EUROPOS
KOMISIJA

Briuselis, 2013 11 27
COM(2013) 847 final

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI

dėl „saugaus uosto“ nuostatų veikimo ES piliečių ir ES įsisteigusių bendrovių požiūriu

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI

dėl „saugaus uosto“ nuostatų veikimo ES piliečių ir ES įsisteigusių bendrovių požiūriu

1. ĮVADAS

1995 m. spalio 24 d. Direktyvoje Nr. 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau – Duomenų apsaugos direktyva) nustatytos asmens duomenų perdavimo iš ES valstybių narių į kitas, ES nepriklausančias, šalis taisyklės[1], taikytinos tuomet, jei toks perdavimas patenka į šios priemonės taikymo sritį[2].

Vadovaudamasi šia direktyva Komisija gali nuspręsti, kad trečioji šalis užtikrina tinkamo lygio apsaugą pagal savo nacionalinę teisę arba tarptautinius įsipareigojimus, prisiimtus siekiant apsaugoti asmenų teises – tokiu atveju nebūtų taikomi konkretūs duomenų perdavimo tokiai šaliai apribojimai. Šie sprendimai apibendrinamai vadinami **sprendimais dėl tinkamumo**.

2000 m. liepos 26 d. Komisija priėmė Sprendimą 520/2000/EB[3] (toliau – **„Saugaus uosto“ sprendimas**), kuriuo pripažinta, kad „saugaus uosto“ privatumo principai ir JAV komercijos departamento parengti „Dažnai užduodami klausimai“ (toliau – privatumo principai ir DUK) suteikia tinkamo lygio apsaugą perduodant asmens duomenis iš ES. „Saugaus uosto“ sprendimas priimtas prieš tai gavus 29 straipsnio darbo grupės ir 31 straipsnio komiteto nuomones, kurios buvo priimtos kvalifikuota valstybių narių balsų dauguma. Pagal Tarybos sprendimą 1999/468 „Saugaus uosto“ sprendimas buvo iš anksto patikrintas Europos Parlamento.

Todėl dabar galiojantis „Saugaus uosto“ sprendimas sudaro sąlygas laisvai perduoti[4] asmens informaciją iš ES valstybių narių[5] JAV bendrovėms, įsipareigojusioms taikyti privatumo principus tais atvejais, kai antraip – kadangi šiapus ir anapus Atlanto privatumo užtikrinimo tvarka labai skiriasi – toks perdavimas neatitiktų ES taikomų tinkamos duomenų apsaugos standartų.

Dabar galiojančio „saugaus uosto“ susitarimo veikimas grindžiamas sistemoje dalyvaujančių bendrovių įsipareigojimu ir jų autosertifikavimu. Šie susitarimai pasirašomi savanoriškai, tačiau juos pasirašius nustatytų taisyklių laikytis privaloma. Pagrindiniai tokių susitarimų principai:

a) įsipareigojusių bendrovių privatumo taisyklių skaidrumas,

b) rėmimasis „saugaus uosto“ principais bendrovių privatumo taisyklėse ir

c) vykdymo užtikrinimas, įskaitant atliekamą valdžios institucijų.

Šį esminį „saugaus uosto“ pagrindą reikia peržiūrėti atsižvelgiant į **pasikeitusias aplinkybes**:

---

1 Duomenų apsaugos direktyvos 25 ir 26 straipsniuose nustatytas teisinis pagrindas, kuriuo remiantis asmens duomenys perduodami iš ES į trečiąsias šalis, nepriklausančias EEE.

2 Kitos šios srities taisyklės nustatytos 2008 m. lapkričio 27 d. pamatinio sprendimo 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos 13 straipsnyje – jos taikytinos tuomet, jei toks perdavimas susijęs su asmens duomenimis, vienos valstybės narės perduodamais arba suteikiamais kitai valstybei narei, kuri tuos duomenis ketina perduoti trečiajai valstybei arba tarptautinei organizacijai siekiant nusikalstamų veikų prevencijos, tyrimo, išaiškinimo ir baudžiamojo persekiojimo ar baudžiamųjų sankcijų vykdymo tikslų.

3 2000 m. liepos 26 d. Komisijos sprendimas dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl saugaus uosto privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų DUK, OL L 215, 2000 8 28, p. 7.

4 Tai nereiškia, kad duomenų tvarkymui netaikytini kiti reikalavimai, jei tokių nustatyta nacionalinės teisės aktuose, kuriais įgyvendinama ES Duomenų apsaugos direktyva.

5 Duomenų perdavimui iš šių trijų EEE valstybių narių tai turi panašų poveikį, nes 1999 m. birželio 25 d. sprendimu 38/1999 (OL L 296/41, 2000 11 23) nustatyta, kad Direktyva Nr. 95/46/EB taikoma ir EEE susitarimo šalims.

a) geometrine progresija didėjančius duomenų srautus, kurie anksčiau atliko pagalbinę funkciją, o dabar tapo būtini greitai augant skaitmeninei ekonomikai, taip pat didžiulius pokyčius duomenų rinkimo, tvarkymo ir naudojimo srityse;

b) ypatingą duomenų srautų svarbą, ypač transatlantinei ekonomikai;[6]

c) greitai augantį „saugaus uosto“ sistemai priklausančių JAV bendrovių skaičių – nuo 2004 m. jis išaugo aštuonis kartus (nuo 400 2004 m. iki 3 246 2013 m.);

d) neseniai paskelbtą informaciją apie JAV sekimo programas, dėl kurios kyla klausimų apie apsaugos lygį, kuris užtikrinamas pagal „saugaus uosto“ susitarimą.

Atsižvelgiant į šias aplinkybes komunikate iš naujo įvertinamas „saugaus uosto“ sistemos veikimas. Jis **grindžiamas** Komisijos surinktais **įrodymais**, „EU-US Privacy Contact Group“ 2009 m. veiklos rezultatais, 2008 m. nepriklausomos organizacijos atliktu tyrimu[7] ir informacija, pateikta *ad hoc* ES ir JAV darbo grupei (toliau – darbo grupė), kuri buvo įsteigta paviešinus informaciją apie JAV sekimo programas (*žr. kitą susijusį dokumentą*). Šis komunikatas pateikiamas po dviejų **Komisijos vertinimo ataskaitų**, pateiktų pradiniu „Saugaus uosto“ susitarimo įgyvendinimo laikotarpiu, 2002 m.[8] ir 2004 m.[9]

2. „SAUGAUS UOSTO“ SISTEMA IR JOS VEIKIMAS

2.1. „Saugaus uosto“ sistema

JAV bendrovė, norinti prisijungti prie „saugaus uosto“ sistemos, turi: a) viešai skelbiamose privatumo taisyklėse nustatyti, kad ji pripažįsta ir iš tikrųjų taiko privatumo principus, taip pat b) atlikti autosertifikavimą, t. y. paskelbti JAV komercijos departamentui, kad ji laikosi šių principų. Toks autosertifikavimas iš naujo atliekamas kiekvienais metais. Prie „Saugaus uosto“ sprendimo pridėtame I priede išdėstyti „saugaus uosto“ privatumo principai apima reikalavimus, taikytinus tiek asmens duomenų apsaugai materialinės teisės požiūriu (duomenų vientisumo, saugumo, pasirinkimo ir tolesnio perdavimo principai), tiek procedūrinėms duomenų subjektų teisėms (pranešimo, prieigos ir vykdymo užtikrinimo principai).

„Saugaus uosto“ sistemos vykdymo užtikrinimą JAV atlieka dvi pagrindinės šios šalies institucijos – JAV komercijos departamentas ir JAV federalinė prekybos komisija.

Komercijos departamentas peržiūri kiekvieną bendrovių pateikiamą autosertifikatą ir kiekvieną kasmetinį jo atnaujinimą – taip užtikrinama, kad jie atitiktų visus reikalavimus, keliamus sistemai priklausančioms bendrovėms[10]. Jis atnaujina bendrovių, pateikusių autosertifikavimo raštus, sąrašą ir paskelbia šį sąrašą bei raštus savo svetainėje. Be to, jis kontroliuoja, kaip veikia „saugaus uosto“ sistema, ir išbraukia iš sąrašo bendroves, nesilaikančias jos principų.

---

6 Kai kurių tyrimų duomenimis, jei dėl privalomų bendrovių vidaus taisyklių, tipinių sutarčių nuostatų ir „saugaus uosto“ nuostatų nesilaikymo paslaugos ir tarpvalstybiniai duomenų srautai sutriktų, ES BVP gali sumažėti iki 0,8–1,3 %, o ES paslaugų eksporto į JAV apimtis dėl prastesnio konkurencingumo sumažėtų 6,7 %. Žr. “The Economic Importance of Getting Data Protection Right”, Europos tarptautinės politinės ekonomikos centro tyrimą, 2013 m. kovo mėn. atliktą JAV prekybos rūmų užsakymu.

7 Poveikio vertinimo tyrimas, 2008 m. Europos Komisijos pavedimu atliktas Namiūro universiteto Informatikos ir teisės tyrimų centro (*Centre de Recherche Informatique et Droit*, CRID).

8 2000 m. liepos 26 d. Komisijos tarnybų darbinis dokumentas „Komisijos sprendimo Nr. 520/2000/EB dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl saugaus uosto privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų DUK taikymas“, SEC(2002) 196, 2002 12 13.

9 Komisijos tarnybų darbinis dokumentas „Komisijos sprendimo Nr. 520/2000/EB dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl „saugaus uosto“ privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų DUK įgyvendinimas“, SEC(2004) 1323, 2004 10 20.

10 Jei įmonės autosertifikatas arba jo atnaujinimas neatitinka saugaus uosto reikalavimų, Komercijos departamentas praneša apie tai bendrovei, nurodydamas, kokių veiksmų ji turėtų imtis (pvz., patikslinti ar pakeisti duomenų apsaugos taisyklių aprašą), kad jos sertifikatas būtų patvirtintas.

Federalinė prekybos komisija, neviršydama savo įgaliojimų vartotojų apsaugos srityje, pagal laisvosios prekybos komisijos įstatymo (*Free Trade Commission Act*) 5 straipsnį imasi intervencinių priemonių nesąžiningos ar klaidinančios veiklos atveju. Federalinės prekybos komisijos vykdymo užtikrinimo veiksmai apima tyrimus dėl sistemai priklausančių bendrovių melagingų pranešimų apie atitiktį saugaus uosto reikalavimams ir šių principų nesilaikymo. Tam tikrais atvejais institucija, kompetentinga užtikrinti, kad oro vežėjai laikytųsi saugaus uosto principų, yra JAV transporto departamentas[11].

Dabar galiojantis „Saugaus uosto“ sprendimas yra ES teisės dalis ir turi būti taikomas valstybių narių valdžios institucijų. Sprendime nustatyta, kad ES nacionalinės **duomenų apsaugos institucijos** (toliau – DAI) tam tikrais atvejais gali neleisti perduoti duomenų „saugaus uosto“ sertifikatus turinčioms bendrovėms[12]. Komisijai nėra žinoma apie tokius atvejus nuo „saugaus uosto“ sistemos sukūrimo 2000 m. Be įgaliojimų, kurie ES nacionalinėms duomenų apsaugos institucijoms suteikti pagal „Saugaus uosto“ sprendimą, jos taip pat yra įgaliotos imtis intervencinių priemonių (taip pat tarptautinio duomenų perdavimo atvejais), kad būtų užtikrintas 1995 m. Duomenų apsaugos direktyvoje nustatytų bendrųjų duomenų apsaugos principų laikymasis.

