

II

(Ne teisėkūros procedūra priimami aktai)

SPRENDIMAI

KOMISIJOS ĮGYVENDINIMO SPRENDIMAS (ES) 2016/1250

2016 m. liepos 12 d.

dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB

(pranešta dokumentu Nr. C(2016) 4176)

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ⁽¹⁾, ypač į jos 25 straipsnio 6 dalį,

pasikonsultavusi su Europos duomenų apsaugos priežiūros pareigūnu ⁽²⁾,

1. ĮVADAS

- (1) Direktyvoje 95/46/EB nustatytos asmens duomenų perdavimo iš valstybių narių į trečiąsias šalis taisyklės, susijusios su tomis duomenų perdavimo operacijoms, kurioms taikoma minėta direktyva;
- (2) Direktyvos 95/46/EB 1 straipsnio ir preambulės 2 bei 10 konstatuojamųjų dalių paskirtis – užtikrinti ne tik veiksmingą ir visapusišką fizinių asmenų pagrindinių teisių ir laisvių, visų pirma pagrindinės teisės į privataus gyvenimo gerbimą tvarkant asmens duomenis, apsaugą, bet ir aukštą šių pagrindinių teisių ir laisvių apsaugos lygį ⁽³⁾;
- (3) Teisingumo Teismas savo praktikoje taip pat pabrėžia pagrindinės teisės į privataus gyvenimo gerbimą ir pagrindinės teisės į asmens duomenų apsaugą, kurios garantuojamos atitinkamai Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 straipsniuose, svarbą ⁽⁴⁾;
- (4) pagal Direktyvos 95/46/EB 25 straipsnio 1 dalį valstybės narės privalo imtis priemonių, kad asmens duomenys trečiajai šaliai būtų perduodami tik tuo atveju, jei ta trečioji šalis užtikrina tinkamą apsaugos lygį ir jei prieš perduodant duomenis yra laikomasi valstybės narės įstatymų, kuriais įgyvendinamos kitos Direktyvos nuostatos. Komisija, atsižvelgdama į trečiosios šalies vidaus teisę arba tarptautinius įsipareigojimus, kuriuos prisiėmė siekdama apsaugoti asmenų teises, gali nustatyti, kad ta trečioji šalis užtikrina tokį tinkamą apsaugos lygį. Tokiu atveju ir nepažeidžiant pagal kitas Direktyvos nuostatas priimtų nacionalinių nuostatų asmens duomenys iš valstybių narių gali būti perduodami nereikalaujant papildomų garantijų;

⁽¹⁾ OL L 281, 1995 11 23, p. 31.

⁽²⁾ Žr. 2016 m. gegužės 30 d. paskelbtą nuomonę Nr. 4/2016 dėl ES ir JAV sprendimo dėl „privatumo skydo“ tinkamumo projekto.

⁽³⁾ Byla C-362/14 Maximilian Schrems prieš Data Protection Commissioner (Schrems), ES:C:2015:650, 39 punktas.

⁽⁴⁾ Byla C-553/07 Rijkeboer, ES:C:2009:293, 47 punktas; sujungtos bylos C-293/12 ir C-594/12 Digital Rights Ireland ir kiti, ES:C:2014:238, 53 punktas; byla C-131/12 Google Spain ir Google, ES:C:2014:317, 53, 66 ir 74 punktai.

- (5) pagal Direktyvos 95/46/EB 25 straipsnio 2 dalį trečiosios šalies suteikiamas duomenų apsaugos lygis turėtų būti vertinamas atsižvelgiant į duomenų perdavimo operacijos arba tokios operacijos sekos aplinkybes, įskaitant toje trečiojoje šalyje galiojančias bendrąsias ir sektorines teisės taisykles;
- (6) Komisijos sprendime 2000/520/EB ⁽⁵⁾, atsižvelgiant į Direktyvos 95/46/EB 25 straipsnio 2 dalyje nustatytus tikslus, laikytasi nuomonės, kad „saugaus uosto privatumo principais“, išdėstytais JAV komercijos departamento parengtame „Dažnai užduodamų klausimų“ rekomendaciniame dokumente, užtikrinama tinkama iš Sąjungos į Jungtinėse Amerikos Valstijose įsisteigusias organizacijas perduodamų asmens duomenų apsauga;
- (7) savo 2013 m. lapkričio 27 d. priimtuose komunikatuose COM(2013) 846 final ⁽⁶⁾ ir COM(2013) 847 final ⁽⁷⁾ Komisija nusprendė, kad, atsižvelgiant į įvairius veiksnus, įkaitant proporcingai didėjančius duomenų srautus ir jų lemiamą reikšmę transatlantinei ekonomikai, sparčiai didėjančių JAV įmonių, dalyvaujančių „saugaus uosto“ schemoje, skaičių ir naują informaciją apie tam tikrų JAV žvalgybos programų mastą ir taikymo sritį, kuriai paaiškėjus suabejota JAV garantuojamu apsaugos lygiu, reikėtų peržiūrėti „saugaus uosto“ schemos pagrindą ir jį sustiprinti. Be to, Komisija nustatė daugybę „saugaus uosto“ schemos spragų ir trūkumų;
- (8) remdamasi Komisijos surinktais įrodymais, įskaitant informaciją, kurią dirbdama gavo ES ir JAV privatumo kontaktinė grupė ⁽⁸⁾, ir ES ir JAV ad hoc darbo grupėje ⁽⁹⁾ gauta informacija apie JAV žvalgybos programas, Komisija suformulavo 13 rekomendacijų dėl „saugaus uosto“ schemos peržiūros. Šiose rekomendacijose daugiausia dėmesio skirta esminių privatumo principų stiprinimui, JAV autosertifikuotų įmonių privatumo politikos skaidrumo didinimui, geresnei priežiūrai, stebėsenai ir vykdymo užtikrinimui atsižvelgiant į tai, kaip JAV valdžios institucijos laikosi šių principų, prieinamo ginčų sprendimo mechanizmo nustatymui ir poreikiui užtikrinti, kad Sprendime 2000/520/EB nustatyta nacionalinio saugumo išimtis būtų taikoma tik tiek, kiek tai iš tikrųjų yra griežtai būtina ir proporcinga;
- (9) 2015 m. spalio 6 d. byloje C-362/14 Maximilian Schrems prieš Data Protection Commissioner ⁽¹⁰⁾ priimtame sprendime Europos Sąjungos Teisingumo Teismas Sprendimą 2000/520/EB paskelbė negaliojančiu. Nenagrinėdamas „saugaus uosto“ privatumo principų, Teisingumo Teismas laikėsi nuomonės, kad Komisija tame sprendime nenurodė, jog Jungtinės Amerikos Valstijos iš tikrųjų „užtikrino“ tinkamą apsaugos lygį, atsižvelgdamos į savo vidaus teisę arba tarptautinius įsipareigojimus ⁽¹¹⁾;
- (10) šiuo atžvilgiu Teisingumo Teismas paaiškino, kad Direktyvos 95/46/EB 25 straipsnio 6 dalyje vartojama sąvoka „tinkamas apsaugos lygis“ nereiškia, kad apsaugos lygis turi būti identiškas tam, kuris garantuojamas pagal ES teisinę tvarką, ši sąvoka turi būti suprantama kaip reikalavimas, kad trečioji šalis užtikrintų tokį pagrindinių teisių ir laisvių apsaugos lygį, koks „iš esmės“ atitinka apsaugos lygį, garantuojamą Sąjungoje pagal Direktyvą 95/46/EB, siejant ją su Pagrindinių teisių chartija. NET jeigu priemonės, kuriomis šiuo atžvilgiu gali pasinaudoti ta trečioji šalis, gali skirtis nuo Sąjungos taikomų priemonių, tos priemonės vis tiek turi būti praktiškai veiksmingos ⁽¹²⁾;
- (11) Teisingumo Teismas kritiškai vertino tai, kad Sprendime 2000/520/EB pateikta per mažai išvadų dėl Jungtinėse Amerikos Valstijose galiojančių priimtų valstybinių taisyklių, kuriomis siekiama nustatyti bet kokias asmenų, kurių asmens duomenys perduoti iš Sąjungos į Jungtines Amerikos Valstijas, pagrindinių teisių apribojimų ribas, t. y. apribojimų, kuriuos šios šalies valstybiniai subjektai gali nustatyti siekdami teisėtų tikslų, pavyzdžiui, nacionalinio saugumo, ir dėl veiksmingos teisinės apsaugos nuo tokio pobūdžio apribojimų buvimo ⁽¹³⁾;

⁽⁵⁾ 2000 m. liepos 26 d. Komisijos sprendimas 2000/520/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 „Dažnai užduodamų klausimų“ (OL L 215, 2000 8 28, p. 7).

⁽⁶⁾ 2013 m. lapkričio 27 d. Komisijos komunikatas Europos Parlamentui ir Tarybai „Pasitikėjimo ES ir JAV duomenų mainais atkūrimas“, COM(2013) 846 final.

⁽⁷⁾ 2013 m. lapkričio 27 d. Komisijos komunikatas Europos Parlamentui ir Tarybai dėl „saugaus uosto“ nuostatų veikimo ES piliečių ir ES įsisteigusių bendrovių požiūriu, COM(2013) 847 final.

⁽⁸⁾ Žr., pvz., Europos Sąjungos Tarybos sudarytos ES ir JAV aukšto lygio ryšių palaikymo grupės dėl keitimosi informacija privatumo ir asmens duomenų apsaugos galutinę ataskaitą, 2008 m. gegužės 28 d. pranešimas 9831/08, skelbiamas adresu <http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf>.

⁽⁹⁾ Ataskaita apie ES ir JAV ad hoc duomenų apsaugos darbo grupės ES pirmininkų išvadas, 2013 m. lapkričio 27 d., skelbiama adresu <http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf>.

⁽¹⁰⁾ Žr. 3 išnašą.

⁽¹¹⁾ Schrems, 97 punktą.

⁽¹²⁾ Schrems, 73–74 punktai.

⁽¹³⁾ Schrems, 88–89 punktai.

