slepenības politikā ir dots solījums nodrošināt aizsardzību saskaņā ar „drošības zonu", tad fakts, ka uzņēmums nav veicis vai atjaunojis reģistrāciju, pats par sevi nevar būt iemesls, lai pret attiecīgo uzņēmumu nevērstu *FTC* pasākumus minēto „drošības zonas" saistību izpildes panākšanai"**[41].

Tirdzniecības ministrija 2013. gada novembrī informēja Eiropas Komisiju, ka, "lai palīdzētu nodrošināt, ka uzņēmumi nesniedz "nepatiesus apgalvojumus" par dalību „drošības zonā", Tirdzniecības ministrija sāks sazināties ar „drošības zonas" dalībniekiem mēnesi pirms to atkārtotās sertifikācijas datuma, lai informētu, kādi pasākumi tiem jāveic gadījumā, ja tie izvēlētos neveikt atkārtotu sertifikāciju". **Tirdzniecības ministrija "brīdinās šīs kategorijas uzņēmumus**, ka tiem no savas slepenības politikas jāsvītro un no savas tīmekļa vietnes jāizņem visas atsauces uz dalību „drošības zonā", kā arī ministrijas „drošības zonas" sertifikācijas zīme, **un tos skaidri informēs, ka pretējā gadījumā pret tiem var tikt vērstas *FTC* darbības piemērošanas nodrošināšanai**"[42].

Lai vērstos pret nepatiesiem apgalvojumiem par „drošības zonas" ievērošanu, pašsertificētu uzņēmumu tīmekļa vietnēs publicētajā slepenības politikā vienmēr vajadzētu būt iekļautai saitei uz Tirdzniecības ministrijas „drošības zonas" tīmekļa vietni, kur uzskaitīti visi shēmas "aktuālie" dalībnieki. Tas ļaus Eiropas datu subjektiem nekavējoties, bez papildu meklēšanas pārliecināties, vai uzņēmums konkrētajā brīdī ir „drošības zonas" dalībnieks. Tirdzniecības ministrija 2013. gada martā sāka to pieprasīt no uzņēmumiem, bet šis process būtu jāveic intensīvāk.

Federālās tirdzniecības komisijas veikta „drošības zonas" principu faktiskās ievērošanas nepārtraukta uzraudzība un konsekventa piemērošanas nodrošināšana – papildus jau minētajiem Tirdzniecības ministrijas veiktajiem pasākumiem –, joprojām ir galvenā prioritāte shēmas pienācīgas un efektīvas darbības nodrošināšanā. Proti, ir jāpastiprina ***ex-officio* pārbaudes un izmeklēšanas attiecībā uz to, kā uzņēmumi ievēro „**drošības zonas" principus. Būtu jāturpina atvieglot sūdzību par pārkāpumiem iesniegšanu Federālajai tirdzniecības komisijai.

5.2. ES Datu aizsardzības komisija

ES Datu aizsardzības komisija ir struktūra, kas izveidota saskaņā ar Lēmumu par „drošības zonu". Tā ir kompetenta izskatīt sūdzības, kuras iesniedz privātpersonas attiecībā uz personas datiem, kas savākti saistībā ar darba attiecībām, kā arī lietas, kas saistītas ar sertificētiem uzņēmumiem, kuri izvēlējušies šo iespēju strīdu izšķiršanai saskaņā ar „drošības zonu" (53 % no visiem uzņēmumiem). Tajā darbojas pārstāvji no dažādām ES datu aizsardzības iestādēm.

Līdz šim komisija ir saņēmusi četras sūdzības (divas 2010. gadā un divas 2013. gadā). Divas sūdzības tā 2010. gadā nosūtīja valstu datu aizsardzības iestādēm (Apvienotajā Karalistē un Šveicē). Trešā un ceturtā sūdzība pašlaik tiek izskatītas. Mazo sūdzību skaitu var izskaidrot ar faktu, ka komisijas pilnvaras, kā norādīts iepriekš, galvenokārt attiecas tikai uz konkrēta veida datiem.

---

39 http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf un http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf

40 Federālās tirdzniecības komisijas priekšsēdētājas *Edith Ramirez* vēstule EK priekšsēdētāja vietniecei *Viviane Reding*.

41 Federālās tirdzniecības komisijas priekšsēdētājas *Edith Ramirez* vēstule EK priekšsēdētāja vietniecei *Viviane Reding*.

42 "*U.S.-EU Cooperation to Implement the Safe Harbor Framework*", 2013. gada 12. novembris.

Komisijā izskatāmo lietu nelielo skaitu daļēji var arī izskaidrot ar to, ka nav pietiekamas informētības par šādas komisijas esamību. Kopš 2004. gada Komisija uzskatāmāk informē par neformālo komisiju savā tīmekļa vietnē[43].