Kaip išdėstyta dabar galiojančiame „Saugaus uosto“ sprendime, **Komisija kompetentinga** – pagal Reglamente 182/2011 nustatytą peržiūros procedūrą – atsižvelgdama į sprendimo taikymo patirtį bet kada šį sprendimą pataisyti, sustabdyti jo galiojimą arba apriboti jo taikymo sritį. Visų pirma tai taikytina JAV pusėje atsiradus sisteminių trūkumų, pavyzdžiui, jei įstaiga, turinti užtikrinti, kad Jungtinėse Amerikos Valstijose būtų laikomasi „saugaus uosto“ privatumo principų, netinkamai vykdo savo funkcijas, arba jei apsaugos lygį lemia ne „saugaus uosto“ principai, o juos užgožiančios JAV teisės nuostatos. Kaip ir bet kuris kitas Komisijos sprendimas, jis gali būti iš dalies pakeistas ar net panaikintas ir dėl kitų priežasčių.

2.2. „Saugaus uosto“ sistemos veikimas

Sertifikatus turi 3246[13] **bendrovės** – jų yra ir mažų, ir didelių[14]. Nors finansinių paslaugų ir telekomunikacijų sektoriai nepatenka į Federalinės prekybos komisijos vykdymo užtikrinimo sritį ir todėl jie nepriklauso „saugaus uosto“ sistemai, tarp sertifikuotų bendrovių yra daug pramonės ir paslaugų sektorių atstovų, įskaitant gerai žinomas interneto bendroves, taip pat pačių įvairiausių sričių – nuo informacinių ir kompiuterinių paslaugų iki farmacijos produktų, kelionių ir turizmo paslaugų, sveikatos priežiūros ir kredito kortelių paslaugų – įmonių[15]. Dažniausiai tai JAV bendrovės, teikiančios paslaugas ES vidaus rinkoje. Taip pat tai gali būti kai kurių ES bendrovių, kaip antai „Nokia“ arba „Bayer“, patronuojamosios bendrovės. 51 proc. sudaro bendrovės, tvarkančios Europos darbuotojų duomenis, kurie perduodami JAV žmogiškųjų išteklių valdymo tikslais[16].

---

11 Pagal JAV kodekso 49 antraštinės dalies 41712 punktą.

12 Tai yra, neleisti perduoti duomenis gali būti reikalinga tokiais dviem atvejais:
a) jei JAV valdžios institucija nustatė, kad bendrovė pažeidžia „saugaus uosto“ privatumo principus arba
b) jei yra didelė tikimybė, kad „saugaus uosto“ privatumo principai pažeidžiami; jei galima pagrįstai manyti, kad naudojant atitinkamą vykdymo užtikrinimo mechanizmą nesiimama ar nebus imtasi pakankamų ir savalaikių priemonių iškilusiai problemai išspręsti; tęsiant duomenų perdavimą kiltų neišvengiamas pavojus rimtai pakenkti duomenų subjektams; valstybės narės kompetentingos institucijos ėmėsi pagrįstų pastangų tokiomis aplinkybėmis pranešti apie tai bendrovei ir suteikti jai galimybę atsakyti.

13 2013 m. rugsėjo 26 d. „saugaus uosto“ organizacijų sąraše **3246** organizacijos buvo pažymėtos kaip **dalyvaujančios** (*current*), o **935** – kaip **nedalyvaujančios (*not current*)**.

14 „Saugaus uosto“ organizacijos, kuriose yra ne daugiau kaip 250 darbuotojų: 60 **%** (1925 iš 3246). „Saugaus uosto“ organizacijos, kuriose yra 251 arba daugiau darbuotojų: **40 %** (1295 iš 3246).

15 Pavyzdžiui, bendrovė „MasterCard“ dirba su tūkstančiais bankų – tai puikus pavyzdys, kad „saugaus uosto“ nuostatų negalima pakeisti kitomis asmens duomenų perdavimui skirtomis teisinėmis priemonėmis, kaip antai privalomomis bendrovių vidaus taisyklėmis arba sutartinėmis nuostatomis.

16 „Saugaus uosto“ organizacijos, kurių „saugaus uosto“ sertifikatas galioja ir žmogiškųjų išteklių duomenų tvarkymui (ir kurios įsipareigojo bendradarbiauti su ES duomenų apsaugos institucijomis ir laikytis jų reikalavimų): **51 %** (1671 iš 3246).

Kai kurios ES duomenų apsaugos institucijos **vis labiau nerimauja** dėl duomenų perdavimo pagal dabar taikomą „saugaus uosto“ sistemą. Kai kurių valstybių narių duomenų apsaugos institucijos kritikavo pernelyg bendrą principų formuluotę ir tai, kad per daug pasikliaujama autosertifikavimu ir savireguliavimu. Panašų susirūpinimą išreiškė ir pramonės atstovai – jie teigia, kad dėl vykdymo užtikrinimo trūkumo iškraipoma konkurencija.

Dabar galiojantis „Saugaus uosto“ susitarimas grindžiamas savanorišku bendrovių įsipareigojimu, įsipareigojusių bendrovių autosertifikavimu ir valdžios institucijų vykdomu autosertifikavimo įsipareigojimų vykdymo užtikrinimu. Tokiomis sąlygomis nepakankamas skaidrumas ir bet kokie vykdymo užtikrinimo trūkumai iš pagrindų kenkia „saugaus uosto“ sistemai.

Bet kokia skaidrumo arba vykdymo užtikrinimo spraga JAV pusėje reiškia, kad atsakomybė tenka Europos duomenų apsaugos institucijoms ir sistemai priklausančioms bendrovėms. 2010 m. balandžio 29 d. Vokietijos duomenų apsaugos institucijos priėmė sprendimą, pagal kurį bendrovės, perduodančios duomenis iš Europos į JAV, turi aktyviai patikrinti, ar duomenis gaunančios JAV bendrovės iš tikrųjų laikosi „saugaus uosto“ privatumo principų, ir kuriame rekomenduojama, kad „duomenis perduodanti bendrovė turi bent nustatyti, ar duomenų gavėjo „saugaus uosto“ sertifikatas dar galioja“[17].

Po to, kai buvo atskleista informacija apie JAV sekimo programas, Vokietijos DAI ėmėsi tolesnių priemonių ir 2013 m. liepos 24 d. išreiškė nerimą, kad „labai tikėtina, jog Komisijos sprendimuose nustatyti principai yra pažeidinėjami“[18]. Tam tikrais atvejais kai kurios DAI (pvz., Bremeno) paprašė bendrovių, perduodančių asmens duomenis JAV paslaugų teikėjams, pranešti joms, ar ir kaip atitinkami paslaugų teikėjai užtikrina, kad duomenys nebūtų prieinami Nacionalinei saugumo agentūrai. Airijos DAI pranešė neseniai, paskelbus apie JAV žvalgybos agentūrų programas, gavusi du skundus dėl „saugaus uosto“ programos, tačiau atsisakiusi juos nagrinėti, kadangi asmens duomenų perdavimas trečiajai šaliai atitiko Airijos duomenų apsaugos teisės reikalavimus. Išnagrinėjusi panašų skundą Liuksemburgo DAI nustatė, kad perduodamos duomenis į JAV bendrovės „Microsoft“ ir „Skype“ nepažeidė Liuksemburgo duomenų apsaugos įstatymo[19]. Vis dėlto Airijos aukštasis teismas neseniai leido pareikšti apeliacinį skundą, kurio pagrindu jis nagrinės, kodėl paskelbus apie JAV sekimo programas Airijos duomenų apsaugos komisaras nesiėmė veiksmų. Vieną iš šių dviejų skundų pateikė studentų grupė „Europa prieš *Facebook*“, taip pat pateikusi panašų skundą prieš bendrovę „Yahoo“ Vokietijoje – jį nagrinėja kompetentingos Vokietijos duomenų apsaugos institucijos.

Šios skirtingos duomenų apsaugos institucijų reakcijos į paskelbtą informaciją apie sekimą rodo, kad skirtingo reglamentavimo pavojus „saugaus uosto“ sistemoje yra realus, ir kelia abejonių, ar vykdymo užtikrinimas šioje sistemoje yra pakankamas.

---

17 Žr. 2010 m. balandžio 28–29 d. *Düsseldorfer Kreis* sprendimą. Žr. *Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29*. 2010 m., Hanoveris. http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile Tačiau Europos duomenų apsaugos priežiūros pareigūnas Peteris Hustinxas 2013 m. spalio 7 d. Europos Parlamento LIBE komitete kalbėdamas apie „saugų uostą“ pasakė, kad „padaryta didelė pažanga, ir daugelis problemų jau išspręstos“: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf .

18 Žr. Vokietijos duomenų apsaugos komisijos narių konferencijos rezoliuciją, kurioje pabrėžiama, kad žvalgybos tarnybos kelia didžiulę grėsmę duomenų srautams tarp Vokietijos ir ne Europos šalių: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870

19 Žr. 2013 m. lapkričio 18 d. Liuksemburgo DAI pranešimą spaudai.

3. SISTEMAI PRIKLAUSANČIŲ BENDROVIŲ PRIVATUMO TAISYKLIŲ SKAIDRUMAS

Pagal 6 DUK, pateikiamą „Saugaus uosto“ sprendimo II priede, bendrovės, norinčios įgyti „saugaus uosto“ sistemos sertifikatą, turi pateikti Komercijos departamentui savo privatumo taisykles ir jas viešai paskelbti. Jose turi būti įsipareigojama laikytis privatumo principų. Reikalavimas **viešai paskelbti** autosertifikuotų bendrovių **privatumo taisykles** ir jų pasižadėjimą laikytis privatumo principų yra labai svarbus sistemos veikimui.

Dėl ribotų galimybių susipažinti su tokių bendrovių privatumo taisyklėmis nukenčia asmenys, kurių asmens duomenys yra renkami ir tvarkomi, be to, tai gali būti **pranešimo principo pažeidimas**. Tokiais atvejais asmenys, kurių duomenys yra perduodami iš ES, gali nežinoti apie savo teises ir autosertifikuotos bendrovės pareigas.

Be to, bendrovių įsipareigojimas laikytis privatumo principų **susijęs su Federalinės prekybos komisijos įgaliojimais užtikrinti šių principų vykdymą** tais atvejais, kai bendrovės jų nesilaiko vykdydamos nesąžiningą ar klaidinančią veiklą. Dėl nepakankamo skaidrumo JAV bendrovėse Federalinės prekybos komisijai sunkiau vykdyti priežiūrą ir mažėja vykdymo užtikrinimo veiksmingumas.

Pastaraisiais metais daug autosertifikuotų bendrovių viešai nepaskelbė savo privatumo taisyklių ir (arba) pasižadėjimo laikytis privatumo principų. 2004 m. „saugaus uosto“ ataskaitoje nurodyta, kad Komercijos departamentui būtina imtis **aktyvesnio vaidmens tikrinant, ar laikomasi** šio reikalavimo.