- (12) 2014 m. Komisija pradėjo derybas su JAV valdžios institucijomis, kad aptartų „saugaus uosto“ schemos stiprinimą pagal Komunikatą COM(2013) 847 final pateiktas 13 rekomendacijų. Europos Sąjungos Teisingumo Teismui priėmus sprendimą Schrems byloje, šios derybos tapo intensyvesnės siekiant priimti galimai naują sprendimą dėl tinkamumo, kuris atitiktų Direktyvos 95/46/EB 25 straipsnio reikalavimus, kaip juos išaiškino Teisingumo Teismas. Prie šio sprendimo pridedami dokumentai, kurie taip pat bus skelbiami JAV federaliniame registre, yra šių diskusijų rezultatas. Privatumo principai (II priedas) kartu su įvairių JAV valdžios institucijų pateiktais oficialiais pareiškimais ir įsipareigojimais, kurie išdėstyti I, III–VII prieduose, sudaro „ES ir JAV privatumo skydą“;
- (13) Komisija atidžiai išnagrinėjo JAV teisę ir praktiką, įskaitant šiuos oficialius pareiškimus ir įsipareigojimus. Remdamasi 136–140 konstatuojamosiose dalyse išdėstytomis faktinėmis aplinkybėmis, Komisija daro išvadą, kad Jungtinės Amerikos Valstijos užtikrina tinkamą asmens duomenų, kurie iš Sąjungos perduodami Jungtinių Amerikos Valstijų autosertifikuotoms organizacijoms pagal ES ir JAV „privatumo skydą“, apsaugos lygį;

2. ES IR JAV „PRIVATUMO SKYDAS“

- (14) ES ir JAV „privatumo skydas“ yra pagrįstas autosertifikavimo sistema, kurią taikydamos JAV organizacijos įsipareigoja laikytis privatumo principų rinkinio – tai yra ES ir JAV „privatumo skydo“ sistemos principai, įskaitant papildomus principus (toliau kartu – privatumo principai), – kurių paskelbė JAV komercijos departamentas ir kuris pateiktas šio sprendimo II priede. Jis taikomas duomenų valdytojams ir tvarkytojams (atstovams), be to, nustatoma, kad duomenų tvarkytojai pagal sutartį turi būti įsipareigoję veikti tik pagal ES duomenų valdytojo instrukcijas ir padėti pastarajam bendrauti su asmenimis, kurie įgyvendina su privatumo principais susijusias teises ⁽¹⁴⁾;
- (15) nepažeidžiant prievolės laikytis pagal Direktyvą 95/46/EB priimtų nacionalinių nuostatų, dabartinio sprendimo poveikis yra susijęs su tuo, kad Sąjungos duomenų valdytojui ar tvarkytojui leidžiama perduoti duomenis JAV organizacijoms, kurios, taikydamos autosertifikavimo procedūrą, patvirtino Komercijos departamentui, kad paiso privatumo principų ir įsipareigoja jų laikytis. Privatumo principai taikomi tik tais atvejais, kai JAV organizacija tvarko asmens duomenis ir tiek, kiek tokių organizacijų tvarkomiems asmens duomenims netaikomi Sąjungos teisės aktai ⁽¹⁵⁾. „Privatumo skydas“ nedaro poveikio Sąjungos teisės aktų, kuriais reglamentuojamas asmens duomenų tvarkymas valstybėse narėse, taikymui ⁽¹⁶⁾;

⁽¹⁴⁾ Žr. II priedo III.10.a skirsnį. Pagal I.8.c skirsnyje pateiktą apibrėžtį ES duomenų valdytojas nustatys asmens duomenų tvarkymo tikslą ir priemones. Be to, sutartyje su atstovu turi būti aiškiai nurodyta, ar leidžiamas tolesnis duomenų perdavimas (žr. III.10.a.ii.2 skirsnį).

⁽¹⁵⁾ Ši taisyklė taip pat taikoma perduodant iš Sąjungos žmoniškųjų išteklių duomenis įdarbinimo tikslais. Privatumo principų nuostatose pabrėžiama, kad ES darbdavys neša „pagrindinę atsakomybę“ (žr. II priedo III.9.d.i skirsnį), tačiau kartu aiškiai nurodoma, kad jo elgesys bus vertinamas pagal Sąjungoje ir (arba) atitinkamoje valstybėje narėje taikytinas taisykles, o ne pagal privatumo principus. Žr. II priedo III.9.a.i., b.ii., c.i., d.i skirsnius.

⁽¹⁶⁾ Ši taisyklė taip pat taikoma asmens duomenų tvarkymui naudojantis Sąjungoje esančia įranga, kurią naudoja už Sąjungos ribų įsisteigusi organizacija (žr. Direktyvos 95/46/EB 4 straipsnio 1 dalies c punktą). Nuo 2018 m. gegužės 25 d. Bendrasis duomenų apsaugos reglamentas (BDAR) bus taikomas i) asmens duomenų tvarkymo veiklai, kurią vykdo Sąjungoje buveinę turintis duomenų valdytojas arba tvarkytojas (net jeigu duomenys tvarkomi Jungtinėse Amerikos Valstijose), arba ii) už Sąjungos ribų įsisteigusiam duomenų valdytojui arba tvarkytojui vykdomai Sąjungos duomenų subjekto asmens duomenų tvarkymo veiklai, kai tokia veikla yra susijusi su a) prekių ar paslaugų siūlymu (nesvarbu, ar reikalaujama, kad duomenų subjektas už prekes ar paslaugas susimokėtų) tokiems Sąjungos duomenų subjektams, arba b) jų elgesio stebėsenai tiek, kiek jis stebimas Sąjungoje. Žr. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) 3 straipsnio 1 ir 2 dalis (OL L 119, 2016 5 4, p. 1).

- (16) „privatumo skyde“ užtikrinama asmens duomenų apsauga galioja visiems ES duomenų subjektams ⁽¹⁷⁾, kurių asmens duomenys perduodami iš Sąjungos JAV organizacijoms, kurios, taikydamos autosertifikavimo procedūrą, patvirtino Komercijos departamentui, kad laikosi privatumo principų;
- (17) „privatumo skydo“ principai taikomi iš karto nuo jų patvirtinimo momento. Vienintelė išimtis yra susijusi su atskaitomybės už tolesnį duomenų perdavimą principu ir ji taikoma tuo atveju, kai organizacija, kuri patvirtina, kad laikosi „privatumo skydo“ principų, turi iš anksto užmegztus komercinius santykius su trečiosiomis šalimis. Atsižvelgiant į tai, kad šių komercinių santykių suderinimas su atskaitomybės už tolesnį duomenų perdavimą principo taisyklėmis gali užimti šiek tiek laiko, organizacija bus įpareigota tai padaryti kuo greičiau ir bet kuriuo atveju ne vėliau kaip per devynis mėnesius nuo autosertifikavimo (jeigu autosertifikavimas įvykdomas per pirmuosius du mėnesius nuo „privatumo skydo“ veikimo pradžios). Šiuo pereinamuoju laikotarpiu organizacija privalo taikyti pranešimo ir pasirinkimo principą (taip leisdamas ES duomenų subjektui atsisakyti duomenų tvarkymo) ir, tais atvejais, kai asmens duomenys perduodami trečiajai šaliai, kuri veikia kaip atstovas, privalo užtikrinti, kad ši šalis užtikrintų tokių patį arba didesnę apsaugos lygį, kurio reikalaujama pagal privatumo principus ⁽¹⁸⁾. Per šį pereinamąjį laikotarpį užtikrinama pagrįsta ir tinkama pusiausvyra tarp pagarbos pagrindinei teisei į duomenų apsaugą ir teisėtus įmonių poreikius turėti pakankamai laiko prisitaikyti prie naujos sistemos, kurioje taip pat reikia pakoreguoti savo komercinius santykius su trečiosiomis šalimis;
- (18) šią sistemą, atsižvelgdamas į JAV komercijos sekretoriaus pareiškimuose (šio sprendimo I priedas) išdėstytus įsipareigojimus, administruos ir stebės Komercijos departamentas. Šio sprendimo IV ir V prieduose pateikiami Federalinės prekybos komisijos (FPK) ir Transporto departamento pareiškimai dėl privatumo principų laikymosi užtikrinimo;

2.1. Privatumo principai

- (19) organizacijos, kurios pagal ES ir JAV „privatumo skydą“ taiko autosertifikavimo procedūrą, įsipareigoja laikytis privatumo principų ⁽¹⁹⁾;
- (20) pagal pranešimo principą organizacijos turi pareigą teikti informaciją duomenų subjektams apie įvairius aspektus, susijusius su jų asmens duomenų tvarkymu (pvz., renkamų duomenų rūšį, tvarkymo tikslą, teisę susipažinti su duomenimis ir pasirinkimo teisę, tolesnio perdavimo sąlygas ir atsakomybę). Taip pat taikomos papildomos apsaugos priemonės, visų pirma reikalaujama, kad organizacijos paskelbtų savo privatumo politiką (kurioje atspindėtų privatumo principai) ir pateiktų nuorodas į Komercijos departamento svetainę (įskaitant išsamesnę informaciją apie autosertifikavimą, duomenų subjektų teises ir teisių gynimo institucijas, į kurias galima kreiptis), 30 konstatuojamojoje dalyje nurodytą „privatumo skydo“ sąrašą ir atitinkamo alternatyvaus ginčų sprendimo paslaugų teikėjo svetainę;
- (21) pagal duomenų vientisumo ir tikslo ribojimo principą duomenys turi būti susiję tik su jų tvarkymo tikslu, būti patikimi atsižvelgiant į numatomą jų naudojimo paskirtį, tikslūs, išsamūs ir nauji. Organizacija neturi teisės tvarkyti asmens duomenų tokiais būdais, kurie neatitinka tikslo, dėl kurio jie buvo iš pradžių surinkti arba dėl kurio vėliau buvo gautas duomenų subjekto sutikimas juos naudoti. Organizacijos privalo užtikrinti, kad asmens duomenys būtų patikimi atsižvelgiant į jų numatomą naudojimą, tikslūs, išsamūs ir naujausi;

⁽¹⁷⁾ Šis sprendimas yra svarbus EEE. Europos ekonominės erdvės susitarime (EEE susitarimas) nustatyta, kad Europos Sąjungos vidaus rinkos taisyklės galioja trijose EEE valstybėse: Islandijoje, Lichtenšteine ir Norvegijoje. Sąjungos duomenų apsaugos teisės aktai, įskaitant Direktyvą 95/46/EB, patenka į EEE susitarimo taikymo sritį ir yra įtraukti į šio susitarimo XI priedą. EEE jungtinis komitetas turi priimti sprendimą dėl šio sprendimo įtraukimo į EEE susitarimą. Kai tik šis sprendimas bus pradėtas taikyti Islandijai, Lichtenšteinui ir Norvegijai, ES ir JAV „privatumo skydas“ taip pat galios šioms trimis šalims, o „privatumo skydo“ dokumentų rinkinyje pateiktos nuorodos į ES ir jos valstybės nares taip pat reiškia nuorodas į Islandiją, Lichtenšteiną ir Norvegiją.

⁽¹⁸⁾ Žr. II priedo III.6.e skirsnį.

⁽¹⁹⁾ Įdarbinimo tikslais surinktiems žmoniškųjų išteklių duomenims taikomos specialios taisyklės, kuriose nustatytos papildomos apsaugos priemonės, kaip reikalaujama pagal papildomą privatumo principą „žmoniškųjų išteklių duomenys“ (žr. II priedo III.9 skirsnį). Pavyzdžiui, darbdaviai turėtų atsižvelgti į darbuotojų privatumo pageidavimus ir apriboti prieigą prie asmens duomenų, nuasmenindami tam tikrus duomenis arba suteikdami duomenims kodus ar pseudonimus. Svarbiausia, reikalaujama, kad organizacijos, pradėdamos tvarkyti tokius duomenis, bendradarbiautų ir laikytųsi Sąjungos duomenų apsaugos institucijų konsultacijų.