Lai komisiju izmantotu efektīvāk, uzņēmumiem ASV, kuri izvēlējušies sadarboties ar to un izpilda tās lēmumus, attiecībā uz visām vai dažām personas datu kategorijām, uz kurām attiecas to pašsertifikācija, skaidri un saprotami būtu jānorāda savā slepenības politikā apņemšanās ļaut Tirdzniecības ministrijai rūpīgi pārbaudīt šo aspektu. Lai uzlabotu Eiropas uzņēmumu un datu subjektu informētību par „drošības zonu", katras ES datu aizsardzības iestādes tīmekļa vietnē būtu jāizveido īpaša „drošības zonas" lapa.

5.3. Piemērošanas nodrošināšanas uzlabošana

Pārredzamības un piemērošanas nepilnības, kas norādītas iepriekš, ir radījušas Eiropas uzņēmumiem bažas par „drošības zonas" shēmas negatīvo ietekmi uz Eiropas uzņēmumu konkurētspēju. Ja Eiropas uzņēmums konkurē ar ASV uzņēmumu, kas darbojas „drošības zonas" ietvaros, bet praksē nepiemēro tās principus, Eiropas uzņēmumam tiek radīti neizdevīgi konkurences apstākļi salīdzinājumā ar šo ASV uzņēmumu.

Turklāt Federālās tirdzniecības komisijas jurisdikcija ietver arī negodīgu vai maldinošu rīcību vai praksi, "kuru veic tirdzniecībā vai kura to ietekmē". Federālās tirdzniecības komisijas likuma 5. pantā ir noteikti izņēmumi attiecībā uz Federālās tirdzniecības komisijas pilnvarām saistībā ar negodīgu vai maldinošu rīcību vai praksi, cita starpā **telesakaru** jomā. Tā kā uz telesakaru uzņēmumiem Federālās tirdzniecības komisijas veiktās piemērošanas nodrošināšanas darbības neattiecas, tiem nav atļauts iesaistīties „drošības zonā". Tomēr, palielinoties tehnoloģiju un pakalpojumu konverģencei, daudzi no to tiešajiem konkurentiem ASV IKT nozarē ir „drošības zonas" dalībnieki. Telesakaru uzņēmumu neiekļaušana datu apmaiņā saskaņā ar „drošības zonas" shēmu rada bažas dažiem Eiropas telesakaru operatoriem. Kā norādījusi Eiropas Telesakaru tīklu operatoru asociācija (*ETNO*), "tas ir acīmredzamā pretrunā telesakaru operatoru vissvarīgākajam argumentam par nepieciešamību nodrošināt vienlīdzīgus konkurences apstākļus"[44].

6. „DROŠĪBAS ZONAS" PRIVĀTUMA PRINCIPU NOSTIPRINĀŠANA

6.1. Strīdu alternatīva izšķiršana

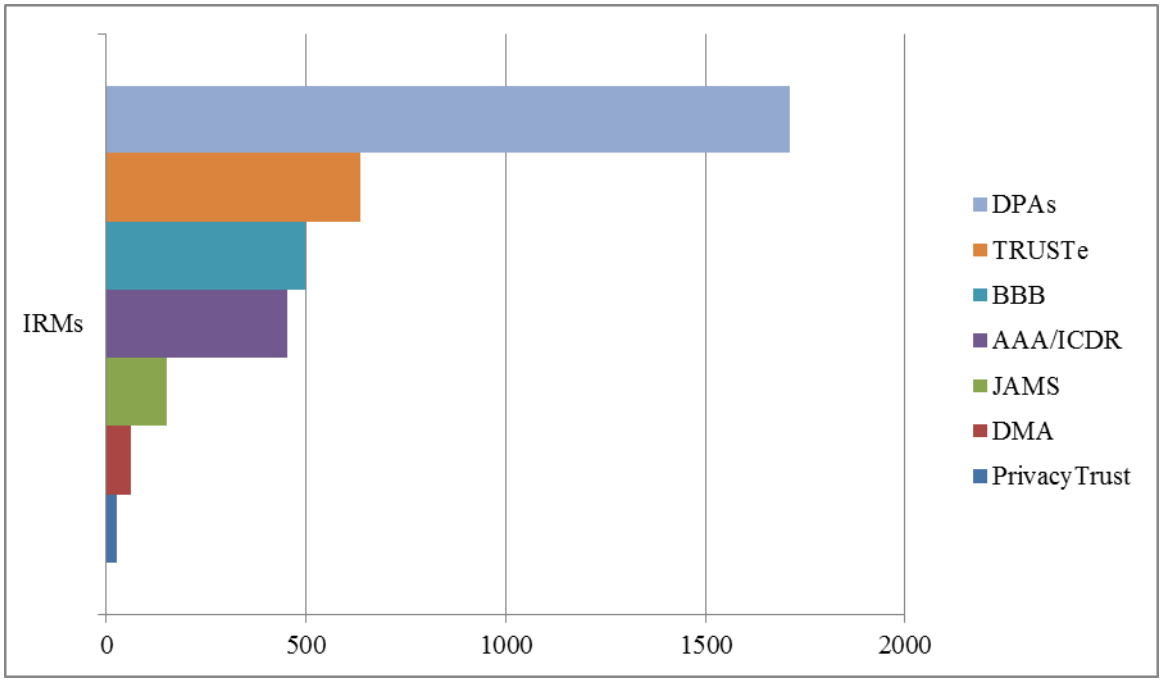
Piemērošanas nodrošināšanas princips nosaka, ka jābūt "**gataviem un pieejamiem tiesību aizsardzības mehānismiem**, saskaņā ar kuriem izmeklē katras personas sūdzības un domstarpības". Šajā nolūkā „drošības zonas" shēma nosaka strīdu alternatīvas izšķiršanas (SAI) sistēmu, ko īsteno neatkarīga trešā persona[45], lai nodrošinātu personām ātrus risinājumus. Trīs galvenās tiesību aizsardzības struktūras ir ES Datu aizsardzības komisija, *BBB* (*Better Business Bureaus*) un *TRUSTe*.