Nuo 2004 m. Komercijos departamentas parengė **naujas informavimo priemones**, kurios turėtų padėti bendrovėms laikytis savo skaidrumo įsipareigojimų. Atitinkamos informacijos apie šią sistemą galima rasti „saugiam uostui“ skirtoje Komercijos departamento svetainėje[20], kurioje bendrovės taip pat gali įkelti savo privatumo taisykles. Komercijos departamentas nurodė, kad bendrovės naudojasi šia galimybe ir skelbia Komercijos departamento svetainėje savo privatumo taisykles pateikdamos paraišką prisijungti prie „saugaus uosto“ sistemos[21]. Be to, 2009–2013 m. Komercijos departamentas paskelbė kelis vadovus bendrovėms, norinčioms prisijungti prie „saugaus uosto“ sistemos, kaip antai „Guide to Self-Certification“ ir „Helpful Hints on Self-Certifying Compliance“[22].

Atitikties skaidrumo reikalavimams lygis įvairiose bendrovėse skirtingas. kai kurios bendrovės vykdydamos autosertifikavimo procedūrą savo privatumo taisykles tik pateikia Komercijos departamentui, tačiau dauguma ne tik įkelia jas į Komercijos departamento svetainę, bet ir viešai paskelbia savo svetainėse. Tačiau šios **taisyklės ne visada pateikiamos vartotojui patogia ir lengvai suprantama forma**. Nuorodos į privatumo taisykles ne visada gerai veikia, o kartais nukreipia ne į tą puslapį.

Iš sprendimo ir jo priedų aišku, kad bendrovėms keliamas reikalavimas viešai paskelbti savo privatumo taisykles **apima daugiau nei vien pareigą pranešti** Komercijos departamentui apie autosertifikavimą. Sertifikavimo reikalavimai, išdėstyti DUK, apima privatumo taisyklių aprašymą ir skaidrų informavimą apie tai, kur jos viešai skelbiamos[23]. Privatumo taisyklių aprašas turi būti aiškus ir lengvai prieinamas visuomenei. Jame turi būti pateikiama nuoroda į Komercijos departamento „saugaus uosto“ svetainę, kurioje skelbiami visi sistemoje šiuo metu dalyvaujantys nariai, ir nuoroda į alternatyvaus ginčų sprendimo paslaugų teikėją.

---

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

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

22 Vadovą galima rasti sistemos svetainėje, adresu http://export.gov/SafeHarbour/ Helpful Hints: http://export.gov/SafeHarbour/eu/eg_main_018495.asp.

23 2013 m. lapkričio 12 d. Komercijos departamentas patvirtino, kad „šiuo metu bendrovės, turinčios viešas svetaines ir dirbančios su vartotojų / klientų / lankytojų duomenimis, turi jose paskelbti saugaus uosto reikalavimus atitinkančias privatumo taisykles“ (žr. 2013 m lapkričio 12 d. dokumentą „U.S.-EU Cooperation to Implement the Safe Harbor Framework“).

Tačiau 2000–2013 m. daug sistemoje dalyvaujančių bendrovių šių reikalavimų neįvykdė. 2013 m. vasario mėn. susirašinėdamas su Komisija darbiniais klausimais Komercijos departamentas pripažino, kad tikėtina, jog iki 10 proc. sertifikuotų bendrovių savo svetainėse nėra paskelbusios privatumo taisyklių, kuriose būtų pateikiamas aiškus jų pasižadėjimas laikytis „saugaus uosto“ principų.

Naujausi statistiniai duomenys taip pat rodo, kad vis dar neišspręsta **melagingų teiginių apie atitiktį „saugaus uosto“ reikalavimams** problema. Maždaug 10 proc. bendrovių, kurios teigia priklausančios „saugus uosto“ sistemai, nėra įtrauktos į Komercijos departamento sudaromą esamų narių sąrašą[24]. Tokie melagingi teiginiai gali būti dvejopos prigimties: juos naudoja bendrovės, niekada nepriklausiusios saugaus uosto sistemai, ir bendrovės, anksčiau jai priklausiusios, tačiau Komercijos departamente reguliariai kartą per metus neatnaujinusios savo sertifikato. Tokiu atveju jos lieka „saugaus uosto“ svetainės sąraše, su prierašu „nedalyvaujanti“ (*not current*), kuris reiškia, kad bendrovė yra buvusi sistemos narė ir privalo toliau užtikrinti jau tvarkytų duomenų apsaugą. Federalinė prekybos komisija įgaliota imtis intervencinių priemonių nesąžiningos veiklos ar „saugaus uosto“ principų nesilaikymo atvejais (žr. 5.1. skirsnį). Tai, kad nėra aiškiai apibrėžta, kas yra melagingi teiginiai, kenkia sistemos patikimumui.

Europos Komisija, palaikydama su Komercijos departamentu nuolatinį ryšį, 2012 ir 2013 m. įspėjo jį, kad vien pateikusios Komercijos departamentui savo privatumo taisyklių aprašą, bendrovės dar neįvykdo skaidrumo įsipareigojimų. Privatumo taisyklių aprašas turi būti viešai paskelbtas. Komercijos departamento taip pat paprašyta **sugriežtinti reguliarius bendrovių svetainių patikrinimus**, kurie pagal patikros procedūrą atliekami bendrovei pateikus pirmąjį sertifikatą arba jį kasmet atnaujinant, taip pat taikyti sankcijas bendrovėms, kurios nesilaiko skaidrumo reikalavimų.

Pirmiausia, reaguodamas į ES išreikštą susirūpinimą, **Komercijos departamentas nuo 2013 m. kovo mėn. nustatė privalomą reikalavimą**, kad „saugaus uosto“ bendrovės, turinčios svetainę, skelbtų joje klientų ir (arba) vartotojų duomenų privatumo taisykles. Be to, nuo šiol Komercijos departamentas praneša visoms bendrovėms, kurių privatumo taisyklėse nebuvo nuorodos į Komercijos departamento „saugaus uosto“ svetainę, kad tokia nuoroda jose turi būti, taip suteikiant įmonės puslapį skaitančiam vartotojui galimybę tiesiogiai patekti į oficialų „saugaus uosto“ sąrašą ir svetainę. Taip Europos duomenų subjektai galės nedelsdami, neatlikdami atskiros paieškos internete, pasitikrinti, kokie yra bendrovės įsipareigojimai, apie kuriuos ji pranešė Komercijos departamentui. Be to, nuo šiol Komercijos departamentas praneša bendrovėms, kad viešai skelbiamose jų privatumo taisyklėse turi būti nurodomi nepriklausomo ginčų sprendimo paslaugų teikėjo kontaktiniai duomenys[25].

Šį procesą reikia paspartinti, kad ne vėliau kaip 2014 m. kovo mėn. (t. y. iki kasmetinio sertifikatų atnaujinimo termino, skaičiuojant nuo naujų reikalavimų nustatymo 2013 m. kovo mėn.) visos sertifikuotos bendrovės visiškai atitiktų „saugaus uosto“ reikalavimus.

---

[24] 2013 m. rugsėjo mėn. Australijos konsultacijų įmonė „Galexia“ palygino melagingus teiginius apie dalyvavimą „saugaus uosto“ sistemoje 2008 m. ir 2013 m. Pagrindinė išvada: 2008–2013 m. padidėjus saugaus „saugaus uosto“ sistemos narių skaičiui (nuo 1 109 iki 3 246), melagingų teiginių skaičius taip pat padidėjo, nuo 206 iki 427. http://www.galexia.com/public/about/news/about_news-id225.html .

[25] 2013 m. kovo–rugsėjo mėn. Komercijos departamentas:
• pranešė 101 bendrovei, *į „saugaus uosto“ svetainę jau įkėlusiai savo „saugaus uosto“ reikalavimus atitinkančias privatumo taisykles*, kad šias taisykles būtina paskelbti ir savo įmonės svetainėje;
• pranešė 154 bendrovėms, kurios savo privatumo taisyklėse dar nepateikia nuorodos į „saugaus uosto“ svetainę, kad jos privalo tai padaryti;
• daugiau kaip 600 bendrovių pranešė, kad savo privatumo taisyklėse jos privalo pateikti nepriklausomo ginčų sprendimo paslaugų teikėjo kontaktinius duomenis.

Nepaisant to, vis dar kyla abejonių, ar visos autosertifikuotos bendrovės visiškai atitinka skaidrumo reikalavimus. Komercijos departamentas turėtų griežiau stebėti ir tirti, kaip laikomasi įsipareigojimų, prisiimtų atliekant pradinį sertifikavimą ir jį kasmet atnaujinant.

4. RĖMIMASIS „SAUGAUS UOSTO“ PRINCIPAIS BENDROVIŲ PRIVATUMO TAISYKLĖSE

Autosertifikuotos bendrovės, norėdamos įgyti ir išlaikyti „saugaus uosto“ privalumus, privalo laikytis Sprendimo I priede nurodytų privatumo principų.

2004 m. ataskaitoje Komisija nustatė, kad daug bendrovių savo duomenų tvarkymo taisyklėse **neteisingai pritaikė „saugaus uosto“ privatumo principus**. Pavyzdžiui, asmenims ne visada suteikiama aiški ir skaidri informacija apie tikslus, kuriais buvo tvarkomi jų duomenys, arba jiems nebuvo suteikta galimybė pasirinkti, ar leisti atskleisti savo duomenis trečiajai šaliai arba panaudoti juos tikslui, nesuderinamam su pirminiu jų rinkimo tikslu. 2004 m. Komisijos ataskaitoje teigiama, kad Komercijos departamentas *turėtų aktyviau dalyvauti reguliuojant dalyvavimą „saugaus uosto“ sistemoje ir gerinant informuotumą apie privatumo principus*[26].

Kol kas šioje srityje padaryta labai nedidelė pažanga. Nuo 2009 m. sausio 1 d. prieš atnaujindamas bet kurios bendrovės „saugaus uosto“ sertifikatą – jis turi būti atnaujinamas kasmet – Komercijos departamentas įvertina tos bendrovės privatumo taisykles. Tačiau šis vertinimas nėra išsamus. **Neatliekamas išsamus** autosertifikuotų bendrovių **realios veiklos vertinimas**, kuris labai padidintų pasitikėjimą autosertifikavimo procedūra.

Atsižvelgiant į Komisijos raginimus Komercijos departamentui griežčiau ir sistemingiau prižiūrėti autosertifikuotas bendroves, **naujoms paraiškoms dabar skiriama daugiau dėmesio**. 2010–2013 m. gerokai padaugėjo naujų paraiškų, kurios nepriimtos, o grąžintos bendrovėms su prašymu pakoreguoti privatumo taisykles: sertifikatus atnaujinančių bendrovių atveju jų padaugėjo du kartus, o pirmą „saugaus uosto“ paraišką teikiančių bendrovių – tris kartus[27]. Komercijos departamentas patikino Komisiją, kad visi, pirmą kartą išduodami ar atnaujinami sertifikatai tvirtinami tik tuomet, jei bendrovės privatumo taisyklės atitinka visus reikalavimus, t. y. jose aiškiai įsipareigojama laikytis nustatytų saugaus uosto privatumo principų, ir šios taisyklės viešai paskelbtos. Savo „saugaus uosto“ sąrašo įraše bendrovė privalo nurodyti, kur galima rasti šias taisykles. Taip pat reikalaujama savo svetainėje aiškiai nurodyti alternatyvaus ginčų sprendimo paslaugų teikėją ir pateikti nuorodą į Komercijos departamento „saugaus uosto“ sertifikavimo puslapį. Tačiau manoma, kad daugiau kaip 30 proc. saugaus uosto narių savo svetainėse skelbiamose privatumo taisyklėse neteikia informacijos apie ginčų sprendimą[28].