- (22) jeigu naujas (pakeistas) tikslas yra iš esmės skirtingas, tačiau vis tiek suderinamas su pradiniu tikslu, pasirinkimo principu duomenų subjektams suteikiama teisė prieštarauti (atsisakyti duomenų tvarkymo). Pasirinkimo principas nėra viršesnis už aiškų draudimą tvarkyti duomenis nesuderinamais tikslais⁽²⁰⁾. Pagal specialias taisykles duomenų naudojimo tiesioginės rinkodaros tikslais paprastai leidžiama atsisakyti „bet kuriuo metu“⁽²¹⁾. Jeigu organizacijos tvarko neskelbtinus duomenis, jos iš esmės privalo gauti teigiamą ir aiškų duomenų subjekto sutikimą (pritarimas);
- (23) vis dėlto pagal duomenų vientisumo ir tikslo ribojimo principą asmeninė informacija gali būti saugoma forma, iš kurios galima nustatyti tapatybę arba kuri sudarytų sąlygas nustatyti asmens tapatybę (todėl tai reikštų asmens duomenų saugojimą), tik tiek, kiek tai yra reikalinga siekiant tikslo (-ų), kuriuo (-iais) jie buvo iš pradžių surinkti arba kuriais juos vėliau leista rinkti. Ši pareiga neužkerta kelio „privatumo skydo“ organizacijoms toliau tvarkyti asmeninę informaciją ilgesniais terminais, tačiau tik tiek, kiek toks tvarkymas yra pagrįstas atsižvelgiant į vieną iš šių konkrečių tikslų: archyavimas dėl viešojo intereso, žurnalistika, literatūra ir menas, moksliniai ir istoriniai tyrimai ir statistinė analizė. Ilgiau asmens duomenis kuriuo nors iš nurodytų tikslų galima saugoti taikant privatumo principų nuostatose nustatytas apsaugos priemones;
- (24) pagal saugumo principą organizacijos, kurios kuria, tvarko, naudoja arba platina asmens duomenis, privalo, atsižvelgdamos į riziką, susijusią su duomenų tvarkymu, ir duomenų pobūdį, imtis „pagrįstų ir tinkamų“ saugumo priemonių. Jeigu vykdomas pagalbinis duomenų tvarkymas, organizacijos privalo sudaryti sutartį su pagalbinio duomenų tvarkytoju, kuria garantuojamas toks pat apsaugos lygis, koks užtikrinamas pagal privatumo principus, ir imtis priemonių, kad toks susitarimas būtų tinkamai vykdomas;
- (25) pagal prieigos prie duomenų principą⁽²²⁾ duomenų subjektai turi teisę, nenurodydami motyvų ir tik už pagrįsto dydžio mokestį, gauti iš organizacijos patvirtinimą, ar ji tvarko su jais susijusius asmens duomenis, ir per pagrįstą terminą gauti tokius duomenis, jei jie yra tvarkomi. Ši teisė gali būti ribojama tik išimtinėmis aplinkybėmis; bet koks teisės susipažinti su duomenimis atsakymas arba apribojimas turi būti būtinas ir tinkamai pagrįstas ir šiuo atveju organizacija turi pareigą įrodyti, kad šie reikalavimai yra įvykdyti. Duomenų subjektams turi būti suteikiama galimybė taisyti, keisti arba ištrinti asmens duomenis, jei jie yra netikslūs ar buvo tvarkomi pažeidžiant privatumo principus; Srityse, kuriose labiausiai tikėtina, kad bendrovės naudos automatizuoto asmens duomenų tvarkymo priemones, kad priimtų asmeniui poveikį darančius sprendimus (pvz., kredito paskolos, hipotekos garantijos, įsidarbinimas), galioja JAV teisėje nustatytos konkrečios apsaugos nuo neigiamų sprendimų priemonės⁽²³⁾. Šiuose teisės aktuose paprastai nustatyta, kad asmenys turi teisę būti informuoti apie konkrečias priimto sprendimo priežastis (pvz., atmeta kredito paraišką), kad galėtų ginčyti neišsamią arba netikslią informaciją (taip pat remtis neteisėtumo aplinkybėmis) ir siekti apginti savo teises. Šiose taisyklėse nustatytos apsaugos priemonės taikomos gana ribotai, atsižvelgiant į atvejus, kai automatizuotus sprendimus priima pati „privatumo skydo“ organizacija⁽²⁴⁾. Vis dėlto, atsižvelgiant į dažnėjantį automatizuotą duomenų tvarkymą (įskaitant profilių sudarymą), kuris yra asmenims poveikį turinčių sprendimų priėmimo modernios skaitmeninės ekonomikos sąlygomis pagrindas, tai yra sritis, kurią reikia atidžiai stebėti. Siekiant palengvinti šią stebėseną, su JAV valdžios institucijomis sutarta, kad dialogas automatizuoto sprendimo priėmimo klausimais, įskaitant informavimą apie ES ir JAV požiūrių šiuo atžvilgiu panašumus ir skirtumus, bus įtrauktas į pirmąją metinę peržiūrą ir prireikus į vėlesnes peržiūras;

⁽²⁰⁾ Ši taisyklė taikoma visiems pagal „privatumo skydą“ perduodamiems duomenims, įskaitant tuos atvejus, kai šie duomenys yra susiję su įdarbinimo metu surinktais duomenimis. Nors JAV autosertifikuota organizacija iš esmės gali naudoti žmogiškųjų išteklių duomenis kitais, su įdarbinimu nesusijusiais tikslais (pvz., tam tikrų rinkodaros pranešimų siuntimo tikslais), ji privalo paisyti draudimo tvarkyti duomenis nesuderinamais tikslais, be to, ji gali tai daryti tik laikydamasi *pranešimo* ir *pasirinkimo* principų. Draudimas JAV organizacijai imtis kokių nors baudžiamųjų veiksmų prieš darbuotoją, kuris pasinaudoja tokia pasirinkimo teise, įskaitant bet koki įsidarbinimo galimybių ribojimą, padės užtikrinti, kad, nepaisant subordinacijos santykio ir būdingos priklausomybės, darbuotojas nejaus spaudimo, todėl sprendimą galės priimti visiškai laisvai.

⁽²¹⁾ Žr. II priedo III.1.2 skirsnį.

⁽²²⁾ Taip pat žr. papildomą prieigos prie duomenų principą (II priedo III.8 skirsnis).

⁽²³⁾ Žr., pvz., Vienodų galimybių gauti kreditą aktą (ECOA, JAV kodekso 15 antraštinės dalies 1691 ir kiti straipsniai), Sąžiningos kredito ataskaitos aktą (FCRA, JAV kodekso 15 antraštinės dalies 1681 ir kiti straipsniai.) arba Sąžiningos būsto paskolos aktą (FHA, JAV kodekso 42 antraštinės dalies 3601 ir kiti straipsniai).

⁽²⁴⁾ Tais atvejais, kai perduodami ES surinkti asmens duomenys, sutartiniai santykiai su asmeniu (klientu) dažniausiai bus pagrįsti santykiais su ES duomenų valdytoju, kuris turi laikytis ES duomenų apsaugos taisyklių (todėl būtent jis paprastai priims bet koki sprendimą, pagrįstą automatizuotu duomenų tvarkymu). Tai apima scenarijus, kai duomenis tvarko „privatumo skydo“ organizacija, kuri ES duomenų valdytojo vardu veikia kaip atstovas.

- (26) pagal teisių gynimo, vykdymo ir atsakomybės principą ⁽²⁵⁾ dalyvaujančios organizacijos privalo sukurti patikimus mechanizmus, kuriais būtų užtikrinama atitiktis kitiems privatumo principams ir ES duomenų subjektų, kurių asmens duomenys buvo tvarkomi nesilaikant reikalavimų, teisė gintis, įskaitant veiksmingas teisių gynimo priemonės. Organizacija, savanoriškai nusprendusi atlikti autosertifikavimą ⁽²⁶⁾ pagal ES ir JAV „privatumo skydą“, privalo veiksmingai laikytis privatumo principų. Norėdama, kad jai toliau būtų leidžiama pagal „privatumo skydą“ gauti asmens duomenis iš Sąjungos, tokia organizacija privalo kasmet pakartotinai patvirtinti savo dalyvavimą sistemoje. Be to, organizacijos privalo imtis priemonių, kad patikrintų ⁽²⁷⁾, ar jų paskelbta privatumo politika atitinka privatumo principus ir ar jų iš tikrųjų laikomasi. Tai galima padaryti naudojant savikontrolės sistemą, apimančią vidaus procedūras, kuriomis užtikrinama, kad darbuotojai būtų apmokyti organizacijos privatumo politikos įgyvendinimo klausimais ir kad atitiktis būtų periodiškai tikrinama objektyviu būdu arba taikant išorės atitikties peržiūros metodus, pvz., auditą ar atsitiktines patikras. Be to, organizacija privalo nustatyti veiksmingą teisių gynimo instituciją, į kurią būtų galima kreiptis su bet koku skundu (šiuo atžvilgiu taip pat žr. 43 konstatuojamąją dalį), ir patekti į FPK, Transporto departamento arba kitos valstybinės įstaigos, kuri veiksmingai užtikrins privatumo principų laikymąsi, tyrimų ir vykdymo įgaliojimų taikymo sritį;
- (27) specialios taisyklės taikomos vadinamiesiems „tolesniems perdavimams“, tai yra organizacijos trečiajai šaliai, kuri veikia kaip duomenų valdytojas arba tvarkytojas, perduodami asmens duomenys, nepaisant to, ar pastaroji yra Jungtinėse Amerikos Valstijose, ar už Jungtinių Amerikos Valstijų (ir Sąjungos) esančioje trečiojoje šalyje. Šių taisyklių paskirtis – užtikrinti, kad apsaugos priemonės, kurios užtikrinamos garantuojant ES duomenų subjektų asmens duomenų apsaugą, nebus ribojamos ir kad trečiosios šalys negalės jų apeiti. Tai yra ypač svarbu tais atvejais, kai naudojamos sudėtingesnės duomenų tvarkymo grandinės, kurios paprastai yra būdingos šiuolaikinei skaitmeninei ekonomikai;
- (28) pagal atsakomybės už tolesnį duomenų perdavimą principą ⁽²⁸⁾ asmens duomenys toliau gali būti perduodami i) tik ribotais ir konkrečiais tikslais, ii) pagal sutartį (arba panašų įmonių grupėje sudarytą susitarimą ⁽²⁹⁾) ir iii) tik jeigu ta sutartimi užtikrinamas apsaugos lygis atitinka pagal privatumo principus garantuojamą apsaugą, įskaitant reikalavimą, kad privatumo principų taikymas gali būti ribojamas tik tiek, kiek tai būtina siekiant nacionalinio saugumo, teisėsaugos ir kitų viešojo intereso tikslų ⁽³⁰⁾. Šią nuostatą reikėtų vertinti atsižvelgiant į pranešimo principą, ir pasirinkimo principą, jeigu duomenys perduodami trečiajai šaliai duomenų valdytojui ⁽³¹⁾, pagal kurį duomenų subjektus būtina informuoti (be kita ko) apie bet kurios trečiosios šalies gavėjos rūšį/tapatybę, tolesnio duomenų perdavimo tikslą ir siūlomą pasirinkimą arba galimybę atsisakyti (atsisakymas) arba, jeigu perduodami konfidencialūs duomenys, duoti „teigiamą aiškų sutikimą“ (pritarimas) tolesniam duomenų perdavimui. Atsižvelgiant į duomenų vientisumo ir tikslo ribojimo principą, pareiga užtikrinti tokių patį apsaugos lygį, kuris garantuojamas pagal privatumo principus, reiškia, kad trečioji šalis jai perduotą asmeninę informaciją gali tvarkyti tik tokiais tikslais, kurie yra suderinami su tokios informacijos pradinio rinkimo tikslu arba tikslu, kuriuo asmuo leido rinkti informaciją apie save;
- (29) pareiga užtikrinti tokių patį apsaugos lygį, kurio reikalaujama pagal privatumo principus, taikoma bet kuriai ir visoms trečiosioms šalims, tvarkančioms tokiu būdu perduotus duomenis, nepaisant jų buvimo vietos (JAV ar kitoje trečiojoje šalyje), taip pat kai pradinė trečioji šalis gavėja pati tuos duomenis perduoda kitai trečiajai šaliai gavėjai, pvz., papildomo tvarkymo tikslais. Visais atvejais sutartyje su trečiaja šalimi gavėja būtina nustatyti, kad pastaroji informuos „privatumo skydo“ organizaciją, jei nustatys, kad ji nebegali laikytis šios pareigos. Nustačiusi, kad nebegali toliau laikytis minėtos pareigos, trečioji šalis nutrauks duomenų tvarkymą arba imsis kitų pagrįstų ir

⁽²⁵⁾ Taip pat žr. papildomą principą dėl ginčų sprendimo ir reikalavimų užtikrinimo (žr. II priedo III.11 skirsnį).