---

43 Atbilstoši 2004. gada ziņojumam Komisijas tīmekļa vietnē (Tiesiskuma ĢD) ir publicēts informatīvs paziņojums ES Datu aizsardzības komisijas "jautājumu un atbilžu" veidā, lai uzlabotu privātpersonu informētību un palīdzētu viņiem iesniegt sūdzību, ja viņi uzskata, ka viņu personas datu apstrāde veikta, pārkāpjot „drošības zonu": http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf
Standarta sūdzības veidlapa pieejama vietnē http://ec.europa.eu/justice/policies/privacy/docs/adequacy/ complaint_form_en.pdf.

44 "*ETNO* apsvērumos", ko Komisijas dienesti saņēma 2013. gada 4. oktobrī, ir arī aplūkota 1) „drošības zonā" ietverto personas datu definīcija, 2) nepietiekamā „drošības zonas" uzraudzība, 3) fakts, ka "ASV uzņēmumi var pārsūtīt datus ar daudz mazāk ierobežojumiem nekā to Eiropas partneri", kas ir uzskatāms par "Eiropas uzņēmumu acīmredzamu diskrimināciju un ietekmē Eiropas uzņēmumu konkurētspēju". Saskaņā ar „drošības zonas" noteikumiem, izpaužot informāciju trešai personai, organizācijām jāpiemēro informēšanas un izvēles principi. Ja organizācija vēlas informāciju nosūtīt trešai personai, kas darbojas kā pārstāvis, 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 ar šādu trešo personu noslēdz rakstisku līgumu, kurā prasīts, lai trešā persona nodrošina vismaz tādu pašu privātās dzīves aizsardzības līmeni, kādu prasa attiecīgie principi.

45 ES Direktīvā 2013/11/ES par patērētāju strīdu alternatīvu izšķiršanu (SAI) ir uzsvērts neatkarīgu, objektīvu, pārredzamu, efektīvu, ātru un taisnīgu strīdu alternatīvas izšķiršanas procedūru nozīmīgums.



Kopš 2004. gada SAI izmantota aizvien biežāk, un Tirdzniecības ministrija ir pastiprinājusi Amerikas SAI nodrošinātāju uzraudzību, lai pārliecinātos, ka to piedāvātā informācija par sūdzību procedūru ir skaidra, pieejama un saprotama. Tomēr, ņemot vērā līdz šim izskatīto lietu mazo skaitu, šīs sistēmas efektivitāte vēl ir jāpierāda[46].

Lai gan Tirdzniecības ministrija ir veiksmīgi samazinājusi maksu, ko iekasē SAI nodrošinātāji, divi no septiņiem lielākajiem SAI nodrošinātājiem joprojām iekasē maksu no personām, kuras iesniedz sūdzības[47]. Tie ir SAI nodrošinātāji, kurus izmanto aptuveni 20 % „drošības zonas" uzņēmumu. Šie uzņēmumi ir izvēlējušies SAI nodrošinātāju, kas iekasē no patērētājiem maksu par sūdzības iesniegšanu. Šāda prakse neatbilst „drošības zonas" piemērošanas nodrošināšanas principam, kas piešķir personai tiesības piekļūt "gataviem un pieejamiem tiesību aizsardzības mehānismiem". Eiropas Savienībā piekļuve neatkarīgiem strīdu izšķiršanas pakalpojumiem, ko nodrošina ES Datu aizsardzības komisija, visiem datu subjektiem ir bez maksas.

Tirdzniecības ministrija 2013. gada 12. novembrī apstiprināja, ka tā "turpinās ES uzdevumā atbalstīt pilsoņu privātumu un darbu ar SAI nodrošinātājiem, lai noteiktu, vai to maksu var vēl vairāk samazināt".