Dauguma bendrovių, kurias Komercijos departamentas išbraukė iš „saugaus uosto“ sąrašo, to tiesiogiai paprašė pačios (pvz., įmonės, kurios susijungė ar buvo įgytos, pakeitė veiklos pobūdį arba nutraukė veiklą). Rečiau bendrovės išbraukiamos iš sąrašo todėl, kad skelbiamos svetainės yra neveikiančios, atitinkamos bendrovės nebeveikia, o bendrovės statusas sąraše kelerius metus buvo „nedalyvaujanti“ (*not current*)[29]. Svarbu tai, kad nė viena bendrovė

---

[26] Žr. 2004 m. ataskaitą SEC(2004) 1323, p. 8.

[27] Pagal 2013 m. rugsėjo mėn. Komercijos departamento pateiktus statistinius duomenis, 2010 m. Komercijos departamentas 18 proc. (93) iš 512 pirmą kartą paraišką teikiančių bendrovių ir 16 proc. (231) iš 1 417 sertifikatą atnaujinančių bendrovių nurodė pataisyti privatumo taisykles ir (arba) „saugaus uosto“ paraiškas. Tačiau Komisijai paraginus griežčiau, atidžiau ir sistemingiau nagrinėti visas paraiškas, iki 2013 m. rugsėjo vidurio pataisyti privatumo taisykles paprašyta 56 proc. (340) iš 602 pirmą kartą paraišką teikiančių bendrovių ir 27 proc. (493) iš 1 809 sertifikatą atnaujinančių bendrovių.

[28] 2013 m. spalio 7 d. Chriso Connolly („Galexia“) pranešimas Europos Parlamento LIBE komitete.

[29] 2011 m. gruodžio mėn. duomenimis, JAV Komercijos departamentas iš „saugaus uosto“ sąrašo išbraukė 323 bendroves: 94 bendrovės išbrauktos, nes nebevykdė veiklos; 88 bendrovės – dėl įsigijimo ar susijungimo, 95 – patronuojančiosios bendrovės prašymu, 41 – nes kelerius metus nepateikė paraiškos atnaujinti sertifikatą, ir dar 5 – dėl kitų įvairių priežasčių.

nebuvo išbraukta Komercijos departamentui per patikrinimą nustačius atitikties reikalavimams trūkumų.

„Saugaus uosto“ sąraše skelbiami įrašai atlieka viešo pranešimo funkciją, taip pat juose skelbiama, kokius „saugaus uosto“ įsipareigojimus yra prisiėmusi bendrovė. **Įsipareigojimas laikytis „saugaus uosto“ principų yra neterminuotas**, kai kalbama apie duomenis, gautus per laikotarpį, kai bendrovė naudojosi „saugaus uosto“ privalumais – tokiems duomenims privatumo principus bendrovė turi taikyti tol, kol juos saugo, naudoja ar atskleidžia, net jei dėl kokios nors priežasties nebedalyvauja „saugaus uosto“ sistemoje.

„Saugaus uosto“ **paraiškas pateikusios bendrovės, kurios nepraėjo** Komercijos departamento **administracinio patikrinimo** ir todėl nebuvo įtrauktos į „saugaus uosto“ sąrašą, **2010 m.** sudarė tik **6 proc.** – 33 iš 513 pirmą kartą paraišką teikusių bendrovių nebuvo įtrauktos į „saugaus uosto“ sąrašą, nes neatitiko Komercijos departamento autosertifikavimo standartų. **2013 m. 12 proc.** – 75 iš 605 pirmą kartą paraišką teikusių bendrovių nebuvo įtrauktos į „saugaus uosto“ sąrašą, nes neatitiko Komercijos departamento autosertifikavimo standartų.

Kad priežiūra būtų vykdoma skaidriau, Komercijos departamentas turėtų mažų mažiausiai savo svetainėje skelbti sąrašą bendrovių, kurios buvo išbrauktos iš „saugaus uosto“ sąrašo, ir nurodyti priežastis, dėl kurių jų sertifikatai nebuvo atnaujinti. Komercijos departamento „saugaus uosto“ narių sąraše naudojama žyma „nedalyvaujanti“ (*not current*) turėtų būti laikoma ne vien informacine – prie jos turėtų būti **aiškus įspėjimas** (žodinis ir grafinis), kad šiuo metu bendrovė neatitinka „saugaus uosto“ reikalavimų.

Be to, kai kurios bendrovės vis dar neužtikrina atitikties visiems „saugaus uosto“ principams. Be skaidrumo problemos, kuri nagrinėjama pirmiau 3 skirsnyje, iš autosertifikuotų bendrovių privatumo taisyklių dažnai neaišku, kokiais tikslais duomenys renkami, ir ar asmuo turi teisę pasirinkti, leisti ar ne atskleisti duomenis trečiosioms šalims. Todėl kyla abejonių, ar privatumo principų srityje įgyvendinami pranešimo ir pasirinkimo principai. Pranešimas ir pasirinkimas – būtini elementai užtikrinant, kad duomenų subjektai galėtų kontroliuoti, kas daroma su jų asmenine informacija.

Pirmas svarbiausias dalykas atitikties procese – perkelti „saugaus uosto“ privatumo principus į bendrovių privatumo taisykles – įgyvendinamas nepakankamai. Komercijos departamentas šį klausimą turėtų spręsti kuo greičiau: reikia parengti metodiką, pagal kurią būtų užtikrinama komercinės bendrovių veiklos ir jų ryšių su klientais atitiktis reikalavimams. **Komercijos departamentas turi imtis aktyviai tikrinti, ar bendrovės perkelia „saugaus uosto“ privatumo principus į savo privatumo taisykles**, o ne laukti, kol atsiras pagrindas taikyti vykdymo užtikrinimo procedūrą gavus asmenų skundų.

5. VALDŽIOS INSTITUCIJŲ ATLIEKAMAS VYKDYMO UŽTIKRINIMAS

Yra nemažai priemonių, kuriomis galima veiksmingai užtikrinti „saugaus uosto“ nuostatų vykdymą ir suteikti teisinę apsaugą asmenims, kurių asmeninės informacijos apsauga nukentėjo dėl privatumo principų nesilaikymo.

Pagal vykdymo užtikrinimo principą autosertifikuotų bendrovių privatumo taisyklėse turi būti nustatyti veiksmingi atitikties užtikrinimo mechanizmai. Vadovaujantis vykdymo užtikrinimo privatumo srityje principu, kaip išaiškinta 11, 5 ir 6 DUK, šis reikalavimas gali būti vykdomas įsipareigojant pasitelkti **nepriklausomas ginčų sprendimo organizacijas**, viešai deklaruojančias kompetenciją nagrinėti individualius skundus dėl privatumo principų pažeidimo. Taip pat tą galima užtikrinti organizacijoms įsipareigojant bendradarbiauti su **ES**

duomenų apsaugos specialistų grupe[30]**.** Be to, pagal Federalinės prekybos komisijos įstatymo 5 skirsnį, kuriuo draudžiama nesąžininga ar klaidinanti veikla ir praktika, vykdoma prekyboje ar daranti jai poveikį, autosertifikuotos bendrovės patenka į Federalinės prekybos komisijos jurisdikciją[31].

2004 m. ataskaitoje buvo išreikštas susirūpinimas dėl vykdymo užtikrinimo „saugaus uosto“ sistemoje – joje teigiama, kad Federalinė prekybos komisija turėtų atlikti aktyvesnį vaidmenį inicijuojant tyrimus ir didinant asmenų informuotumą apie jų teises. Dar viena problema – tai, kad nėra aiški Federalinės prekybos komisijos kompetencija užtikrinant privatumo principų įgyvendinimą žmogiškųjų išteklių duomenų srityje.

ES duomenų apsaugos specialistų grupė – įstaiga, kompetentinga nagrinėti skundus dėl žmogiškųjų išteklių duomenų – gavo vieną tokį skundą[32]. Tačiau dėl to, kad nėra skundų, negalima daryti išvados, kad sistema nepriekaištingai veikia. Reikėtų numatyti bendrovių atitikties reikalavimams *ex officio* patikras, kurios leistų į, kaip iš tikrųjų įgyvendinami duomenų apsaugos įsipareigojimai. ES duomenų apsaugos institucijos taip pat turėtų imtis veiksmų, kad ES duomenų apsaugos specialistų grupės veikla būtų geriau žinoma.

Nustatyta problemų, susijusių su alternatyvaus ginčo sprendimo organizacijų pasitelkimu vykdymo užtikrinimo funkcijoms atlikti. Kai kurios šių organizacijų nėra pajėgios spręsti ginčų, kylančių dėl privatumo principų nesilaikymo. Šią problemą reikia spręsti.

5.1. Federalinė prekybos komisija

Bendrovėms pažeidus „saugaus uosto“ įsipareigojimus Federalinė prekybos komisija gali imtis vykdymo užtikrinimo priemonių. Sukūrus „saugaus uosto“ sistemą Federalinė prekybos komisija įsipareigojo visas ES valstybių narių institucijų jai perduotas bylas peržiūrėti pirmumo tvarka[33]. Kadangi per pirmuosius dešimt metų nuo susitarimo įsigaliojimo skundų negauta, Federalinė prekybos komisija nusprendė nustatinėti „saugaus uosto“ pažeidimus atlikdama kiekvieną privatumo ir duomenų saugumo tyrimą. Nuo 2009 m. Federalinė prekybos komisija 10 kartų pritaikė vykdymo užtikrinimo priemones bendrovėms, padariusioms „saugaus uosto“ pažeidimų. Pritaikius šias priemones paprastai buvo priimamas taikos susitarimas (*settlement order*) – skiriant nemažą baudą –, kuriuo draudžiama naudoti klaidinančius privatumo teiginius, įskaitant dėl atitikties „saugaus uosto“ reikalavimams, ir atitinkamai bendrovei nurodoma 20 metų vykdyti išsamias privatumo užtikrinimo programas ir auditą. Federalinės prekybos komisijos prašymu bendrovės privalo leisti atlikti nepriklausomą jų privatumo programų vertinimą. Tokie vertinimai reguliariai pateikiami Federalinei prekybos komisijai. Federalinės prekybos komisijos nutartimis šioms bendrovėms taip pat uždraudžiama teikti tikrovės neatitinkančią informaciją apie jų veiklą privatumo užtikrinimo srityje ir dalyvavimą „saugaus uosto“ ar kitose panašiose privatumo užtikrinimo sistemose. Taip buvo, pavyzdžiui, Federalinės prekybos komisijai atlikus tyrimus dėl

---

30 ES duomenų apsaugos specialistų grupė – tai įstaiga, įgaliota nagrinėti asmenų skundus dėl galimų JAV bendrovių, priklausančių „saugaus uosto“ sistemai, padarytų „saugaus uosto“ principų pažeidimų ir priimti sprendimus. Bendrovės, įsipareigojusios taikyti „saugaus uosto“ principus, turi pasirinkti, ar problemos, galinčios kilti dėl „saugaus uosto“ principų nesilaikymo, bus sprendžiamos taikant nepriklausomą ginčų sprendimo mechanizmą, ar bendradarbiaujant su ES duomenų apsaugos specialistų grupe. Tačiau bendradarbiavimas su ES duomenų apsaugos specialistų grupe yra privalomas, jeigu JAV bendrovė tvarko žmogiškųjų išteklių asmens duomenis, perduotus iš ES dėl darbo santykių. Jei bendrovė įsipareigoja bendradarbiauti su ES grupe, ji taip pat privalo įsipareigoti, kad šiai grupei teigiant, jog norėdama užtikrinti atitiktį „saugaus uosto“ principams bendrovė turi imtis konkrečių veiksmų, ji vykdys visas šios grupės rekomendacijas, taip pat rekomendacijas taikyti taisomąsias bei kompensacines priemones.