⁽²⁶⁾ Taip pat žr. papildomą autosertifikavimo principą (II priedo III.6 skirsnis).

⁽²⁷⁾ Taip pat žr. papildomą patikrinimo principą (II priedo III.7 skirsnis).

⁽²⁸⁾ Taip pat žr. papildomą principą dėl privalomų tolesnio duomenų perdavimo sutarčių (žr. II priedo III.10 skirsnį).

⁽²⁹⁾ Žr. papildomą principą dėl privalomų tolesnio duomenų perdavimo sutarčių (žr. II priedo III.10.b skirsnį). Nors pagal šį principą duomenų perdavimą taip pat galima grįsti nesutartinėmis priemonėmis (pvz., reikalavimų laikymasis grupės viduje ir kontrolės priemonės), tekste aiškiai nurodoma, kad šiomis priemonėmis visada būtina „užtikrinti nuolatinę asmeninės informacijos apsaugą pagal privatumo principus“. Be to, atsižvelgiant į tai, kad JAV autosertifikuota organizacija vis tiek liks atsakinga už privatumo principų laikymąsi, ji bus ypač suinteresuota naudoti priemones, kurių praktiniu veiksmingumu neabejojama.

⁽³⁰⁾ Žr. II priedo I.5 skirsnį.

⁽³¹⁾ Asmenys neturės jokių galimybių atsisakyti duomenų tvarkymo, jeigu jų asmens duomenys perduodami trečiajai šaliai, kuri veikia kaip atstovas vykdydama užduotį (-is) JAV organizacijos vardu ir jai vadovaujant. Tačiau šiuo atveju reikalaujama, kad su atstovu būtų sudaryta sutartis ir JAV organizacija, pasinaudodama įgaliojimais duoti instrukcijas, turės pareigą garantuoti pagal privatumo principus užtikrinamas apsaugos priemones.

tinkamų veiksmų, kad ištaisytų susidariusią situaciją ⁽³²⁾. Jeigu (papildomo) duomenų tvarkymo grandinėje kyla atitikties problemų, „privatumo skydo“ organizacija, kuri veikia kaip asmens duomenų valdytoja, turės įrodyti, kad ji neatsako už įvykį, dėl kurio atsirado žala, arba dėl kitų priežasčių nėra atsakinga, kaip nustatyta teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principo nuostatose. Jeigu duomenys perduodami toliau trečiosios šalies atstovui, taikomos papildomos apsaugos priemonės ⁽³³⁾;

2.2. ES ir JAV „privatumo skydo“ skaidrumas, administravimas ir priežiūra

- (30) ES ir JAV „privatumo skyde“ numatyti priežiūros ir reikalavimų užtikrinimo mechanizmai, kurių paskirtis – patikrinti ir užtikrinti, kad JAV autosertifikuotos bendrovės laikytųsi privatumo principų ir kad būtų reaguojama į bet kokių reikalavimų nesilaikymą. Šie mechanizmai apibūdinti privatumo principų nuostatose (II priedas) ir Komercijos departamento (I priedas), FPK (IV priedas) ir Transporto departamento (V priedas) prisiimtuose įsipareigojimuose;
- (31) siekdamas užtikrinti tinkamą ES ir JAV „privatumo skydo“ veikimą, suinteresuotosios šalys, pvz., duomenų subjektai, duomenų eksportuotojai ir nacionalinės duomenų apsaugos institucijos (DAI), privalo sugebėti nustatyti privatumo principų besilaikančias organizacijas. Šiuo tikslu Komercijos departamentas įsipareigojo naudoti ir pateikti visuomenei sąrašą organizacijų, kurios per autosertifikavimo procedūrą patvirtino besilaikančios privatumo principų ir kurios priklauso bent vienos iš šio sprendimo I ir II prieduose išvardytų teisėsaugos institucijų („privatumo skydo“ sąrašas) jurisdikcijai ⁽³⁴⁾. Komercijos departamentas sąrašą atnaujins atsižvelgdamas į organizacijos metinius pareiškimus dėl pakartotinio sertifikavimo ir visais atvejais – kai organizacija nustos dalyvauti ES ir JAV „privatumo skydo“ sistemoje arba bus iš jos pašalinta. Komercijos departamentas taip pat tvarkys ir viešai skelbs patikimą organizacijų, kurios buvo išbrauktos iš sąrašo, registrą ir kaskart nurodys tokio pašalinimo priežastį. Galiausiai šis departamentas pateiks nuorodą į FPK svetainėje skelbiamą FPK vykdymo bylą, susijusią su „privatumo skydu“, sąrašą;
- (32) Komercijos departamentas „privatumo skydo“ sąrašą ir pareiškimus dėl pakartotinio sertifikavimo viešai skelbs specialioje svetainėje. Autosertifikuotos organizacijos privalo nurodyti Departamento svetainės adresą, kurioje galima rasti „privatumo skydo“ sąrašą. Be to, jeigu organizacijos privatumo politika skelbiama internete, joje būtina pateikti saitą į „privatumo skydo“ svetainę, taip pat saitą į nepriklausomos teisių gynimo institucijos arba skundo pateikimo formos, kuria galima pasinaudoti tiriant neišspręstus skundus, svetainę; Komercijos departamentas, atsižvelgdamas į organizacijos sertifikavimo ir pakartotinio sertifikavimo sistemoje procesą, sistemaiškai tikrins, ar organizacijos privatumo politika atitinka privatumo principus;
- (33) nuolat privatumo principų nesilaikančios organizacijos bus išbraukiamos iš „privatumo skydo“ sąrašo ir privalės grąžinti arba ištrinti pagal ES ir JAV „privatumo skydą“ gautus asmens duomenis. Kitais išbraukimo iš sąrašo atvejais, pvz., savanoriškas atsisakymas dalyvauti „privatumo skydo“ sistemoje arba pakartotinio sertifikavimo nebuvimas, organizacija gali išsaugoti tokius duomenis, jei ji kasmet Komercijos departamentui patvirtina savo įsipareigojimą toliau taikyti privatumo principus arba kitomis teisėtomis priemonėmis užtikrina tinkamą asmens duomenų apsaugą (pvz., sudarydama sutartį, kurioje visapusiškai laikomasi Komisijos patvirtintoms standartinėms sutarties sąlygoms taikomų reikalavimų). Šiuo atveju organizacija turi nurodyti savo kontaktinį centrą, kuris bus atsakingas už visų su „privatumo skydu“ susijusių klausimų sprendimą;
- (34) Komercijos departamentas stebės organizacijas, kurios iš ES ir JAV „privatumo skydo“ pasitraukė savanoriškai arba pasibaigus jų sertifikavimo galiojimo terminui, kad patikrintų, ar jos grąžino, ištrynė ar toliau saugo ⁽³⁵⁾ anksčiau, dalyvaujant sistemoje, gautus asmens duomenis. Jeigu organizacijos toliau saugo duomenis, šiems

⁽³²⁾ Situacija gali skirtis priklausomai nuo to, ar trečioji šalis yra duomenų valdytoja ar duomenų tvarkytoja (atstovas). Pirmuoju atveju sutartyje su trečiąja šalimi būtina nustatyti, kad ji nustoja tvarkyti duomenis arba imasi kitų pagrindų ir tinkamų priemonių susidariusiai padėčiai ištaisyti. Antruoju atveju šių priemonių turi imtis „privatumo skydo“ organizacija, kaip duomenų tvarkymo veiklą kontroliuojantis subjektas, kurio instrukcijomis vadovaujasi atstovas.

⁽³³⁾ Tokiu atveju JAV organizacija taip pat privalo imtis pagrindų ir tinkamų priemonių, siekdamas i) užtikrinti, kad atstovas veiksmingai tvarkytų asmeninę informaciją, kuri buvo perduota su organizacijos įsipareigojimais pagal privatumo principus suderinamu būdu, ir ii) sustabdyti neteisėtą duomenų tvarkymą, apie kurį pranešta, ir ištaisyti susidariusią padėtį.

⁽³⁴⁾ Informaciją apie „privatumo skydo“ sąrašo tvarkymą galima rasti I ir II prieduose (I.3 skirsnis, I.4 ir III.6.d skirsniai ir III.11.g skirsnis).

⁽³⁵⁾ Žr., pvz., II priedo I.3 skirsnį, III.6.f skirsnį ir III.11.g skirsnį.

asmens duomenims jos privalo toliau taikyti privatumo principus. Komercijos departamentas, pašalinęs organizacijas iš sistemos dėl to, kad jos nuolat nesilaikė privatumo principų, užtikrina, kad tos organizacijos grąžintų arba ištrintų dalyvavimo sistemoje metu gautus asmens duomenis;