Attiecībā uz sankcijām ne visu SAI nodrošinātāju rīcībā ir vajadzīgie līdzekļi, lai novērstu situācijas, kurās netiek ievēroti privātuma principi. Turklāt šķiet, ka ne visi SAI pakalpojumu nodrošinātāji ir iekļāvuši savā sankciju un pasākumu klāstā konstatēto neatbilstību publicēšanu.

---

46 Piemēram, viens no lielajiem pakalpojumu sniedzējiem (*TRUSTe*) ziņoja, ka 2010. gadā tas ir saņēmis 881 pieprasījumu, bet tikai trīs no tiem tika atzīti par pieņemamiem un pamatotiem, kā rezultātā attiecīgajam uzņēmumam tika prasīts ieviest izmaiņas tā slepenības politikā un tīmekļa vietnē. Savukārt 2011. gadā sūdzību skaits bija 879, un vienā gadījumā uzņēmumam tika prasīts mainīt tā slepenības politiku. Saskaņā ar Tirdzniecības ministrijas norādīto lielākā daļa sūdzību, kas iesniegtas SAI, bija patērētāju pieprasījumi, piemēram, no lietotājiem, kuri aizmirsuši savu paroli un nevarēja to saņemt no interneta pakalpojumu sniedzēja. Pēc Komisijas lūgumiem Tirdzniecības ministrija izstrādāja jaunus statistiskas datu paziņošanas kritērijus, kas izmantojami visās SAI procedūrās. Kritērijos ir nošķirti pieprasījumi un sūdzības, un tajos ir sniegts saņemto sūdzību veidu sīkāks skaidrojums. Tomēr vēl ir jāturpina šo jauno kritēriju apspriešana, lai nodrošinātu, ka 2014. gadā jaunie statistikas dati attiecas uz visiem SAI nodrošinātājiem, ir salīdzināmi un sniedz kritisku informāciju tiesību aizsardzības mehānisma efektivitātes novērtēšanai.

47 Starptautiskais Strīdu izšķiršanas centrs / Amerikas Šķīrējtiesu asociācija (*ICDR/AAA*) iekasē USD 200 un *JAMS* iekasē USD 250 lielu "iesniegšanas maksu". Tirdzniecības ministrija informēja Komisiju, ka tā ir sadarbojusies ar *AAA* — strīdu izšķiršanas nodrošinātāju, kas personām izmaksā visdārgāk —, lai izstrādātu piemērotu „drošības zonas" programmu, ar kuras starpniecību izmaksas patērētājiem tika samazinātas no vairākiem tūkstošiem dolāru līdz nemainīgai USD 200 likmei.

SAI nodrošinātājiem ir arī jānodod lietas Federālajai tirdzniecības komisijai, ja uzņēmums neievēro SAI procesa rezultātu vai noraida SAI nodrošinātāja lēmumu, lai Federālā tirdzniecības komisija varētu izskatīt un izmeklēt lietu un attiecīgā gadījumā veikt piemērošanas pasākumus. Tomēr līdz šim SAI nodrošinātāji nav nodevuši Federālajai tirdzniecības komisijai nevienu lietu, kas saistīta ar neatbilstību[48].

Strīdu alternatīvas izšķiršanas pakalpojumu sniedzēji savās tīmekļa vietnēs uztur to uzņēmumu sarakstus (strīdu izšķiršanas dalībniekus), kuri izmanto to pakalpojumus. Tas ļauj patērētājiem viegli pārbaudīt, vai gadījumā, ja radies strīds ar uzņēmumu, persona var iesniegt sūdzību neatkarīgam strīdu izšķiršanas nodrošinātājam. Tādējādi, piemēram, *BBB* strīdu izšķiršanas nodrošinātājs iekļauj sarakstā visus uzņēmumus, kas ietverti *BBB* strīdu izšķiršanas shēmā. Tomēr ir vairāki uzņēmumi, kas apgalvo, ka ir ietverti īpašā strīdu izšķiršanas shēmā, bet ko SAI pakalpojumu nodrošinātāji nav iekļāvuši sarakstos kā savas strīdu izšķiršanas shēmas dalībniekus[49].

SAI mehānismiem jābūt neatkarīgiem, personām viegli pieejamiem un izmaksu ziņā izdevīgiem. Datu subjektam jābūt iespējai iesniegt sūdzību bez pārmērīgiem ierobežojumiem. Visām SAI struktūrām to tīmekļa vietnēs ir jāpublicē statistikas dati par apstrādātajām sūdzībām un konkrēta informācija par to rezultātiem. Visbeidzot, būtu jāturpina SAI struktūru uzraudzība, lai nodrošinātu, ka to sniegtā informācija par procedūru un par to, kā iesniegt sūdzību, ir skaidra un saprotama, un lai strīdu izšķiršana kļūtu par efektīvu, uzticamu mehānismu, kas sniedz rezultātus. Būtu arī jāatgādina, ka konstatēto neatbilstību publicēšana būtu jāiekļauj kā viena no SAI obligātajām sankcijām.