31 Pagal JAV kodekso 49 antraštinės dalies 41712 skirsnį Transporto departamentas turi panašią kompetenciją oro vežėjų atžvilgiu.

32 Skundas gautas iš Šveicarijos piliečio, todėl ES duomenų apsaugos specialistų grupės buvo perduotas Šveicarijos duomenų apsaugos institucijai (Šveicarijai JAV turi atskirą „saugaus uosto“ sistemą).

33 Žr. 2000 m. liepos 26 d. Komisijos sprendimo 2000/520/EB V priedą.

bendrovių „Google“, „Facebook“ ir „MySpace“.[34] 2012 m. „Google“ sutiko sumokėti 22,5 mln. USD baudą, kad būtų išspręstas ginčas, kuriame ji buvo kaltinama pažeidusi pritarimo tvarką (*consent order*). Visuose savo atliekamuose privatumo tyrimuose Federalinė prekybos komisija *ex officio* tikrina, ar nepažeidžiami „saugaus uosto“ reikalavimai.

Federalinė prekybos komisija neseniai dar kartą priminė savo pažadą ir įsipareigojimus pirmumo tvarka nagrinėti visas privatumo srities savireguliavimo bendrovių ir ES valstybių narių jai perduotas bylas, grindžiamas įtarimais kad bendrovė nesilaiko „saugaus uosto“ principų.[35] Per pastaruosius trejus metus Europos duomenų apsaugos institucijos Federalinei prekybos komisijai perdavė vos kelias bylas.

Pastaraisiais mėnesiais pradėta plėtoti transatlantinį duomenų apsaugos institucijų bendradarbiavimą. Pavyzdžiui, 2013 m. birželio 26 d. Federalinė prekybos komisija ir Airijos duomenų apsaugos biuro vadovas pasirašė susitarimo memorandumą dėl tarpusavio pagalbos užtikrinant asmens duomenų apsaugos privačiajame sektoriuje nuostatų vykdymą. Memorandume nustatoma sistema, leisianti aktyviau, paprasčiau ir veiksmingiau bendradarbiauti užtikrinant privatumo nuostatų vykdymą[36].

2013 m. rugpjūčio mėn. Federalinė prekybos komisija pranešė dar sugriežtinusi patikras bendrovėse, kurios turi prieigą prie didelių asmens informacijos duomenų bazių. Taip pat ji sukūrė portalą, kuriame vartotojai gali pateikti JAV bendrovei skundą dėl privatumo pažeidimo[37].

Federalinė prekybos komisija taip pat turėtų pasistengti geriau ištirti melagingus teiginius apie priklausymą „saugaus uosto“ sistemai. Bendrovė, kuri savo svetainėje teigia, kad atitinka „saugaus uosto“ reikalavimus, tačiau kuri neįtraukta į Komercijos departamento sąrašą kaip dalyvaujanti sistemos narė, klaidina vartotojus ir piktnaudžiauja jų pasitikėjimu. Melagingi teiginiai kenkia visos sistemos patikimumui, todėl jie turi būti nedelsiant ištrinti iš bendrovių svetainių. Bendrovėms turi būti taikomas privalomas reikalavimas neklaidinti vartotojų, kurio nesilaikant gali būti imamasi vykdymo užtikrinimo priemonių. Federalinė prekybos komisija turėtų ir toliau bandyti išaiškinti melagingus teiginius apie „saugų uostą“, kaip pavyzdžiui *Karnani* byloje, kai Federalinė prekybos komisija uždarė Kalifornijos interneto svetainę už tai, kad joje buvo skelbiama melaginga informacija apie registraciją „saugaus uosto“ sistemoje, o bendrovė vertėsi nesąžininga elektroninės prekybos veikla, kuria siekta pasinaudoti Europos vartotojais[38].

2013 m. spalio 29 d. Federalinė prekybos komisija paskelbė „per pastaruosius mėnesius pradėjusi daug tyrimų dėl atitikties „saugaus uosto“ reikalavimams“ ir kad „ateinančiais mėnesiais“ numatyta imtis daugiau vykdymo užtikrinimo priemonių. Be to, Federalinė prekybos komisija patvirtino, kad yra „įsipareigojusi ieškoti būdų padidinti sistemos veiksmingumą“ ir „kaip visada, bus dėkinga už svarius įrodymus, tokius kaip praeitą mėnesį iš Europoje dirbančio vartotojų teisių gynėjo gautas skundas, kuriame pateikiama daug

---

34 2009–2012 m. Federalinė prekybos komisija dešimt kartų pritaikė vykdymo užtikrinimo priemones dėl „saugaus uosto“ įsipareigojimų nevykdymo: Federalinė prekybos komisija prieš Javian Karnani ir „Balls of Kryptonite, LLC“ (2009 m.), „World Innovators, Inc.“ (2009 m.), „Expat Edge Partners LLC“ (2009 m.), „Onyx Graphics, Inc.“ (2009 m.), „Directors Desk LLC“ (2009 m.), „Progressive Gaitways LLC“ (2009 m.), „Collectify LLC“ (2009 m.), „Google Inc.“ (2011 m.), „Facebook, Inc.“ (2011 m.), „Myspace LLC“ (2012 m.). Žr. „Federal Trade Commission of Safe Harbour Commitments: http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf . Taip pat žr. “Case Highlights“: http://business.ftc.gov/us-eu-Safe-Harbour-framework. Daugumoje šių bylų buvo nagrinėjamos problemos dėl bendrovių, kurios buvo prisijungusios prie „saugaus uosto“ sistemos, tačiau neatlikusios kasmetinio sertifikato atnaujinimo ir toliau prisistato kaip sistemos narės.

35 Šis įsipareigojimas buvo patvirtintas 2013 m. balandžio 17 d. Briuselyje įvykusiame Federalinės prekybos komisijos narės Julie Brill susitikime su ES duomenų apsaugos institucijų (29 straipsnio darbo grupės) atstovais.

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

37 Vartotojai gali teikti skundus pasinaudodami Federalinės prekybos komisijos programa „Complaint Assistant“ (https://www.ftccomplaintassistant.gov/), o užsienio vartotojai gali pateikti skundus per econsumer.gov (http://www.econsumer.gov).

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

įtarimų dėl „saugaus uosto“ nuostatų pažeidimų“.[39] Ši įstaiga taip pat įsipareigojo „sistemingai stebėti, kaip vykdomos „saugaus uosto“ klausimais jos priimtos nutartys, kaip stebi visų savo nutarčių vykdymą“[40].

2013 m. lapkričio 12 d. Federalinė prekybos komisija informavo Europos Komisiją, kad „**jei bendrovės privatumo taisyklėse žadama teikti „saugaus uosto“ apsaugą, vien tai, kad ji neužsiregistravo sistemoje arba nepratęsė savo registracijos, nereiškia, kad Federalinė prekybos komisija negalės tai bendrovei taikyti „saugaus uosto“ įsipareigojimų vykdymo užtikrinimo priemonių**“[41].

2013 m. lapkričio mėn. Komercijos departamentas informavo Europos Komisiją, kad „siekdamas padėti užtikrinti, kad bendrovės nesinaudotų melagingais teiginiais apie dalyvavimą „saugaus uosto“ sistemoje, Komercijos departamentas nustatys procedūrą, pagal kurią likus vienam mėnesiui iki sertifikato atnaujinimo termino bus susisiekiama su „saugaus uosto“ nariais ir paaiškinama, kokių žingsnių reikia imtis nebenorint atnaujinti savo sertifikato“. **Komercijos departamentas „perspės tokias bendroves**, kad iš jų privatumo taisyklių ir svetainių reikia ištrinti visą informaciją apie dalyvavimą „saugaus uosto“ sistemoje, įskaitant departamento „saugaus uosto“ sertifikato ženklą, **ir aiškiai joms praneš, kad to nepadarius joms bus pritaikytos Federalinės prekybos komisijos vykdymo užtikrinimo priemonės**“[42].

Siekiant kovoti su melagingais teiginiais apie dalyvavimą „saugaus uosto“ sistemoje, reikia nustatyti, kad autosertifikuotų bendrovių svetainėse turi būti pateikiama nuoroda į Komercijos departamento „saugaus uosto“ svetainę, kurioje skelbiamas visų šiuo metu sistemoje dalyvaujančių narių sąrašas. Tai leis Europos duomenų subjektams nedelsiant, be papildomos paieškos, patikrinti ar bendrovė tikrai yra „saugaus uosto“ sistemos narė. 2013 m. kovo mėn. Komercijos departamentas pradėjo to reikalauti iš bendrovių, tačiau šią priemonę reikėtų taikyti aktyviau.

Federalinės prekybos komisijos vykdomas nuolatinis stebėjimas ir nuoseklus realaus „saugaus uosto“ principų vykdymo užtikrinimas – kartu su pirmiau pažymėtomis Komercijos departamento priemonėmis – išlieka svarbiausias prioritetas užtikrinant sklandų ir veiksmingą sistemos veikimą. Ypač svarbu dažniau atlikti bendrovių **atitikties** „saugaus uosto“ principams ***ex officio* patikras ir tyrimus**. Taip pat reikėtų dar supaprastinti tvarką, pagal kurią Federalinei prekybos komisijai pateikiami skundai dėl pažeidimų.

5.2. ES duomenų apsaugos specialistų grupė

ES duomenų apsaugos specialistų grupė yra įstaiga, sukurta „Saugaus uosto“ sprendimo pagrindu. Ji įgaliota nagrinėti asmenų skundus dėl darbo santykiuose rinktų asmens duomenų, taip pat bylas, kuriose dalyvauja sertifikuotos bendrovės, jei jos yra pasirinkusios tokį būdą ginčams dėl „saugaus uosto“ spręsti (53 proc. visų bendrovių). Ją sudaro įvairių ES duomenų apsaugos institucijų atstovai.

Iki šiol grupė yra gavusi keturis skundus (du 2010 m. ir dar du 2013 m.). Du skundus 2010 m. ji perdavė nacionalinėms duomenų apsaugos institucijoms (Jungtinės Karalystės ir Šveicarijos). Kitus du ji dar nagrinėja. Mažas skundų skaičius gali būti susijęs su tuo, kad grupės įgaliojimai, kaip minėta pirmiau, iš esmės apima tik tam tikrų rūšių duomenis.

---

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

40 Federalinės prekybos komisijos pirmininkės Edith Ramirez raštas Komisijos pirmininko pavaduotojai Viviane Reding.

41 Federalinės prekybos komisijos pirmininkės Edith Ramirez raštas Komisijos pirmininko pavaduotojai Viviane Reding.

42 2013 m lapkričio 12 d. dokumentas „U.S.-EU Cooperation to Implement the Safe Harbor Framework“.

Ribotas grupės bylų nagrinėjimo krūvis iš dalies susijęs ir su tuo, kad trūksta žinių apie jos egzistavimą. Nuo 2004 m. Komisija siekė pagerinti šios įstaigos veiklos matomumą skelbdama atitinkamą informaciją savo svetainėje[43].