- (35) jeigu organizacija dėl kurios nors priežasties nustoja dalyvauti ES ir JAV „privatumo skyde“, ji privalo panaikinti visus viešus pareiškimus, iš kurių galima numanyti, kad ji toliau dalyvauja ES ir JAV „privatumo skyde“ arba turi teisę naudotis šios sistemos privalumais, visų pirma tai pasakytina apie visas tokios organizacijos privatumo politikoje pateiktas nuorodas į ES ir JAV „privatumo skydą“. Komercijos departamentas ieškos ir nustatys klaidingus pareiškimus dėl dalyvavimo sistemoje, įskaitant buvusių narių pareiškimus ⁽³⁶⁾. Sankcijas už bet koki visuomenės klaidinimą dėl organizacijos išpareigojimo laikytis privatumo principų pateikiant klaidingus pareiškimus arba taikant klaidinančią praktiką skiria FPK, Transporto departamentas arba kitos atitinkamos JAV teisėsaugos institucijos; už Komercijos departamentui pateiktą klaidingą informaciją baudžiama pagal Melagingų parodymų aktą (JAV kodekso 18 antraštinės dalies 1001 straipsnis) ⁽³⁷⁾;
- (36) Komercijos departamentas ex officio stebi visus klaidingus pareiškimus, susijusius su dalyvavimu „privatumo skydo“ sistemoje arba netinkamu „privatumo skydo“ sertifikavimo ženklo naudojimu, o DAI gali pranešti apie organizacijas tam specialiam Departamento kontaktiniam centrui, kad būtų atlikta peržiūra. Jeigu organizacija nustojo dalyvauti ES ir JAV „privatumo skyde“, neįvykdo pakartotinio sertifikavimo arba išbraukiama iš „privatumo skydo“ sąrašo, Komercijos departamentas nuolat tikrina, ar ši organizacija iš savo paskelbtos privatumo politikos ištrynė visas nuorodas į „privatumo skydą“, iš kurių galima numanyti, kad ji toliau laikosi privatumo principų, o jeigu ji toliau nurodo klaidingus teiginius, Departamentas gali perduoti klausimą FPK, Transporto departamentui arba kitai kompetentingai institucijai, kad ji prireikus imtųsi vykdymo veiksmų. Komercijos departamentas organizacijoms, kurių autosertifikavimo terminas pasibaigė arba kurios savanoriškai nustojo dalyvauti ES ir JAV „privatumo skyde“, nusiunčia klausimyną, kad jos nustatytų, ar grąžins ar ištrins asmens duomenis, kuriuos gavo dalyvaudamos ES ir JAV „privatumo skyde“, ar toliau tokiems duomenims taikys privatumo principus, o jeigu asmens duomenys turi būti saugomi, – nustatyti asmenį, kuris organizacijoje bus atsakingas už visų su „privatumo skydu“ susijusių klausimų sprendimą;
- (37) Komercijos departamentas nuolat ex officio atliks atitikties peržiūras ⁽³⁸⁾ dėl autosertifikuotų organizacijų, įskaitant išsamių klausimynų siuntimą. Jis taip pat sistemiškai atliks peržiūras visais atvejais, kai gaus konkretų (pagrįstą) skundą, kai organizacija nepateikia patenkinamų atsakymų į gautas užklausas arba kai yra patikimų įrodymų, iš kurių matyti, kad organizacija gali nesilaikyti privatumo principų. Komercijos departamentas, kai tinkama, konsultuosius su DAI dėl tokių atitikties peržiūrų;

2.3. Teisių gynimo institucijos, skundų nagrinėjimas ir reikalavimų užtikrinimas

- (38) pagal ES ir JAV „privatumo skydo“ teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principą reikalaujama, kad organizacijos suteiktų asmenims, kurie nukenčia dėl reikalavimų nesilaikymo, galimybę ginti savo teises, t. y. galimybę ES duomenų subjektams pateikti skundus dėl JAV autosertifikuotų bendrovių reikalavimų nesilaikymo ir reikalauti, kad šie skundai būtų išnagrinėti, įskaitant sprendimo, kuriuo suteikiama veiksminga teisių gynimo priemonė, priėmimą;
- (39) taikydamos autosertifikavimo procedūrą, organizacijos privalo įvykdyti teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principo reikalavimus ir užtikrinti veiksmingų ir veikiančių nepriklausomų teisių gynimo institucijų nustatymą, kuriose būtų galima nemokamai tirti ir greitai išspręsti kiekvieno asmens skundą ir ginčus;
- (40) organizacijos gali pasirinkti Sąjungoje arba Jungtinėse Amerikos Valstijose veikiančias nepriklausomas teisių gynimo institucijas. Tai apima galimybę savanoriškai išpareigoti bendradarbiauti su ES DAI. Tačiau tokios

⁽³⁶⁾ Žr. I priedą „Klaidingų pareiškimų dėl dalyvavimo paieška ir tokių pareiškimų šalinimas“.

⁽³⁷⁾ Žr. II priedo III.6.h skirsnį ir III.11.f skirsnį.

⁽³⁸⁾ Žr. I priedą.

pasirinkimo laisvės nėra tais atvejais, kai organizacijos tvarko žmoniškųjų išteklių duomenis, nes tokiu atveju su DAI privaloma bendradarbiauti. Kitos alternatyvos apima nepriklausomą alternatyvų ginčų sprendimą (ADR) arba privačiojo sektoriaus sukurtas privatumo programas, į kurių taisykles įtraukti privatumo principai. Tokiose programose turi būti nustatyti veiksmingi reikalavimų užtikrinimo mechanizmai, atitinkantys teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principo nuostatas. Organizacijos turi pareigą išspręsti visas su reikalavimų nesilaikymu susijusias problemas. Organizacijos taip pat privalo nurodyti, ar joms taikomi FPK, Transporto departamento ar bet kurios kitos JAV įgalios valstybinės įstaigos tyrimo ir vykdymo įgaliojimai;

- (41) todėl „privatumo skydo“ sistemoje duomenų subjektams numatytos įvairios galimybės įgyvendinti savo teises, pateikti skundus dėl JAV autosertifikuotų bendrovių reikalavimų nesilaikymo ir reikalauti, kad jų skundai būtų išspręsti, įskaitant sprendimo, kuriuo nustatoma veiksminga teisių gynimo priemonė, priėmimą. Asmenys skundą gali pateikti tiesiogiai organizacijai, organizacijos paskirtai nepriklausomai ginčų sprendimo institucijai, nacionalinėms DAI arba FPK;
- (42) jeigu jų skundų neišnagrinėjo nė viena iš šių teisių gynimo arba reikalavimų užtikrinimo institucijų, asmenys taip pat turi teisę naudotis privalomo arbitražo, už kurį atsako „privatumo skydo“ komisija (šios sprendimo II priedo 1 priedas). Išskyrus arbitražo komisiją, į kurią galima kreiptis tik išnaudojus tam tikras teisių gynimo priemones, asmenys gali laisvai savo nuožiūra kreiptis į bet kurią ar visas teisių gynimo institucijas ir neprivalo kreiptis į vieną ar kitą instituciją, ar vadovautis konkrečia veiksmų seka. Tačiau galioja tam tikra toliau aprašyta loginė tvarka, kuria partartina vadovautis;
- (43) pirma, ES duomenų subjektai gali iškelti bylas dėl privatumo principų nesilaikymo kreipdamiesi tiesiogiai į JAV autosertifikuotą bendrovę. Siekdama palengvinti ginčų sprendimą, organizacija privalo nustatyti veiksmingą teisių gynimo instituciją, į kurią būtų galima kreiptis nagrinėjant tokius skundus. Todėl organizacijos privatumo politikoje asmenims turi būti pateikiama aiški informacija apie organizacijoje arba už jos ribų veikiančią kontaktinę centrą, kuris nagrinės skundus (įskaitant bet kokią padalinį Sąjungoje, kuriam gali būti perduodami prašymai arba skundai), ir apie nepriklausomas skundų nagrinėjimo institucijas;
- (44) tiesiogiai iš asmens ar per Komercijos departamentą, kuriam bylą perdavė DAI, gavusi individualų skundą, organizacija ES duomenų subjektui privalo atsakyti per 45 dienų terminą. Šiame atsakyme turi būti pateiktas esminių skundo aplinkybių vertinimas ir informacija apie tai, kaip organizacija išspręs problemą. Be to, reikalaujama, kad organizacijos greitai reaguotų į Komercijos departamento arba DAI ⁽³⁹⁾ (kai organizacija įsipareigojo bendradarbiauti su DAI) užklausas ir kitus prašymus pateikti informaciją, kaip organizacijos laikosi privatumo principų. Organizacijos privalo saugoti su jų privatumo politikos įgyvendinimu susijusius įrašus ir paprašyta leisti su jais susipažinti nepriklausomai teisių gynimo institucijai ar FPK (arba kitai JAV valdžios institucijai, kuri turi jurisdikciją tirti nesąžiningus ir apgaulingus veiksmus), kuri atlieka tyrimą ar nagrinėja skundą dėl reikalavimų nesilaikymo;
- (45) antra, asmenys skundą taip pat gali tiesiogiai pateikti organizacijos paskirtai nepriklausomai ginčų sprendimo institucijai (Jungtinėse Amerikos Valstijose arba Sąjungoje), kad ji tirtų ir spręstų asmenų pateiktus skundus (išskyrus atvejus, kai nustatoma, kad jie akivaizdžiai nepagrįsti ar nerimti) ir suteikti asmeniui tinkamas nemokamas teisių gynimo priemones. Tokios institucijos nustatytos sankcijos ir teisių gynimo priemonės turi būti pakankamai griežtos, kad priverstų organizacijas laikytis privatumo principų, be to, šiomis sankcijomis ir teisių gynimo priemonėmis organizacijos turėtų būti įpareigojamos panaikinti ar ištaisyti su reikalavimų nesilaikymu susijusias pasekmes, liautis toliau tvarkingus asmens duomenis, kuriems kyla pavojus, ir (arba) juos ištrinti, taip pat viešai paskelbti su reikalavimų nesilaikymu susijusias išvadas. Organizacijos paskirtos nepriklausomos ginčų sprendimo institucijos savo svetainėse turės pateikti atitinkamą informaciją apie ES ir JAV „privatumo skydo“ sistemą ir paslaugas, kurias jos teikia veikdamos šioje sistemoje. Kiekvienais metais organizacijos privalo skelbti metinę ataskaitą, kurioje pateikiami apibendrinti statistiniai duomenys apie šias paslaugas ⁽⁴⁰⁾;

⁽³⁹⁾ Tai yra DAI komisijos paskirta nagrinėjimo institucija, kaip nustatyta principo „Duomenų apsaugos institucijų vaidmuo“ nuostatose (II priedo III.5 skirsnis).

⁽⁴⁰⁾ Metinėje ataskaitoje būtina nurodyti: 1) bendrą su „privatumo skydu“ susijusių skundų, gautų per ataskaitinius metus, skaičių; 2) gautų skundų rūšis; 3) kokybinius ginčų sprendimo rodiklius, pvz., skundų nagrinėjimo trukmę, ir 4) sprendimus, kurie buvo priimti išnagrinėjus skundus, visų pirma nustatytų teisių gynimo priemonių arba sankcijų skaičių ir rūšis.