6.2. Tālāka pārsūtīšana

Eksponenciāli palielinoties datu plūsmām, ir jānodrošina personas datu nepārtraukta aizsardzība visos datu apstrādes posmos, jo īpaši tad, kad uzņēmums, kurš iesaistījies „drošības zonā", datus pārsūta **apstrādātājam — trešai personai**. Tāpēc nepieciešamība uzlabot „drošības zonas" piemērošanas nodrošināšanu attiecas ne tikai uz „drošības zonas" dalībniekiem, bet arī uz apakšuzņēmējiem.

„Drošības zonas" shēma ļauj datus pārsūtīt tālāk trešām personām, kas darbojas kā "pārstāvji", ja uzņēmums — „drošības zonas" dalībnieks — "apliecina, ka trešā persona atbalsta principus vai ka uz to attiecas direktīva vai cits atzinums par atbilstību, vai ja tas noslēdz rakstisku līgumu ar šādu trešo personu, kurā prasīts, lai trešā persona nodrošina vismaz tādu pašu privātās dzīves aizsardzības līmeni, kādu prasa privātuma principi"[50]. Piemēram, Tirdzniecības ministrija pieprasa, lai mākoņpakalpojumu sniedzējs noslēgtu līgumu, pat ja tas ir „drošības zonas" dalībnieks un saņem personas datus apstrādei[51]. Tomēr Lēmuma par „drošības zonu" II pielikumā šis noteikums nav skaidrs.

---

48 Sk. *FAQ* 11.

49 Piemēram, *Amazon* ir informējis Tirdzniecības ministriju, ka tas izmanto *BBB* kā savu strīdu izšķiršanas nodrošinātāju. Tomēr *BBB* sarakstā nav iekļāvis *Amazon* kā vienu no saviem strīdu izšķiršanas dalībniekiem. Un otrādi — mākoņmitināšanas pakalpojumu sniedzējs *Arsalon Technologies* (www.arsalon.net) ir iekļauts *BBB* drošības zonas strīdu izšķiršanas sarakstā, bet uzņēmums nav aktuālais „drošības zonas" dalībnieks (situācija 2013. gada 1. oktobrī). *BBB*, *TRUSTe* un citiem SAI pakalpojumu sniedzējiem vajadzētu svītrot vai koriģēt savus apgalvojumus par sertifikāciju. Būtu jānosaka tiem saistoša prasība sertificēt tikai tos uzņēmumus, kas ir „drošības zonas" dalībnieki.

50 Sk. Komisijas Lēmuma 2000/520/EK 7. lappusi ("Tālāka pārsūtīšana").

51 Sk. "*Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing*": http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf

Tā kā pēdējo gadu laikā ir palielinājusies apakšuzņēmēju izmantošana, jo īpaši saistībā ar mākoņdatošanu, noslēdzot šādu līgumu, „drošības zonas" uzņēmumam jāinformē Tirdzniecības ministrija un tam ir pienākums publiskot privātuma aizsardzības pasākumus[52].

Trīs iepriekš minētie jautājumi — strīdu alternatīvas izšķiršanas mehānisms, pastiprināta uzraudzība un datu tālāka pārsūtīšana — būtu jāprecizē sīkāk.

7. PIEKĻUVE DATIEM, KO PĀRSŪTA SAISTĪBĀ AR „DROŠĪBAS ZONAS" SHĒMU

2013. gadā informācija par ASV novērošanas programmu apjomu un tvērumu ir radījusi bažas par to personas datu nepārtrauktu aizsardzību, kurus likumīgi pārsūta uz ASV saskaņā ar „drošības zonas" shēmu. Piemēram, visi uzņēmumi, kas iesaistīti *PRISM* programmā un kas piešķir ASV iestādēm piekļuvi ASV uzglabātiem un apstrādātiem datiem, ir sertificēti „drošības zonas" dalībnieki. Tādējādi „drošības zonas" shēma ir kļuvusi par vienu no kanāliem, pa kuriem ASV izlūkdienesti iegūst piekļuvi to personas datu vākšanai, kas sākotnēji ir apstrādāti ES.

Lēmuma par „drošības zonu" I pielikumā ir noteikts, ka principu ievērošanu var ierobežot, ciktāl tas ir vajadzīgs, lai ievērotu valsts drošību, sabiedrības intereses vai piemērošanas prasības, vai ar likumu, valdības noteikumiem vai tiesu praksi. Lai pamattiesību izmantošanas ierobežojumi būtu spēkā, tie ir jāinterpretē sašaurināti, tiem jābūt paredzētiem publiski pieejamos tiesību aktos, un tiem jābūt vajadzīgiem un samērīgiem demokrātiskā sabiedrībā. Lēmumā par „drošības zonu" ir īpaši noteikts, ka šādi ierobežojumi ir pieļaujami tikai **"ciktāl tas ir vajadzīgs"**, lai ievērotu valsts drošību, sabiedrības intereses vai tiesībaizsardzības prasības[53]. Lai gan datu apstrāde izņēmuma kārtā valsts drošības, sabiedrības interešu vai tiesībaizsardzības prasību mērķiem ir paredzēta „drošības zonas" shēmā, tās pieņemšanas brīdī nebija paredzama izlūkdienestu plaša mēroga piekļuve datiem, ko pārsūta uz ASV saistībā ar komerciāliem darījumiem.