Kad bendradarbiavimas su ES duomenų apsaugos specialistų grupe būtų naudingesnis, JAV bendrovės, pasirinkusios bendradarbiauti su ja ir vykdyti jos sprendimus, susijusius su tam tikrų ar visų rūšių asmens duomenimis, kaip numatyta atitinkamuose jų sertifikatuose, savo privatumo taisyklėse turėtų aiškiai ir matomai nurodyti savo įsipareigojimą leisti Komercijos departamentui patikrinti šį aspektą. Kiekvienos ES duomenų apsaugos institucijos svetainėje turėtų būti sukurtas specialus „saugiam uostui“ skirtas puslapis, kad Europos bendrovės ir duomenų subjektai geriau susipažintų su „saugaus uosto“ sistema.

5.3. Vykdymo užtikrinimo gerinimas

Pirmiau įvardyti trūkumai skaidrumo ir vykdymo užtikrinimo srityse kelia Europos bendrovėms susirūpinimą, kad „saugaus uosto“ sistema gali pakenkti Europos bendrovių konkurencingumui. Jei Europos bendrovė konkuruoja su JAV bendrove, kuri priklauso „saugaus uosto“ sistemai, tačiau praktiškai jos principų netaiko, Europos bendrovės padėtis konkurencijos požiūriu yra prastesnė.

Be to, federalinės prekybos komisijos kompetencijai priklauso nesąžininga ar klaidinanti veikla „prekybos srityje arba daranti poveikį prekybai“. Federalinės prekybos komisijos įstatymo 5 skirsnyje nustatytos Federalinės prekybos komisijos kompetencijos spręsti nesąžiningos ar klaidinančios veiklos ar praktikos klausimus išimtys, be kita ko, **telekomunikacijų** srityje. Telekomunikacijų bendrovės, kurioms Federalinės prekybos komisijos vykdymo užtikrinimo veikla netaikoma, negali priklausyti „saugaus uosto“ sistemai. Tačiau išaugus technologijų ir paslaugų konvergencijai daug šių bendrovių tiesioginių konkurentų JAV IRT sektoriuje priklauso „saugaus uosto“ sistemai. Draudimas telekomunikacijų bendrovėms dalyvauti duomenų mainuose pagal „saugaus uosto“ sistemą kelia susirūpinimą kai kuriems Europos ryšio operatoriams. Europos telekomunikacijų tinklo operatorių asociacijos (ETNO) teigimu, „tai aiškiai prieštarauja pačiam svarbiausiam telekomunikacijų operatorių uždaviniui – skatinti vienodas konkurencijos sąlygas“[44].

6. „SAUGAUS UOSTO“ PRIVATUMO PRINCIPŲ STIPRINIMAS

6.1. Alternatyvus ginčų sprendimas

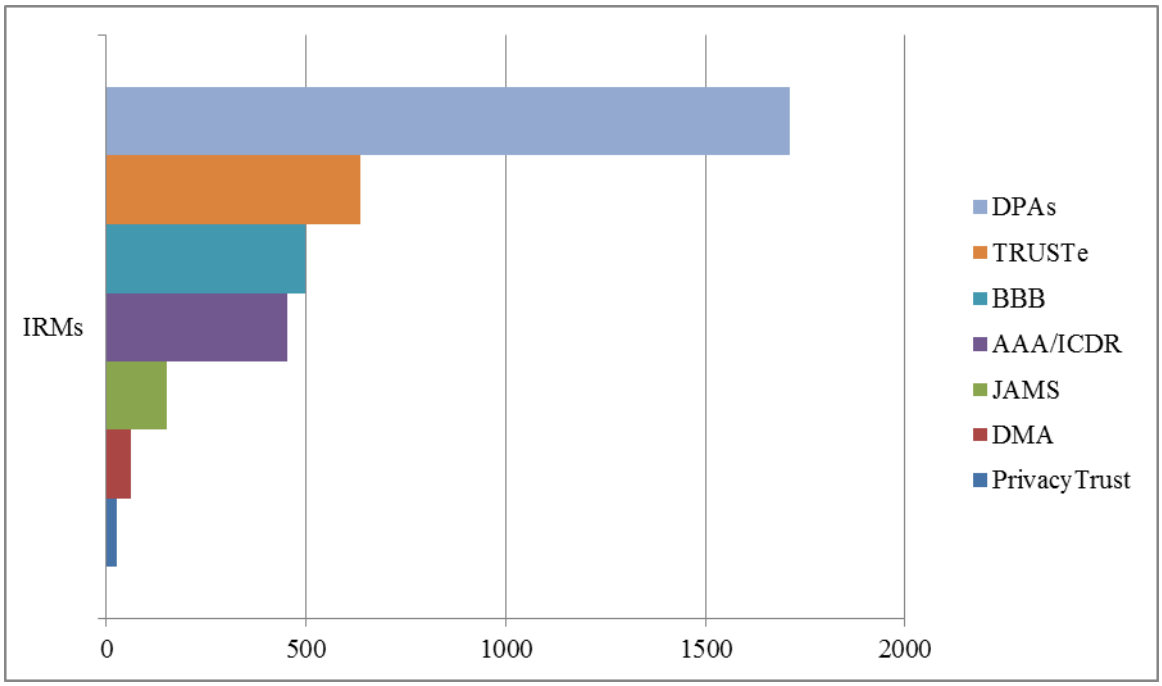
Vykdymo užtikrinimo principui įgyvendinti reikia sukurti „**prieinamas ir nebrangias procedūras**, pagal kurias būtų nagrinėjami asmenų skundai ir sprendžiami ginčai“. Tam „saugaus uosto“ sistemoje nustatyta alternatyvaus ginčų sprendimo sistema, kurioje

---

[43] Po 2004 m. ataskaitos Komisijos (Teisingumo generalinio direktorato) svetainėje paskelbtas informacinis pranešimas su klausimais ir atsakymais, kurio tikslas – gerinti piliečių informuotumą ir padėti jiems pateikti skundą, jei jie mano, kad jų asmens duomenys buvo tvarkomi pažeidžiant „saugaus uosto“ taisykles: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf .

[44] Standartinę skundo formą galima rasti adresu http://ec.europa.eu/justice/policies/privacy/docs/adequacy/ complaint_form_en.pdf. 2013 m. spalio 4 d. Komisijos tarnyboms pateiktoje savo nuomonėje („ETNO considerations“) ETNO taip pat kalba apie: 1) asmens duomenų apibrėžtį „saugaus uosto“ sistemoje; 2) nepakankamą „saugaus uosto“ sistemos stebėseną; 3) tai, kad „JAV bendrovės gali perduoti duomenis patirdamos kur kas mažiau apribojimų nei atitinkamos Europos bendrovės“, o tai „aiški Europos bendrovių diskriminacija, dėl kurios nukenčia jų konkurencingumas“. Pagal „saugaus uosto“ taisykles atskleisdamos informaciją trečiosios šalims organizacijos turi taikyti pranešimo ir pasirinkimo principus. Jei organizacija pageidauja perduoti informaciją agento funkcijas atliekančiai trečiajai šaliai, ji gali tai daryti tik įsitikinusi, kad ta trečioji šalis laikosi privatumo principų, Direktyvos ar kitų pakankamumo nuostatų arba sudaro su ta trečiąja šalimi rašytinę sutartį, kurioje reikalaujama, kad trečioji šalis suteiktų ne mažesnį privatumo užtikrinimo lygį, nei reikalaujama pagal taikytinus privatumo principus.

nepriklausoma trečioji šalis[45] padeda asmenims greitai spręsti ginčus. Trys pagrindinės ginčų sprendimo procedūrose dalyvaujančios įstaigos yra ES duomenų apsaugos specialistų grupė, BBB (*Better Business Bureaus*) ir „TRUSTe“.



Nuo 2004 m. alternatyvus ginčų sprendimas pasitelkiamas dažniau, o Komercijos departamentas pradėjo griežčiau stebėti JAV alternatyvaus ginčų sprendimo paslaugų teikėjus, kad jų pateikiama informacija apie apskundimo procedūrą būtų aiški, prieinama ir suprantama. Tačiau kadangi bylų nagrinėta labai nedaug, apie šių procedūrų veiksmingumą kalbėti dar anksti[46].

Nors Komercijos departamentas sėkmingai mažina alternatyvaus ginčų sprendimo mokesčius, du iš septynių didžiausių tokių paslaugų teikėjų asmenims pateikiant skundus ir toliau taiko mokesčius[47]. Į šiuos alternatyvaus ginčų sprendimo paslaugų teikėjus kreipiasi maždaug 20 proc. „saugaus uosto“ sistemos bendrovių. Šios bendrovės pasirinko alternatyvaus ginčo sprendimo paslaugų teikėją, kuris už asmens pateikiamą skundą ima mokestį. Tokia praktika neatitinka „saugaus uosto“ vykdymo užtikrinimo principo, pagal kurį asmenys turi teisę į „prieinamas ir nebrangias nepriklausomo ginčų sprendimo procedūras“. Europos Sąjungoje

45 ES direktyvoje 2013/11/ES dėl alternatyvaus vartotojų ginčų sprendimo pabrėžiama nepriklausomų, nešališkų, skaidrių, veiksmingų, greitų ir sąžiningų alternatyvaus ginčų sprendimo procedūrų svarba.

46 Pavyzdžiui, vienas didžiausių tokių paslaugų teikėjų ("TRUSTe") teigia 2010 m. gavęs 881 prašymus, tačiau tik trys iš jų buvę priimtini ir pagrįsti. Tais atvejais atitinkamoms bendrovėms nurodyta pakeisti privatumo taisykles ir informaciją svetainėse. 2011 m. gauti 879 skundai, vieno iš jų pagrindu bendrovei nurodyta pakeisti privatumo taisykles. Komercijos departamento pateiktais duomenimis, didžioji dauguma alternatyvaus ginčų sprendimo įstaigoms pateiktų skundų yra vartotojų skundai, pavyzdžiui, dėl to, kad pamiršus slaptažodį jie negalėjo iš interneto tarnybos gauti naujo. Atsižvelgdamas į Komisijos raginimus, Komercijos departamentas parengė naujus statistikos teikimo kriterijus, kuriuos turėtų naudoti alternatyvaus ginčų sprendimo įstaigos. Pagal juos paprasti prašymai atskiriami nuo skundų, be to, geriau išaiškinama, kokių tipų skundai gali būti teikiami. Tačiau šiuos naujus kriterijus reikėtų dar aptarti, užtikrinant, kad 2014 m. statistinius duomenis pateiktų visi alternatyvaus ginčų sprendimo paslaugų teikėjai, kad jie būtų palyginami ir suteiktų svarbios informacijos, leidžiančios įvertinti apskundimo sistemos veiksmingumą.

47 „International Centre for Dispute Resolution“ ir „American Arbitration Association“ taiko 200 USD, o JAMS – 250 USD skundo pateikimo mokestį. Komercijos departamentas pranešė Komisijai, kad kreipėsi į „American Arbitration Association“, asmenims brangiausią ginčų sprendimo paslaugų teikėją, kad šis parengtų specialią „saugaus uosto“ programą, pagal kurią vartotojų išlaidos būtų sumažintos nuo kelių tūkstančių JAV dolerių iki fiksuoto 200 USD mokesčio.

galimybė pasinaudoti teikiamomis ES duomenų apsaugos specialistų grupės nepriklausomo ginčų sprendimo paslaugomis visiems subjektams suteikiama nemokamai.

2013 m. lapkričio 12 d. Komercijos departamentas patvirtino, kad „toliau gins ES piliečių privatumą ir sieks, kad alternatyvaus ginčų sprendimo paslaugų teikėjai dar labiau sumažintų mokesčius“.