- (46) laikydamasis savo atitikties peržiūros procedūrų, Komercijos departamentas taip pat tikrins, ar JAV autosertifikuotos bendrovės, atsižvelgiant į jų pareiškimus dėl registracijos, yra registruotos nepriklausomų teisių gynimo institucijų narės. Organizacijos ir nepriklausomos teisių gynimo institucijos turi greitai reaguoti į Komercijos departamento pateiktas užklaudas ir prašymus pateikti informaciją, susijusią su „privatumo skydu“;
- (47) jeigu organizacija nesilaiko ginčų sprendimo arba savireguliacinės institucijos sprendimo, pastaroji privalo apie tai informuoti Komercijos departamentą ir FPK (arba kitą JAV valdžios instituciją, turinčią jurisdikciją tirti nesąžiningus ir apgaulingus veiksmus) arba kompetentingą teismą ⁽⁴¹⁾. Jeigu organizacija atsisako vykdyti galutinį bet kurios privatumo savireguliacinės institucijos, nepriklausomos ginčų sprendimo institucijos ar Vyriausybės įstaigos sprendimo, arba kai tokia institucija ar įstaiga nustato, organizacija dažnai nesilaiko privatumo principų, tai bus laikoma nuolatinio principų nesilaikymu, todėl Komercijos departamentas, įteikdamas 30 dienų pranešimą ir suteikdamas galimybę organizacijai, kuri nesilaikė reikalavimų, pateikti atsakymą, išbrauks ją iš sąrašo ⁽⁴²⁾. Jeigu iš sąrašo išbraukta organizacija toliau naudoja „privatumo skydo“ sertifikavimo ženklą, Departamentas būtų perduos FPK arba kitai teisėsaugos institucijai ⁽⁴³⁾;
- (48) trečia, asmenys savo skundus taip pat gali pateikti nacionalinei duomenų apsaugos institucijai. Organizacijos turi pareigą bendradarbiauti su skundą tiriančia ir sprendžiančia DAI, kai toks skundas yra susijęs su žmogiškųjų išteklių duomenų, surinktų įdarbinimo metu, tvarkymu arba kai atitinkama organizacija savanoriškai sutiko, kad DAI prižiūrėtų jos veiklą. Visų pirma organizacijos turi atsakyti į užklaudas, paisyti DAI pateiktų rekomendacijų, įskaitant rekomendaciją dėl teisių gynimo ar kompensacinių priemonių, ir pateikti DAI rašytinį patvirtinimą, kad tokių veiksmų buvo imtasi;
- (49) DAI rekomendacijos bus skelbiamos per Sąjungos lygiu įkurtą DAI neformalią komisiją, kuri padės užtikrinti suderintą ir nuoseklų požiūrį į konkretų skundą ⁽⁴⁴⁾. Rekomendacijos bus priimanamos abiem ginčo šalims suteikus pagrįstą galimybę pateikti pastabas ir visus pageidaujamus įrodymus. Komisija pateiks rekomendacijas iš karto, kai tik įvykdys procesinius reikalavimus, paprastai per 60 dienų nuo skundo gavimo. Jeigu organizacija per 25 dienas po rekomendacijų pateikimo neįvykdo rekomendacijose nustatytų reikalavimų ir nepateikia tinkamo paaiškinimo, komisija praneša apie savo ketinimus pateikti klausimą FPK (ar kitai kompetentingai JAV teisėsaugos institucijai) arba nusprendžia, kad bendradarbiavimo įsipareigojimas yra rimtai pažeistas. Pirmuoju atveju pagal FPK akto 5 straipsnį (ar panašų įstatymą) galima imtis intervencinių priemonių. Antruoju atveju komisija informuoja Komercijos departamentą, kuris pripažins, kad organizacijos atsisakymas laikytis DAI komisijos rekomendacijų prilygsta nuolatiniam reikalavimų nesilaikymui, todėl organizacija bus išbraukta iš „privatumo skydo“ sąrašo;
- (50) jeigu DAI, kuriai adresuotas skundas, nesiėmė jokių veiksmų arba ėmėsi netinkamų veiksmų, kad išnagrinėtų skundą, skundo pareiškėjas turi galimybę apskusti tokį veikimą (neveikimą) atitinkamos valstybės narės nacionaliniams teismams;
- (51) asmenys skundus DAI taip pat gali pateikti net jeigu DAI komisija nebuvo paskirta kaip organizacijos ginčų sprendimo institucija. Šiais atvejais DAI gali tokius skundus perduoti Komercijos departamentui arba FPK. Siekdamas palengvinti ir sustiprinti bendradarbiavimą su asmenų skundais ir „privatumo skydo“ organizacijų reikalavimų nesilaikymu susijusiais klausimais, Komercijos departamentas įsteigs specialų kontaktinį centrą, kuris veiks kaip ryšių palaikymo įstaiga ir padės DPA atsakyti į užklaudas, susijusias su tuo, kaip organizacija laikosi privatumo principų ⁽⁴⁵⁾. Be to, FPK įsipareigojo įsteigti specialų kontaktinį centrą ⁽⁴⁶⁾ ir pagal JAV saugaus tinklo aktą ⁽⁴⁷⁾ teikti pagalbą DAI atliekant tyrimus;

⁽⁴¹⁾ Žr. II priedo III.1.1.e skirsnį.

⁽⁴²⁾ Žr. II priedo III.1.1.g skirsnį, visų pirma ii ir iii punktus.

⁽⁴³⁾ Žr. I priedą „Klaudingų pareiškimų dėl dalyvavimo paieška ir tokių pareiškimų šalinimas“.

⁽⁴⁴⁾ Neformalios DAI komisijos darbo taisyklės turėtų nustatyti DAI, remdamosi savo kompetencija organizuoti jų darbą ir bendradarbiauti tarpusavyje.

⁽⁴⁵⁾ Žr. I priedą, skirsnius dėl aktyvesnio bendradarbiavimo su DAI ir lengvesnio skundų, susijusių su reikalavimų nesilaikymu, nagrinėjimo ir II priedo II.7.e skirsnį.

⁽⁴⁶⁾ Žr. IV priedo p. 6.

⁽⁴⁷⁾ Ten pat.

- (52) ketvirta, Komercijos departamentas įsipareigojo gauti ir peržiūrėti skundus, kuriuose teigiama, kad organizacija nesilaiko privatumo principų, ir dėti visas pastangas, kad juos išspręstų. Šiuo tikslu Komercijos departamentas sukūrė DAI skirtas konkrečias procedūras, kurios taikomos perduodant skundus kontaktiniam centrui, stebint skundų nagrinėjimo eigą ir toliau bendradarbiaujant su bendrovėmis, siekiant palengvinti ginčų sprendimą. Siekdamas pagreitinti individualių skundų nagrinėjimą, kontaktinis centras ne vėliau kaip per 90 dienų nuo skundo perdavimo jam dienos, tiesiogiai susisiečia su atitinkama DAI, kad aptartų atitikties klausimus ir visų pirma pateiktų DAI naujausią informaciją apie skundų statusą. Todėl duomenų subjektai gali tiesiogiai savo nacionalinei DAI pateikti skundus, kuriuose JAV autosertifikuotas bendrovės kaltina reikalavimų nesilaikymu, kad pastaroji perduotų juos Komercijos departamentui, kuris veikia kaip JAV valdžios institucija, atsakinga už ES ir JAV „privatumo skydo“ administravimą. Komercijos departamentas taip pat įsipareigojo kartu su metine ES ir JAV „privatumo skydo“ veikimo peržiūra teikti ataskaitą, kurioje būtų analizuojami apibendrinti duomenys apie kasmet gautus skundus ⁽⁴⁸⁾;
- (53) jeigu Komercijos departamentas, remdamasis savo ex officio patikrinimų rezultatais, gautais skundais arba bet kuria kita informacija, padaro išvadą, kad organizacija nuolat nesilaikė privatumo principų, ji išbraukia tokią organizaciją iš „privatumo skydo“ sąrašo. Atsisakymas laikytis galutinio kurios nors savireguliacinės, nepriklausomos ginčų sprendimo arba Vyriausybės įstaigos, įskaitant DAI, sprendimo bus pripažįstamas nuolatiniu reikalavimų nesilaikymu;
- (54) penkta, „privatumo skydo“ organizacija turi pateikti į JAV valdžios institucijų, visų pirma Federalinės prekybos komisijos ⁽⁴⁹⁾, kurios veiksmingai užtikrins atitiktį privatumo principams, tyrimo ir vykdymo įgaliojimų sritį. FPK, siekdama nustatyti, ar nebuvo pažeistas FPK akto 5 straipsnis, prioritetine tvarka nagrinės bylas dėl privatumo principų nesilaikymo, kurias jai perdavė nepriklausomos ginčų sprendimo arba savireguliacijos įstaigos, Komercijos departamentas ir DAI (veikdami savo iniciatyva arba gavusios skundą) ⁽⁵⁰⁾. FPK įsipareigojo sukurti standartizuotą bylų perdavimo procesą, paskirti agentūros kontaktinį centrą, kuris priims DAI perduotas bylas, ir keistis informacija apie perduotas bylas. Be to, FPK priims tiesiogiai asmenų pateiktus skundus ir, nagrinėdama įvairius privatumo klausimus, savo iniciatyva atliks „privatumo skydo“ tyrimus;
- (55) FPK gali užtikrinti atitiktį priimdama administracines nutartis (t. y. draudimas atlikti veiksmus be kitos šalies sutikimo), be to, ji sistemškai stebės, kaip tokių nutarčių laikomasi. Jeigu organizacijos nesilaiko nutarčių, FPK gali perduoti bylą kompetentingam teismui, kad šis paskirtų civilines nuobaudas ir nustatytų kitas teisių gynimo priemones, įskaitant kompensaciją už bet koki neteisėtu elgesiu sukeltą sužalojimą. Kita vertus, FPK gali tiesiogiai kreiptis į federalinį teismą dėl preliminarus ar galutinio sprendimo arba kitų teisių gynimo priemonių. Kiekviename „privatumo skydo“ organizacijai adresuotame draudime atlikti veiksmus be kitos šalies sutikimo bus nustatyti atsisakymo reikalavimai ⁽⁵¹⁾, o organizacijos turės viešai skelbti visus su „privatumo skydu“ susijusius FPK pateiktų atitikties arba vertinimo ataskaitų skirsnius. Galiausiai FPK tvarkys internetinį bendrovių, dėl kurių FPK arba teismas priėmė sprendimą su „privatumo skydu“ susijusiose bylose, sąrašą;
- (56) šešta, ES duomenų subjektas gali prašyti, kad „privatumo skydo“ komisija taikytų privalomą arbitražo procedūrą, kuri naudojama kaip kraštutinis teisių gynimo mechanizmas tuo atveju, jeigu naudojant kitas prieinamas teisių gynimo priemones nepavyko patenkinamai išnagrinėti individualaus skundo. organizacijos privalo informuoti asmenis apie jiems tam tikromis sąlygomis suteikiamą galimybę remtis privalomo arbitražo sąlyga, o arbitražo institucija įpareigojama veikti, kai tik asmuo pasinaudoja šia galimybe, ir įteikti pranešimą atitinkamai organizacijai ⁽⁵²⁾;

⁽⁴⁸⁾ Žr. I priedo skirsnį dėl skundų, susijusių su reikalavimų nesilaikymu, nagrinėjimo.

⁽⁴⁹⁾ „Privatumo skydo“ organizacija turi viešai pareikšti savo įsipareigojimą laikytis privatumo principų, viešai atskleisti savo privatumo politiką, kuri atitinka šiuos principus, ir visapusiškai ją įgyvendinti. Jeigu tokia politika neįgyvendinama, pagal FPK akto 5 straipsnį, kuriuo draudžiami nesąžiningi ir apgaulingi veiksmai prekybos srityje arba prekybai kenkiantys tokie veiksmai, skiriamos sankcijos.

⁽⁵⁰⁾ Iš FPK pateiktos informacijos matyti, kad ji neturi jokių įgaliojimų atlikti patikrinimus vietoje, susijusius su privatumo apsauga. Tačiau FPK turi įgaliojimus priversti organizacijas pateikti dokumentus ir liudytojų parodymus (žr. FPK akto 20 straipsnį) ir gali pasinaudoti teismų sistema, kad įvykdytų tokias nutartis, jeigu jų nesilaikoma.

⁽⁵¹⁾ FPK arba teismo sprendimuose gali būti reikalaujama, kad bendrovės įgyvendintų privatumo programas ir reguliariai skelbtų atitikties ataskaitas arba trečiųjų šalių atliktus nepriklausomus vertinimus, kad su jais galėtų susipažinti FPK.