Turklāt pārredzamības un juridiskās noteiktības labad Tirdzniecības ministrijai vajadzētu informēt Eiropas Komisiju par visiem likumiem vai valdības noteikumiem, kas varētu ietekmēt „drošības zonas" privātuma principu ievērošanu[54]. Izņēmumu izmantošana būtu rūpīgi jāuzrauga, un izņēmumus nedrīkst izmantot tādā veidā, ka tiek grauta **principu** nodrošinātā aizsardzība[55]. Proti, ASV iestāžu plaša mēroga piekļuve datiem, ko apstrādā pašsertificēti „drošības zonas" uzņēmumi, var apdraudēt elektronisko sakaru konfidencialitāti.

---

52 Šīs piezīmes attiecas uz mākoņpakalpojumu sniedzējiem, kas nav iesaistījušies „drošības zonā". Kā norādījis *Galexia* konsultāciju uzņēmums, "iesaistīšanās „drošības zonā" (un atbilstība tai) mākoņpakalpojumu sniedzēju vidū ir diezgan aktīva. Mākoņpakalpojumu sniedzējiem parasti ir vairāki privātuma aizsardzības līmeņi, kas bieži apvieno tiešu saziņu ar klientiem un visaptverošu slepenības politiku. Ar vienu vai diviem svarīgiem izņēmumiem mākoņpakalpojumu sniedzēji „drošības zonā" ievēro pamatnoteikumus, kas attiecas uz strīdu izšķiršanu un izpildi. Šobrīd to pakalpojumu sniedzēju sarakstā, kuri nepatiesi apgalvojuši, ka viņi ir shēmas dalībnieki, nav lielu mākoņpakalpojumu sniedzēju." (*Galexia* pārstāvja *Chris Connolly* runa *LIBE* komitejas izvaicāšanā par "ES pilsoņu elektronisko masveida uzraudzību").

53 Sk. Lēmuma par „drošības zonu" I pielikumu: "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 šādus izņēmumus vai atkāpes 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."

54 Atzinums 4/2000 par aizsardzības līmeni, ko nodrošina privātuma „drošības zonas" principi, kuru pieņēmusi 29. panta datu aizsardzības darba grupa 2000. gada 16. maijā.

55 Atzinums 4/2000 par aizsardzības līmeni, ko nodrošina privātuma „drošības zonas" principi, kuru pieņēmusi 29. panta datu aizsardzības darba grupa 2000. gada 16. maijā.

7.1. Samērīgums un nepieciešamība

Kā izriet no ES un ASV *ad-hoc* darba grupas konstatējumiem par datu aizsardzību, ASV tiesību akti rada vairākus juridiskos pamatus, ļaujot veikt tādu personas datu plaša mēroga vākšanu un apstrādi, kurus uzglabā vai citādi apstrādā uzņēmumi, kas atrodas ASV. Tas var attiekties uz datiem, kas iepriekš pārsūtīti no ES uz ASV saskaņā ar „drošības zonas" shēmu, un tas rada jautājumu par „drošības zonas" principu nepārtrauktu ievērošanu. Šo programmu plašais mērogs var radīt situāciju, ka saskaņā ar „drošības zonu" pārsūtītiem datiem piekļūst un to turpmāku apstrādi veic ASV iestādes, pārsniedzot to, kas ir samērīgs un nepieciešams tikai valsts drošības aizsardzībai, kā to paredz Lēmumā par „drošības zonu" noteiktais izņēmums.

7.2. Ierobežojumi un tiesiskās aizsardzības iespējas

Kā izriet no ES un ASV *ad-hoc* darba grupas konstatējumiem par datu aizsardzību, aizsardzības pasākumi, kas noteikti ASV tiesību aktos, ir pieejami pārsvarā ASV pilsoņiem vai personām, kuras likumīgi uzturas valstī. Turklāt ne ES, ne ASV datu subjektiem nav iespēju iegūt piekļuvi datiem vai panākt to labošanu vai dzēšanu, vai izmantot administratīvus vai juridiskus tiesiskās aizsardzības līdzekļus attiecībā uz viņu personas datu vākšanu un turpmāku apstrādi, kas notiek saskaņā ar ASV novērošanas programmām.