Kalbant apie sankcijas, ne visi alternatyvaus ginčų sprendimo paslaugų teikėjai turi reikiamas priemones, kad galėtų spręsti ginčus, kylančius dėl privatumo principų pažeidimų. Be to, kaip viena iš alternatyvaus ginčų sprendimo paslaugų teikėjų sankcijų ir priemonių nenumatytas paskelbimas apie priimtą sprendimą dėl pažeidimo.

Alternatyvaus ginčų sprendimo paslaugų teikėjai privalo perduoti Federalinei prekybos komisijai tas bylas, kuriose bendrovės nesilaiko alternatyvaus ginčų sprendimo keliu pasiekto susitarimo arba nesutinka su alternatyvaus ginčų sprendimo paslaugų teikėjo sprendimu; Federalinė prekybos komisija jas peržiūri, išnagrinėja ir prireikus imasi vykdymo užtikrinimo priemonių. Tačiau kol kas tokių atvejų, kai byla alternatyvaus ginčų sprendimo paslaugų teikėjo būtų perduota Federalinei prekybos komisijai, nepasitaikė[48].

Alternatyvaus ginčų sprendimo paslaugų teikėjai savo svetainėse skelbia bendrovių, kurios naudojasi jų paslaugomis, sąrašą. Taip vartotojai, kilus ginčui su bendrove, gali lengvai pasitikrinti, ar asmuo gali pateikti skundą nurodytam ginčų sprendimo paslaugų teikėjui. Pavyzdžiui, ginčų sprendimo paslaugų teikėja BBB pateikia sąrašą bendrovių, kurios yra pasirinkusios BBB ginčų sprendimo sistemą. Tačiau yra daug bendrovių, deklaruojančių, kad naudoja konkrečią ginčų sprendimo sistemą, nors jos nėra įtrauktos į šių paslaugų teikėjų sąrašus kaip jų ginčų sprendimo sistemų naudotojos[49].

Alternatyvaus ginčų sprendimo mechanizmai asmenims turi būti lengvai prieinami, nepriklausomi ir nebrangūs. Duomenų subjektui turi būti sudarytos sąlygos be didesnių sunkumų pateikti skundą. Visos alternatyvaus ginčų sprendimo įstaigos savo svetainėse turi skelbti statistiką apie išnagrinėtus skundus ir konkrečią informaciją apie priimtus sprendimus. Galiausiai, alternatyvaus ginčų sprendimo įstaigos turėtų būti stebimos siekiant užtikrinti, kad jų teikiama informacija apie procedūrą ir skundo pateikimo tvarką būtų aiški ir suprantama, ir kad ginčų sprendimas būtų veiksminga ir patikima priemonė, kuria pasiekiama rezultatų. Taip pat reikia pabrėžti, kad sprendimų apie nustatytus privatumo principų pažeidimus skelbimas turėtų būti privaloma alternatyvaus ginčų sprendimo įstaigų taikoma sankcija.

6.2. Perdavimas

Sparčiai didėjant duomenų srautams būtina užtikrinti nuolatinę asmens duomenų apsaugą visais duomenų tvarkymo etapais, visų pirma „saugaus uosto“ sistemos bendrovei perduodant duomenis **trečiajai šaliai tvarkymo tikslu**. Todėl gerinti vykdymo užtikrinimą reikia ne tik saugaus uosto narių, bet ir subrangovų atžvilgiu.

Pagal „saugaus uosto“ sistemą duomenys gali būti perduodami trečiosioms šalims, veikiančioms kaip agentai, jei bendrovė – „saugaus uosto“ narė – „įsitikina, kad ta trečioji šalis laikosi privatumo principų, Direktyvos ar kitų pakankamumo nuostatų, arba sudaro su ta trečiąja šalimi rašytinę sutartį, pagal kurią trečioji šalis privalo suteikti ne žemesnio lygio

[48] Žr. 11 DUK.

[49] Pavyzdžiai: Bendrovė „Amazon“ pranešė Komercijos departamentui naudojanti BBB ginčų sprendimo sistemą. Tačiau BBB ginčų sprendimo sistemos dalyvių sąraše „Amazon“ nėra. Ir priešingai – „Arsalon Technologies“ (www.arsalon.net), nuotolinės kompiuterijos paslaugų teikėja, į BBB paslaugų naudotojų sąrašą įtraukta, tačiau ši bendrovė šiuo metu nedalyvauja „saugaus uosto“ sistemoje (2013 m. spalio 1 d. duomenys). BBB, „TRUSTe“ ir kiti alternatyvaus ginčų sprendimo paslaugų teikėjai turėtų pašalinti arba pataisyti informaciją apie sertifikatus. Jiems turėtų būti taikomas reikalavimas sertifikuoti tik tas bendroves, kurios yra „saugaus uosto“ narės, kurio nesilaikant būtų taikomos vykdymo užtikrinimo priemonės.

privatumo apsaugą, nei reikalaujama pagal privatumo principus“[50]. Pavyzdžiui, Komercijos departamentas reikalauja, kad nuotolinės kompiuterijos paslaugų teikėjas sudarytų sutartį net ir tuomet, jei jis atitinka „saugaus uosto“ principus ir jau gauna duomenis tvarkymo tikslais[51]. Tačiau ši nuostata „Saugaus uosto“ sprendimo II priede suformuluota neaiškiai.

Kadangi pastaraisiais metais visų pirma nuotolinės kompiuterijos srityje yra pasitelkiama kur kas daugiau subrangovų, saugaus uosto bendrovė, sudarydama su subrangovu sutartį, turėtų pranešti apie tai Komercijos departamentui ir privalomai paskelbti savo privatumo užtikrinimo priemones[52].

Reikėtų aiškiau sureguliuoti tris pirmiau nurodytus aspektus – alternatyvaus ginčų sprendimo mechanizmą, griežtesnę priežiūrą ir tolesnį duomenų perdavimą.

7. PRIEIGA PRIE DUOMENŲ, PERDUOTŲ NAUDOJANTIS „SAUGAUS UOSTO“ SISTEMA

2013 m. paviešinta informacija apie JAV sekimo programų apimtį ir mastą sukėlė abejonių, ar tebėra užtikrinama asmens duomenų, teisėtai perduotų JAV pagal „saugaus uosto“ sistemą, apsauga. Pavyzdžiui, visos bendrovės, dalyvaujančios programoje PRISM, kuri suteikia JAV valdžios institucijoms prieigą prie visų JAV saugomų ar tvarkomų duomenų, turi „saugaus uosto“ sertifikatus. Taip „saugaus uosto“ sistema tapo informacijos kanalu, per kurį JAV žvalgybos tarnybos gali rinkti asmens duomenis, prieš tai tvarkytus ES.

„Saugaus uosto“ sprendimo I priede nustatyta, kad privatumo principų taikymas gali būti apribotas įstatymais, Vyriausybės aktu ar pagal teismų praktiką, jei tai pagrįsta dėl nacionalinio saugumo, viešojo intereso arba vykdymo užtikrinimo priežasčių. Pagrindinių teisių apribojimai galioja tik tuomet, kai yra aiškinami siaurai, yra išdėstyti visuomenei prieinamame teisės akte ir yra demokratinei visuomenei būtini ir proporcingi. „Saugaus uosto“ sprendime nustatyta, kad tokie apribojimai galimi „**tik tiek, kiek būtina**“ atsižvelgiant į nacionalinio saugumo, viešojo intereso arba vykdymo užtikrinimo reikalavimus[53]. Nors „Saugaus uosto“ sprendime numatyta, kad išimties tvarka duomenys gali būti tvarkomi nacionalinio saugumo, viešojo intereso arba vykdymo užtikrinimo tikslais, šio sprendimo priėmimo metu nebuvo galima numatyti, kad žvalgybos tarnybos tokiu dideliu mastu naudosis duomenimis, kurie JAV buvo perduodami vykdant komercinius sandorius.

Be to, dėl skaidrumo ir teisinio tikrumo priežasčių Komercijos departamentas turėtų pranešti Europos Komisijai apie bet kokius įstatymus ar Vyriausybės aktus, darančius poveikį

---

50 Žr. Komisijos sprendimą 2000/520/EB, p. 7 (Tolimesnis perdavimas).

51 Žr. “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

52 Šios pastabos taikytinos nuotolinės kompiuterijos paslaugų teikėjams, kurie nepriklauso „saugaus uosto“ sistemai. Konsultacijų įmonė „Galexia“ teigia, kad „gana didelė dalis nuotolinės kompiuterijos paslaugas teikiančių bendrovių priklauso „saugaus uosto“ sistemai ir laikosi jos principų. Nuotolinės kompiuterijos paslaugų teikėjai paprastai taiko kelių sluoksnių privatumo apsaugą, dažnai derindami tiesiogines sutartis su klientais ir bendrąsias privatumo apsaugos priemones. Neskaitant kelių svarbių išimčių, „saugaus uosto“ sistemai priklausantys nuotolinės kompiuterijos paslaugų teikėjai atitinka pagrindines nuostatas dėl ginčų sprendimo ir vykdymo užtikrinimo. Šiuo metu melagingus teiginius apie narystę „saugaus uosto“ sistemoje naudojančių bendrovių sąraše stambių nuotolinės kompiuterijos paslaugų teikėjų nėra“. („Galexia“ atstovo Chriso Connolly pranešimas LIBE komiteto posėdyje „Masinis ES piliečių sekimas elektroninėmis priemonėmis“).

53 Žr. „Saugaus uosto“ sprendimo I priedą: „Principų laikymasis gali būti ribojamas: a) tiek, kiek būtina atsižvelgiant į nacionalinio saugumo, visuomenės interesus arba teisės aktų vykdymo reikalavimus; b) įstatymais, Vyriausybės nutarimais arba precedentine teise, dėl kurių atsiranda prieštaringų įsipareigojimų ar aiškių įgaliojimų, jei vykdydama tokius įgaliojimus organizacija gali įrodyti, kad Principų nesilaikoma tik tiek, kiek tai būtina atsižvelgiant į organizacijos palaikomus viršesnius teisėtus interesus; arba c) jei valstybės narės įstatymai dėl Direktyvos numato išimtis ar leidžiančias nukrypti nuostatas ir jei tokios išimtys ar leidžiančias nukrypti nuostatos taikomos dėl panašių priežasčių. Siekdamos privatumo apsaugos stiprinimo, organizacijos turi stengtis visiškai ir skaidriai laikytis šių Principų, o jei ankstesnio sakinio b punkte nurodytos išimtys bus taikomos reguliariai, jos turi tai nurodyti savo privatumo taisyklėse. Dėl tos pačios priežasties pageidaujama, kad tais atvejais, kai pagal Principus ir (arba) JAV teisės aktus galima pasirinkti kelis variantus, organizacijos pasirinktų geriausią apsaugą suteikiantį variantą“.

„saugaus uosto“ privatumo principų laikymuisi[54]. Išimties taikymas turi būti griežtai kontroliuojamas – ji negali būti naudojama siekiant išvengti apsaugos, užtikrinamos **privatumo principais[55].** Tai yra, JAV valdžios institucijų turima plataus masto prieiga prie asmens duomenų, tvarkomų „saugaus uosto“ sertifikatus turinčių bendrovių, gali pakenkti elektroninės komunikacijos konfidencialumui.