⁽⁵²⁾ Žr. II priedo II.1.xi ir III.7.c skirsnius.

- (57) šią arbitražo komisiją sudaro ne mažiau kaip 20 arbitrų, kuriuos Komercijos departamentas ir Komisija paskiria atsižvelgdami į jų nepriklausomumą, sąžiningumą, taip pat patirtį JAV privatumo ir Sąjungos duomenų apsaugos teisės srityje. Šalys iš šių 20 arbitrų pasirenka vieną arba tris ⁽⁵³⁾ arbitrus, kurie nagrinės jų ginčą. Byla nagrinėjama taikant standartines arbitražo taisykles, dėl kurių susitaria Komercijos departamentas ir Komisija. Šios taisyklės papildys jau veikiančią sistemą, kurioje nustatyta keletas funkcijų, padedančių užtikrinti geresnę ES duomenų subjektų prieigą prie šio mechanizmo: i) duomenų subjektui komisijai adresuotą reikalavimą gali padėti suformuluoti jo valstybės nacionalinė DAI; ii) nors arbitražo procedūra vyksta Jungtinėse Amerikos Valstijose, ES duomenų subjektai gali nuspręsti dalyvauti naudodamiesi vaizdo arba telefoninės konferencijos paslaugomis, kurios asmeniui teikiamos nemokama; iii) nors arbitražo procedūra paprastai vyks anglų kalba, jeigu duomenų subjektas, pateikęs pagrįstą prašymą, gali gauti nemokamas vertimo žodžiu ir raštu paslaugas ⁽⁵⁴⁾; iv) galiausiai kiekviena šalis turi sumokėti savo advokato mokesčius, tačiau jeigu šaliai advokatas atstovauja komisijoje, Komercijos departamentas įsteigs fondą, į kurį „privatumo skydo“ organizacijos mokės metines įmokas, ir iš šio fondo bus atlyginamos tinkamos finansuoti arbitražo procedūros išlaidos, kurių maksimalų dydį JAV valdžios institucijos nustatys pasikonsultavusios su Komisija;
- (58) „privatumo skydo“ komisijai bus suteikti įgaliojimai nustatyti privalomą „individualią lygiavertę nepiniginę teisių gynimo priemonę“ ⁽⁵⁵⁾, kuri yra būtina dėl privatumo principų nesilaikymo susidariusiai padėčiai ištaisyti. Nors komisija, priimdama sprendimą, atsižvelgia į kitas teisių gynimo priemones, kurios buvo nustatytos taikant kitus „privatumo skydo“ mechanizmus, asmenys vis tiek gali kreiptis į arbitražą, jei mano, kad šios kitos teisių gynimo priemonės nėra tinkamos. Tai leis ES duomenų subjektams taikyti arbitražą visais atvejais, kai dėl kompetentingų JAV valdžios institucijų (pvz., FPK) veikimo ar neveikimo jų skundai nebuvo patenkinamai išnagrinėti. Arbitražo negalima taikyti, jeigu DAI turi teisinius įgaliojimus nagrinėti pareikštą reikalavimą, susijusį su JAV autosertifikuota bendrove, t. y. tais atvejais, kai organizacija įpareigojama bendradarbiauti ir paisyti DAI rekomendacijų dėl žmogiškųjų išteklių duomenų, surinktų įdarbinant asmenį, tvarkymo arba savanoriškai įsipareigojo tai daryti. Asmenys arbitražo sprendimą JAV teismuose gali vykdyti pagal Federalinį arbitražo aktą – taip užtikrinamas teisių gynimas, jeigu bendrovė nesilaiko arbitražo sprendimo;
- (59) septinta, jeigu organizacija nesilaiko įsipareigojimo laikytis privatumo principų ir viešai skelbti privatumo politiką, pagal JAV valstijų įstatymus galima pasinaudoti papildomomis teisminėmis teisių gynimo priemonėmis, t. y. deliktų teisėje nustatytomis teisių gynimo priemonėmis, kurios taikomos apgaulingo klaidinimo, nesąžiningų arba apgaulingų veiksmų ar praktikos arba sutarties pažeidimo atvejais;
- (60) be to, jeigu DAI, gavusi ES duomenų subjekto prašymą, mano, kad asmens duomenų perdavimas Jungtinių Amerikos Valstijų organizacijai vykdomas pažeidžiant ES duomenų apsaugos teisę, įskaitant atvejus, kai ES duomenų eksportuotojas turi pagrindo manyti, kad ta organizacija nesilaiko Principų, ji gali pasinaudoti savo įgaliojimais ir duomenų eksportuotojo atžvilgiu ir prireikus nurodyti sustabdyti duomenų perdavimą;
- (61) atsižvelgdama į šiame skirsnyje pateiktą informaciją, Komisija mano, kad JAV komercijos departamento nustatytais privatumo principais iš tikrųjų užtikrinamas asmens duomenų apsaugos lygis, kuris iš esmės yra lygiavertis apsaugos lygiui, garantuojamam taikant Direktyvoje 95/46/EB nustatytus pagrindinius principus;
- (62) be to, veiksmingas privatumo principų taikymas garantuojamas Komercijos departamento įsipareigojimų skaidrumu ir „privatumo skydo“ sistemos administravimu ir atitikties peržiūra;
- (63) Komisija taip pat mano, kad, atsižvelgiant į visas aplinkybes, „privatumo skydo“ sistemoje užtikrinama priežiūra ir teisių gynimas, o nurodytos teisių gynimo institucijos sudaro sąlygas nustatyti „privatumo skydo“ organizacijų padarytus privatumo principų pažeidimus ir taikyti praktines bausmes bei suteikti teises teisių gynimo priemones duomenų subjektui, kad jis galėtų susipažinti su savo asmens duomenimis ir galiausiai panaikinti arba ištrinti tokius duomenis;

⁽⁵³⁾ Dėl komisijos arbitrų skaičiaus turės susitarti šalys.

⁽⁵⁴⁾ Tačiau komisija gali nustatyti, kad, atsižvelgiant į konkretaus arbitražo aplinkybes, arbitražo procedūra gali būti nepagrįstai arba neproporcingai brangi.

⁽⁵⁵⁾ Asmenys per arbitražo procedūrą negali reikalauti atlyginti nuostolių, tačiau arbitražo taikymas nereiškia, kad tokie asmenys netenka galimybės prisiteisti nuostolių atlyginimą JAV teismuose.

3. JAV VALDŽIOS INSTITUCIJŲ PRIEIGA PRIE ASMENS DUOMENŲ, PERDUOTŲ PAGAL ES IR JAV „PRIVATUMO SKYDO“ SISTEMĄ, IR ŠIŲ DUOMENŲ NAUDOJIMAS

- (64) kaip matyti iš II priedo I.5 skirsnio, privatumo principų reikia laikytis tiek, kiek būtina siekiant įvykdyti nacionalinio saugumo, viešojo intereso arba teisėsaugos reikalavimus;
- (65) Komisija įvertino JAV teisėje nustatytus apribojimus ir apsaugos priemones, susijusias su JAV valdžios institucijų prieiga prie asmens duomenų, perduotų pagal ES ir JAV „privatumo skydo“ sistemą, ir šių duomenų naudojimu nacionalinio saugumo, teisėsaugos ir kitais viešojo intereso tikslais. Be to, JAV Vyriausybė per savo Nacionalinės žvalgybos direktoriaus biurą (ODNI) ⁽⁵⁶⁾ pateikė Komisijai išsamius pareiškimus ir išsipareigojimus, kurios išdėstytos šio sprendimo VI priede. Rašte, kuris prie šio sprendimo pridedamas kaip II priedas, JAV Vyriausybė taip pat išsipareigojo sukurti naują nacionalinio saugumo priemonių priežiūros mechanizmą, t. y. „privatumo skydo“ ombudsmeną, kuris bus nepriklausomas nuo žvalgybos bendruomenės. Galiausiai JAV teisingumo departamento pareiškime, kuris pateiktas šio sprendimo VII priede, aprašomi valdžios institucijų prieigos prie duomenų ir jų naudojimo teisėsaugos ir kitais viešojo intereso tikslais apribojimai ir su tuo susijusios saugumo priemonės. Siekiant didinti skaidrumą ir užtikrinti šių išsipareigojimų teisinį pobūdį, kiekvienas šiame sprendime nurodytas ir prie jo pridėtas dokumentas bus skelbiamas JAV federaliniame registre;
- (66) Komisijos išvados dėl JAV valdžios institucijų prieigos prie asmens duomenų, perduotų iš Europos Sąjungos į Jungtines Amerikos Valstijas, ir šių duomenų naudojimo apribojimų ir veiksmingos teisinės apsaugos užtikrinimo išsamiau aptariamos toliau;

3.1. JAV valdžios institucijų prieiga prie duomenų ir jų naudojimas nacionalinio saugumo tikslais

- (67) iš Komisijos analizės matyti, kad JAV teisėje nustatyti įvairūs apribojimai, kurie taikomi prieigai prie duomenų, perduotų pagal ES ir JAV „privatumo skydo“ sistemą, ir šių duomenų naudojimo nacionalinio saugumo tikslais, taip pat nustatytos priežiūros ir teisių gynimo institucijos, kuriose užtikrinamos apsaugos priemonės, padedančios veiksmingai apsisaugoti nuo neteisėto šių duomenų naudojimo ir piktnaudžiavimo jais rizikos ⁽⁵⁷⁾. Nuo 2013 m., kai Komisija priėmė du komunikatus (žr. 7 konstatuojamąją dalį), ši teisinė sistema buvo gerokai sustiprinta, kaip aprašyta toliau;

3.1.1. Apribojimai

- (68) pagal JAV Konstituciją nacionalinio saugumo užtikrinimas – prezidento prerogatyva, jis veikia kaip vyriausiasis vadas ir vykdomasis direktorius, o užsienio žvalgybos srityje tvarko JAV užsienio reikalus ⁽⁵⁸⁾. Nors Kongresas, atsižvelgdamas į šias ribas, turi įgaliojimus nustatyti apribojimus ir tai darė įvairiais atvejais, tačiau prezidentas gali nukreipti JAV žvalgybos bendruomenės veiklą, visų pirma priimdamas vykdomuosius įsakus arba prezidento direktyvas. Ši taisyklė, žinoma, taikoma ir tose srityse, kuriose Kongresas neturi jokių įgaliojimų. Šiuo atžvilgiu dabar galioja dvi pagrindinės teisinės priemonės – tai vykdomasis įsakas (angl. Executive Order) Nr. 12333 (toliau – E.O. 12333) ⁽⁵⁹⁾ ir Prezidento politinė direktyva Nr. 28 (angl. Presidential Policy Directive);

⁽⁵⁶⁾ Nacionalinės žvalgybos direktorius (DNI) veikia kaip žvalgybos bendruomenės vadovas ir vyriausiasis prezidento ir Nacionalinės saugumo tarybos patarėjas. Žr. 2004 m. Žvalgybos reformos ir terorizmo prevencijos aktą, 2004 12 17 Oficialusis leidinys Nr. 108–458. ODNI, be kita ko, nustato reikalavimus, kurie taikomi žvalgybos bendruomenei vykdant užduotis, renkant, analizuojant, apibendrinant ir platinant nacionalinės žvalgybos duomenis, taip pat valdo tokią veiklą ir jai vadovauja, įskaitant gairių dėl informacijos ar žvalgybos duomenų tikrinimo, naudojimo ir dalijimosi tvarkos rengimą. Žr. E.O. 12333 1.3 skirsnio 12333.