7.3. Pārredzamība

Uzņēmumi savā slepenības politikā sistemātiski nenorāda, kad tie piemēro izņēmumus attiecībā uz principiem. Līdz ar to privātpersonas un uzņēmumi nav informēti par to, kas tiek darīts ar viņu datiem. Tas jo īpaši attiecas uz konkrēto ASV novērošanas programmu darbību. Rezultātā eiropiešus, kuru dati tiek pārsūtīti uzņēmumam ASV saskaņā ar „drošības zonu", šie uzņēmumi var neinformēt par to, ka viņu datiem var piekļūt[56]. Tas rada jautājumu par „drošības zonas" pārredzamības principu ievērošanu. Būtu jānodrošina maksimālā iespējamā pārredzamība, bet neapdraudot valsts drošību. Papildus esošajām prasībām uzņēmumiem norādīt to slepenības politikā, kad principi var tikt ierobežoti ar likumu, valdības noteikumiem vai tiesu praksi, uzņēmumi būtu arī jāaicina norādīt slepenības politikā, kad tie piemēro izņēmumus attiecībā uz principiem, lai ievērotu valsts drošību, sabiedrības intereses vai tiesībaizsardzības prasības.

8. SECINĀJUMI UN IETEIKUMI

Kopš „drošības zonas" pieņemšanas 2000. gadā tā ir kļuvusi par instrumentu personas datu plūsmām starp ES un ASV. Eksponenciāli palielinoties datu plūsmām, kam ir svarīga nozīme digitālajā ekonomikā, un ievērojami attīstoties datu vākšanai, apstrādāšanai un izmantošanai, ir palielinājies arī personas datu efektīvas aizsardzības nozīmīgums šādu datu pārsūtīšanas gadījumos. Tīmekļa uzņēmumiem (piemēram, *Google*, *Facebook*, *Microsoft*, *Apple*, *Yahoo)* ir simtiem miljonu klientu Eiropā un tie pārsūta uz ASV apstrādei personas datus tādā apjomā, kādu nevarēja iedomāties 2000. gadā, kad tika izveidota „drošības zona".

Ņemot vērā šīs shēmas pārredzamības un piemērošanas nodrošināšanas trūkumus, joprojām pastāv konkrētas problēmas, kas būtu jāatrisina:

[56] Salīdzinoši pārredzamu informāciju šajā ziņā sniedz daži „drošības zonā" ietverti Eiropas uzņēmumi. Piemēram, *Nokia*, kas darbojas ASV un ir „drošības zonas" dalībnieks, savā slepenības politikā ir paziņojis šādi: "Mums var būt pienākums saskaņā ar obligāta likuma prasībām izpaust jūsu personas datus konkrētām iestādēm vai citām trešām personām, piemēram, tiesībaizsardzības aģentūrām valstīs, kurās darbojamies mēs vai trešās personas mūsu vārdā."

(a) drošības zonas" dalībnieku slepenības politikas pārredzamība,

(b) privātuma principu efektīva piemērošana ASV uzņēmumos un

(c) piemērošanas nodrošināšanas efektivitāte.

Turklāt **izlūkdienestu plaša mēroga piekļuve datiem, ko sertificēti „drošības zonas" uzņēmumi pārsūta uz ASV**, liek uzdot nopietnus papildu jautājumus par eiropiešu datu aizsardzības tiesību nepārtrauktību, kad viņu dati tiek pārsūtīti uz ASV.

Pamatojoties uz iepriekš minēto, Komisija ir sagatavojusi turpmāk izklāstītos **ieteikumus**.

Pārredzamība

1. *Pašsertificētiem uzņēmumiem būtu jāpublisko sava slepenības politika.* Nepietiek ar to, ka uzņēmumi iesniedz Tirdzniecības ministrijai savas slepenības politikas aprakstu. Slepenības politikai vajadzētu būt publiski pieejamai uzņēmumu tīmekļa vietnēs un izklāstītai skaidrā un saprotamā valodā.

2. Pašsertificētu uzņēmumu tīmekļa vietnēs publicētajā slepenības politikā vienmēr vajadzētu būt iekļautai saitei uz Tirdzniecības ministrijas „drošības zonas" tīmekļa vietni, kur uzskaitīti visi shēmas "aktuālie" dalībnieki. Tas ļaus Eiropas datu subjektiem nekavējoties, bez papildu meklēšanas pārliecināties, vai uzņēmums konkrētajā brīdī ir „drošības zonas" dalībnieks. Tas arī palīdzēs palielināt shēmas uzticamību, mazinot iespējas sniegt nepatiesus apgalvojumus par dalību „drošības zonā". Tirdzniecības ministrija 2013. gada martā sāka to pieprasīt no uzņēmumiem, bet šis process būtu jāveic intensīvāk.

3. Pašsertificētiem uzņēmumiem būtu jāpublicē privātuma nosacījumi, kas ietverti visos to noslēgtajos līgumos ar apakšuzņēmējiem, piemēram, par mākoņdatošanas pakalpojumiem. „Drošības zona" ļauj pašsertificētiem „drošības zonas" uzņēmumiem pārsūtīt datus tālāk trešām personām, kas darbojas kā „pārstāvji", piemēram, mākoņpakalpojumu sniedzējiem. Pēc mūsu izpratnes, šādos gadījumos Tirdzniecības ministrija pieprasa pašsertificētiem uzņēmumiem noslēgt līgumu. Tomēr, noslēdzot šādu līgumu, „drošības zonas" uzņēmumam arī vajadzētu informēt Tirdzniecības ministriju un obligāti publiskot savus privātuma aizsardzības pasākumus.