7.1. Proporcingumas ir būtinumas

Kaip parodė *ad hoc* ES ir JAV duomenų apsaugos darbo grupės išvados, JAV teisėje yra daug teisės aktų, suteikiančių teisinį pagrindą plačiu mastu rinkti ir tvarkyti asmens duomenis, kurie saugomi ar tvarkomi JAV įsteigtose bendrovėse. Tai gali būti duomenys, kurie anksčiau buvo perduoti iš ES į JAV pagal „saugaus uosto“ sistemą, todėl kyla abejonių, ar tebėra užtikrinama atitiktis „saugaus uosto“ principams. Didžiulis šių programų mastas gali reikšti tai, kad JAV valdžios institucijos galės gauti ir toliau tvarkyti pagal „saugaus uosto“ sistemą perduotus duomenis, viršydamos tai, kas tikrai būtina ir proporcinga užtikrinant nacionalinį saugumą, kaip numatyta pagal „Saugaus uosto“ sprendime įtvirtintą išimtį.

7.2. Apribojimai ir galimybės apskųsti

Kaip parodė *ad hoc* ES ir JAV duomenų apsaugos darbo grupės išvados, JAV teisėje nustatytos apsaugos priemonės visų pirma taikytinos JAV piliečiams ar teisėtai šioje šalyje gyvenantiems asmenims. Be to, nei ES, nei JAV duomenų subjektams nesuteikiama galimybė prieiti prie duomenų, juos taisyti ar ištrinti arba pateikti administracinį ar teisminį skundą dėl jų asmens duomenų rinkimo ar tvarkymo pagal JAV sekimo programas.

7.3. Skaidrumas

Savo privatumo taisyklėse bendrovės paprastai nenurodo, kada taiko privatumo principų išimtis. Todėl asmenys ir bendrovės nežino, kas daroma su jų duomenimis. Tai ypač svarbu kalbant apie minėtų JAV sekimo programų naudojimą. Dėl to europiečiai, kurių duomenys pagal „saugaus uosto“ sistemą perduodami į JAV, gali iš tų bendrovių nesužinoti, kad prie jų duomenų gali būti suteikta tokia prieiga[56]. Tai kelia abejonių dėl atitikties „saugaus uosto“ skaidrumo principui. Jei tai nekelia grėsmės nacionaliniam saugumui, turi būti užtikrinamas kuo didesnis skaidrumas. Be jau taikomų reikalavimų bendrovėms savo privatumo taisyklėse nurodyti, kokiais atvejais privatumo principų taikymas gali būti ribojamas pagal įstatymus, Vyriausybės aktus ar teismų praktiką, bendrovės taip pat turėtų būti raginamos savo privatumo taisyklėse nurodyti, kokiais atvejais jos taiko privatumo principų išimtis vykdydamos nacionalinio saugumo, viešojo intereso ar vykdymo užtikrinimo reikalavimus.

8. IŠVADOS IR REKOMENDACIJOS

Nuo 2000 m., kai buvo priimtas „Saugaus uosto“ sprendimas, jis tapo asmens duomenų perdavimo tarp ES ir JAV pagrindu. Veiksmingos apsaugos perduodant asmens duomenis svarba išaugo dėl greitai didėjančių duomenų srautų, kas susiję su skaitmenine ekonomika ir

---

54 Nuomonė 4/2000 dėl saugaus uosto principų užtikrinamos apsaugos lygio, 2000 m. gegužės 16 d. priimta 29 straipsnio darbo grupės.

55 Nuomonė 4/2000 dėl saugaus uosto principų užtikrinamos apsaugos lygio, 2000 m. gegužės 16 d. priimta 29 straipsnio darbo grupės.

56 Palyginti skaidrią informaciją apie tai pateikia kai kurios „saugaus uosto“ sistemai priklausančios Europos bendrovės. Pavyzdžiui, saugaus uosto sistemos narė „Nokia“, vykdanti veiklą JAV, savo privatumo taisyklėse nurodo: *„Vykdydami privalomą įstatymą mes galime būti priversti atskleisti jūsų asmens duomenis tam tikroms valdžios institucijoms ar trečiosioms šalims, pavyzdžiui, vykdymo užtikrinimo institucijoms šalyse, kuriose mes ar trečiosios šalys mūsų vardu vykdo veiklą“.*

didžiuliais duomenų rinkimo, tvarkymo ir naudojimo pokyčiais. Tokios interneto bendrovės kaip „Google“, „Facebook“, „Microsoft“, „Apple“, „Yahoo“ turi šimtus milijonų klientų Europoje ir tvarkymo tikslais perduoda į JAV tokį kiekį asmens duomenų, kuris 2000 m. kuriant „saugaus uosto“ sistemą buvo neįsivaizduojamas.

Dėl skaidrumo trūkumo ir susitarimo vykdymo užtikrinimo vis dar yra konkrečių spręstinų problemų:

a) „saugaus uosto“ narių privatumo taisyklių skaidrumas,

b) veiksmingas privatumo principų taikymas JAV bendrovėse ir

c) vykdymo užtikrinimo veiksmingumas.

Be to, **plataus masto žvalgybos tarnybų prieiga prie duomenų, kurie buvo perduoti „saugaus uosto“ sertifikatus turinčioms JAV bendrovėms**, kelia rimtų abejonių, ar tebėra užtikrinama europiečių apsauga jų duomenis perduodant JAV.

Remdamasi tuo, kas išdėstyta, Komisija teikia tokias **rekomendacijas**:

Skaidrumas

1. *Autosertifikuotos bendrovės turėtų viešai skelbti savo privatumo taisykles*. Nepakanka, kad bendrovės pateikia Komercijos departamentui savo privatumo taisyklių aprašą. Privatumo taisyklės, surašytos aiškiai ir suprantama kalba, turėtų būti viešai skelbiamos bendrovių svetainėse.

2. *Reikia nustatyti, kad autosertifikuotų bendrovių svetainėse turi būti pateikiama nuoroda į Komercijos departamento „saugaus uosto“ svetainę, kurioje skelbiamas visų šiuo metu sistemoje dalyvaujančių narių sąrašas*. Tai leis Europos duomenų subjektams nedelsiant, be papildomos paieškos, patikrinti ar bendrovė tikrai yra „saugaus uosto“ sistemos narė. Tai padidintų sistemos patikimumą ir sumažintų tikimybę, kad bus naudojami melagingi teiginiai apie dalyvavimą „saugaus uosto“ sistemoje. 2013 m. kovo mėn. Komercijos departamentas pradėjo to reikalauti iš bendrovių, tačiau šią priemonę reikėtų taikyti aktyviau.

3. *Autosertifikuotos bendrovės turėtų skelbti privatumo taisykles, nustatytas jų sutartyse su subrangovais, pavyzdžiui, nuotolinės kompiuterijos paslaugų teikėjais*. Pagal „saugaus uosto“ sistemą sertifikuotos bendrovės gali perduoti duomenis trečiosioms šalims, kurios veikia kaip agentai, pavyzdžiui, nuotolinės kompiuterijos paslaugų teikėjams. Mūsų žiniomis, tokiu atveju Komercijos departamentas reikalauja, kad autosertifikuotos bendrovės sudarytų sutartį. Tačiau sudarydama tokią sutartį „saugaus uosto“ bendrovė taip pat turi pranešti apie ją Komercijos departamentui ir privalo viešai paskelbti apie taikomas privatumo užtikrinimo priemones.

4. *Komercijos departamento svetainėse turi būti aiškiai pažymėtos visos bendrovės, kurios šiuo metu nėra sistemos narės*. Komercijos departamento „saugaus uosto“ narių sąraše prie žymos „nedalyvaujanti“ (*not current*) turėtų būti pateikiamas aiškus perspėjimas, kad šiuo metu bendrovė neatitinka „saugaus uosto“ reikalavimų. Vis dėlto tokia nedalyvaujanti bendrovė privalo toliau taikyti „saugaus uosto“ reikalavimus duomenims, kurie buvo gauti jai dar veikiant „saugaus uosto“ sistemoje.

Teisių gynimas

5. *Bendrovių svetainėje skelbiamose privatumo taisyklėse turi būti pateikiama nuoroda į alternatyvaus ginčų sprendimo paslaugų teikėją ir (arba) ES duomenų apsaugos*

specialistų grupę. Taip Europos duomenų subjektai kilus problemai galės nedelsdami susisiekti su alternatyvaus ginčų sprendimo paslaugų teikėju arba ES duomenų apsaugos specialistų grupe. 2013 m. kovo mėn. Komercijos departamentas pradėjo iš bendrovių to reikalauti, tačiau šią priemonę reikėtų taikyti aktyviau.

6. *Alternatyvus ginčų sprendimas turėtų būti prieinamas ir nebrangus*. Kai kurios saugaus uosto sistemoje dirbančios alternatyvaus ginčų sprendimo įstaigos toliau taiko asmenims skundo nagrinėjimo mokesčius (200–250 USD), kurie atskiram vartotojui gali būti gana dideli. Palyginti, Europoje Duomenų apsaugos specialistų grupė ginčus, susijusius su „saugaus uosto“ sistema, nagrinėja nemokamai.

7. *Komercijos departamentas turėtų sistemingiau stebėti alternatyvaus ginčų sprendimo paslaugų teikėjų informacijos apie naudojamas procedūras ir ginčų nagrinėjimą skaidrumą ir prieinamumą.* Tuomet ginčų sprendimas būtų veiksminga ir patikima priemonė, leidžianti pasiekti rezultatų. Taip pat reikia pabrėžti, kad sprendimų apie nustatytus privatumo principų pažeidimus skelbimas turėtų būti privaloma alternatyvaus ginčų sprendimo įstaigų taikoma sankcija.

Vykdymo užtikrinimas

8. *Suteikus „saugaus uosto“ sertifikatą ar jį atnaujinus, dalis juos gavusių bendrovių turėtų būti* ex officio *patikrintos, įvertinant jų privatumo taisyklių veiksmingumą (ne tik atitikties formaliems reikalavimams požiūriu)*.

9. *Nustačius trūkumų, gavus skundą ar atlikus tyrimą po vienų metų atitinkamoje bendrovėje turėtų būti atliktas specialus tyrimas.*

10. *Jei kyla abejonių dėl bendrovės atitikties reikalavimams arba jei nagrinėjamas skundas Komercijos departamentas praneša apie tai kompetentingai ES duomenų apsaugos institucijai.*

11. *Toliau reikėtų tirti melagingus teiginius apie priklausymą „saugaus uosto“ sistemai.* Bendrovė, kuri savo svetainėje teigia, kad atitinka „saugaus uosto“ reikalavimus, tačiau kuri neįtraukta į Komercijos departamento sąrašą kaip dalyvaujanti sistemos narė, klaidina vartotojus ir piktnaudžiauja jų pasitikėjimu. Melagingi teiginiai kenkia visos sistemos patikimumui, todėl jie turi būti nedelsiant ištrinti iš bendrovių svetainių.

JAV bendrovių prieiga

12. *Autosertifikuotų bendrovių privatumo taisyklėse turėtų būti pateikiama informacija apie tai, kokiu mastu JAV teisė suteikia valdžios institucijoms galimybę rinkti ir tvarkyti pagal „saugaus uosto“ sistemą perduotus duomenis. Bendrovės turėtų būti raginamos savo privatumo taisyklėse nurodyti, kokiais atvejais jos taiko privatumo principų išimtis dėl nacionalinio saugumo, viešojo intereso ar vykdymo užtikrinimo priežasčių.*

13. *Svarbu, kad „Saugaus uosto“ sprendime numatyta nacionalinio saugumo išimtis būtų naudojama tik tiek, kiek būtina ir proporcinga.*