4. *Tirdzniecības ministrijas tīmekļa vietnē būtu skaidri jānorāda visi uzņēmumi, kas nav "aktuālie" shēmas dalībnieki.* Norāde "neaktuāls" Tirdzniecības ministrijas „drošības zonas" dalībnieku sarakstā būtu jāpapildina ar skaidru brīdinājumu, ka uzņēmums konkrētajā brīdī neatbilst „drošības zonas" prasībām. Tomēr, ja uzņēmuma statuss ir "neaktuāls", uzņēmumam ir pienākums turpināt „drošības zonas" prasību piemērošanu attiecībā uz datiem, kas saņemti saskaņā ar „drošības zonu".

Tiesiskās aizsardzības līdzekļi

5. Uzņēmumu tīmekļa vietnē publicētajā slepenības politikā būtu jāiekļauj saite uz strīdu alternatīvas izšķiršanas (SAI) nodrošinātāju un/vai ES Datu aizsardzības komisiju. Tas ļaus Eiropas datu subjektiem nekavējoties sazināties ar SAI vai ES Datu aizsardzības komisiju problēmu gadījumā. Tirdzniecības ministrija 2013. gada martā sāka to pieprasīt no uzņēmumiem, bet šis process būtu jāveic intensīvāk.

6. SAI jābūt pieejamai un cenas ziņā izdevīgai. Dažas SAI struktūras „drošības zonas" shēmā turpina iekasēt maksu no personām — kas var būt salīdzinoši liela konkrētai privātpersonai par sūdzības apstrādi (USD 200–250). Turpretī Eiropā piekļuve Datu

aizsardzības komisijai, kas paredzēta sūdzību izskatīšanai „drošības zonas” ietvaros, ir bez maksas.

7. Tirdzniecības ministrijai būtu sistemātiskāk jāuzrauga SAI nodrošinātāji attiecībā uz to, cik pārredzama un pieejama ir to sniegtā informācija par procedūru, ko tie izmanto, un to turpmāko rīcību pēc sūdzību saņemšanas. Tādējādi strīdu izšķiršana kļūst par efektīvu un uzticamu mehānismu, kas sniedz rezultātus. Būtu arī jāatgādina, ka konstatēto neatbilstību publicēšana būtu jāiekļauj kā viena no SAI obligātajām sankcijām.

Piemērošana

8. Pēc uzņēmumu sertifikācijas vai atkārtotas sertifikācijas „drošības zonā” noteiktai procentuālai daļai šo uzņēmumu būtu jāpiemēro ex officio pārbaudes par to, vai tie faktiski ievēro savu slepenības politiku (pārbaudot ne tikai atbilstību oficiālajām prasībām).

9. Ikreiz, kad pēc sūdzības saņemšanas vai pēc izmeklēšanas veikšanas tiek konstatēta neatbilstība, uzņēmumā būtu jāveic īpaša atkārtota izmeklēšana pēc viena gada.

10. Ja ir šaubas par uzņēmuma atbilstību vai tiek izskatītas sūdzības, Tirdzniecības ministrijai būtu jāinformē kompetentā ES datu aizsardzības iestāde.

11. Būtu jāturpina izmeklēt nepatiesi apgalvojumi par dalību „drošības zonā”. Uzņēmums, kas savā tīmekļa vietnē norāda, ka tas ievēro „drošības zonas” prasības, bet nav iekļauts Tirdzniecības ministrijas sarakstā kā ‘‘aktuāls’’ shēmas dalībnieks, maldina patērētājus un ļaunprātīgi izmanto viņu uzticību. Nepatiesi apgalvojumi grauj sistēmas uzticamību kopumā, un tāpēc būtu nekavējoties jāsvītro no uzņēmumu tīmekļa vietnēm.

ASV iestāžu piekļuve

12. Pašsertificētu uzņēmumu slepenības politikā būtu jāiekļauj informācija par apmēru, kādā ASV tiesību akti ļauj publiskām iestādēm vākt un apstrādāt datus, kas pārsūtīti saskaņā ar „drošības shēmu”. Uzņēmumi būtu īpaši jāaicina norādīt to slepenības politikā, kad tie piemēro izņēmumus attiecībā uz principiem, lai ievērotu valsts drošību, sabiedrības intereses vai tiesībaizsardzības prasības.

13. Ir svarīgi, lai izņēmums valsts drošības nolūkos, kas paredzēts Lēmumā par „drošības zonu”, tiktu izmantots tikai tādā apmērā, kādā tas ir absolūti nepieciešams un samērīgs.