⁽⁵⁷⁾ Žr. Schrems, 91 punktą.

⁽⁵⁸⁾ JAV Konstitucijos II straipsnis. Taip pat žr. PPD-28 įžanginę dalį.

⁽⁵⁹⁾ E.O. 12333: Jungtinių Amerikos Valstijų žvalgybos veikla, Federalinis registras, 40 tomas, Nr. 235, (1981 m. gruodžio 8 d.). Viešai paskelbtoje vykdomojo įsako dalyje apibrėžiami JAV žvalgybos veiksmų tikslai, kryptys ir atsakomybė (įskaitant įvairių žvalgybos bendruomenės subjektų vaidmenį) ir nustatomi bendrieji žvalgybinės veiklos vykdymo aspektai (visų pirma poreikis skelbti konkrečias procedūrinės taisykles). Pagal E.O. 12333 3.2 skirsnį Prezidentas, padedamas Nacionalinio saugumo tarybos, ir Nacionalinės žvalgybos direktorius (DNI) priima tokias reikalingas direktyvas, procedūras ir gaires, kurios yra būtinos įsakui įgyvendinti.

(69) 2014 m. sausio 17 d. priimtoje Prezidento politinėje direktyvoje Nr. 28 (PPD-28) nustatyti įvairūs signalų žvalgybos operacijų apribojimai⁽⁶⁰⁾. Ši prezidento direktyva turi privalomą galią JAV žvalgybos institucijoms⁽⁶¹⁾ ir lieka toliau galioji pasikeitus JAV Administracijai⁽⁶²⁾. PPD-28 yra ypač svarbi ne JAV asmenims, įskaitant ES duomenų subjektus. Be kita ko, joje nustatyta, kad:

- a) signalų žvalgybos duomenų rinkimas turi būti pagrįstas įstatymu arba prezidento leidimu, be to, tokie duomenys turi būti renkami pagal JAV Konstituciją (visų pirmą Ketvirtąją pataisą) ir JAV įstatymus;
- b) su visais asmenimis turėtų būti elgiamasi nepažeidžiant jų orumo ir pagarbiai, nepaisant jų pilietybės ar gyvenamosios vietos;
- c) visi asmenys turi teisėtus privatumo interesus, susijusius su jų asmens duomenų tvarkymu;
- d) privatumas ir pilietinės laisvės yra esminiai aspektai, į kuriuos atsižvelgiama planuojant JAV signalų žvalgybos veiklą;
- e) todėl vykdant JAV signalų žvalgybos veiklą būtina numatyti tinkamas visų asmenų asmens duomenų apsaugos priemonės, nepaisant jų pilietybės ar gyvenamosios vietos;

(70) PPD-28 nurodyta, kad signalų žvalgybos duomenys gali būti renkami tik užsienio žvalgybos ar kontržvalgybos tikslais, siekiant paremti nacionalines ar departamentų misijas, o ne kuriuo nors kitu tikslu (pvz., suteikti JAV bendrovėms konkurencinį pranašumą); šiuo atžvilgiu ODNI paaiškina, kad žvalgybos bendruomenės subjektai „turėtų reikalauti, kad, jei įmanoma, renkant duomenis daugiausia dėmesio būtų skiriama konkretiems užsienio žvalgybos tikslams arba temoms ir būtų naudojami diskriminantai (pvz., konkretūs įrenginiai, atrankos sąlygos ir identifikatoriai)“⁽⁶³⁾. be to, pareiškimuose pateikiamos garantijos, kad teisė priimti sprendimus dėl žvalgybos duomenų rinkimo nepaliekama atskirų žvalgybos agentūrų diskrecijai, bet įtraukiama į politiką ir procedūras, kurias įvairūs JAV žvalgybos bendruomenės subjektai (agentūros) turi taikyti, kad įgyvendintų PPD-28⁽⁶⁴⁾. Todėl tinkami sekami įrenginiai analizuojami ir nustatomi vadovaujantis bendra „nacionaline žvalgybos prioritetų sistema (NIPF)“, kuria užtikrinamas žvalgybos prioritetų nustatymas aukštu politiniu lygmeniu ir reguliari jų peržiūra siekiant, kad jie išliktų aktualūs atsižvelgiant į grėsmes nacionaliniam saugumui ir būtų nustatomi atsižvelgiant į galimą riziką, įskaitant privatumui kylančią riziką⁽⁶⁵⁾. Šiuo pagrindu agentūros personalas analizuoja ir nustato konkrečias atrankos sąlygas, kuriomis tikimasi rinkti prioritetus atitinkančius užsienio žvalgybos duomenis⁽⁶⁶⁾. Atrankos sąlygų arba sekamų įrenginių sąrašas turi būti reguliariai peržiūrimas siekiant patikrinti, ar jis vis dar naudingas renkant prioritetinius žvalgybos duomenis⁽⁶⁷⁾;

⁽⁶⁰⁾ Pagal E.O. 12333 Nacionalinės saugumo agentūros (NSA) direktorius veikia kaip signalų žvalgybos funkcinis valdytojas ir vadovauja bendrai signalų žvalgybos veiklą vykdančiai organizacijai.

⁽⁶¹⁾ Žvalgybos bendruomenės sąvokos apibrėžtis pateikta E.O. 12333 3.5 skirsnio h punkte ir PPD-28 1 dalyje.

⁽⁶²⁾ Žr. Teisingumo departamento (DOJ) advokato 2000 m. sausio 29 d. memorandumą Prezidentui B. Clintonui. Pagal šią teisinę nuomonę prezidento direktyvos sukelia „tokias pat materialines teises pasekmes kaip ir vykdomasis įsakas“.

⁽⁶³⁾ ODNI pareiškimai (VI priedas), p. 3.

⁽⁶⁴⁾ Žr. PPD-28 4 skirsnio b ir c punktus. Iš viešai prieinamos informacijos matyti, kad, 2015 m. atlikus peržiūrą, patvirtinta apie šešis galiojančius tikslus. Žr. ODNI, signalų žvalgybos reformą, 2016 m. pažangos ataskaitą.

⁽⁶⁵⁾ ODNI pareiškimai (VI priedas), p. 6 (pateikiama nuoroda į Žvalgybos bendruomenės direktyvą Nr. 204). Taip pat žr. PPD-28 3 skirsnį.

⁽⁶⁶⁾ ODNI pareiškimai (VI priedas), p. 6. Žr., pvz., NSA Pilietinių laisvių ir privatumo biuras (NSA CLPO), NSA pilietinių laisvių ir privatumo apsaugos priemonės, susijusios su tikslinga signalų žvalgybos veikla pagal 2014 m. spalio 7 d. vykdomąjį įsaką. Taip pat žr. ODNI 2014 m. būklės ataskaitą. Dėl prašymų leisti susipažinti su duomenimis pagal FISA 702 straipsnį pažymėtina, kad užklausoms taikomos FISC patvirtintos minimalios informacijos procedūros. Žr. NSA CLPO, NSA užsienio žvalgybos stebėjimo akto 702 straipsnio įgyvendinimas, 2014 m. balandžio 16 d.

⁽⁶⁷⁾ Žr. signalų žvalgybos reformą, 2015 m. metinę ataskaitą. Taip pat žr. ODNI pareiškimus (VI priedas), p. 6, 8–9, 11.

- (71) be to, PPD-28 nustatytiuose reikalavimuose, pagal kuriuos duomenys visada ⁽⁶⁸⁾ turi būti „kuo proporcingesni“ ir kad žvalgybos bendruomenė pirmenybę teikia kitai prieinamai informacijai ir tinkamoms ir pagrįstoms alternatyvoms ⁽⁶⁹⁾, atspindi bendrą taisyklę, kurioje pirmenybė teikiama ne masiniam, bet tikslingam duomenų rinkimui. Pagal ODNI pateiktą patikinimą, minėtais reikalavimais visų pirma užtikrinama, kad masinis duomenų rinkimas nėra nei „masinis“, nei „be atrankos“ ir kad išimtis nėra platesnė už taisyklę ⁽⁷⁰⁾;
- (72) nors PPD-28 paaiškinama, kad žvalgybos bendruomenės subjektai kartais tam tikromis aplinkybėmis privalo rinkti masinius signalų žvalgybos duomenis, pvz., siekdami nustatyti ir įvertinti naujas arba kylančias grėsmes, joje taip pat nurodoma, kad šie subjektai turi nustatyti prioritetines alternatyvas, kurios sudarytų sąlygas atlikti tikslingą signalų žvalgybą ⁽⁷¹⁾. Vadinas duomenys masiškai bus renkami tik tais atvejais, kai tikslingas duomenų rinkimas naudojant diskriminantus, t. y. su konkrečiu sekamu asmeniu susijusius identifikatorius, neįmanomas dėl „techninių ar operatyvinių aplinkybių“ ⁽⁷²⁾. Ši taisyklė taikoma tiek būdai, kuriuo signalų žvalgybos duomenys renkami, tiek faktiškai renkamiems duomenims ⁽⁷²⁾;
- (73) remiantis ODNI pareiškimais, net jeigu žvalgybos bendruomenė negali panaudoti konkrečių identifikatorių, kad tikslingai rinktų duomenis, ji stengsis „kuo sumažinti“ susiaurinti renkamų duomenų kiekį. Siekdama šio tikslo, žvalgybos bendruomenė „taiko filtrus ir kitas technines priemones, kad daugiausia duomenų surinktų iš tų įrenginių, kuriuose, tikėtina, yra didžiausią užsienio žvalgybinę vertę turinčių ryšių“ (ir taip laikysis JAV politikos formuotojų pagal 70 konstatuojamojoje dalyje aprašytą procedūrą nustatytų reikalavimų). Todėl masinis duomenų rinkimas bus tikslingas bent dviem atžvilgiais: pirma, jis visada bus susijęs su konkrečiais užsienio žvalgybos uždaviniais (pvz., įgyti signalų žvalgybos duomenų apie konkrečiame regione veikiančią teroristinę grupę) ir orientuoti duomenų rinkimą į su tokiu uždaviniu susijusius ryšius. Remiantis ODNI pateiktu patikinimu, šią nuostatą įrodo ir tai, kad „Jungtinių Amerikos Valstijų signalų žvalgybos veikla yra susijusi tik su dalimi internete perduodamų ryšių“ ⁽⁷³⁾. Antra, ODNI pareiškimuose paaiškinama, kad naudojami filtrai ir kitos techninės priemonės bus suprojektuoti taip, kad padėtų užtikrinti „kuo tikslesnių“ duomenų rinkimą, siekiant, kad būtų renkamas minimalus „nesusijusios informacijos“ kiekis;
- (74) galiausiai net jeigu Jungtinės Amerikos Valstijos mano, kad signalų žvalgybos duomenis masiškai rinkti yra būtina vadovaujantis 70–73 konstatuojamosiose dalyse nustatytais sąlygomis, PPD-28 tokios informacijos naudojimas, atsižvelgiant į konkretų šešių nacionalinių saugumo principų sąrašą, ribojamas siekiant apsaugoti visų asmenų, nepaisant jų pilietybės ir gyvenamosios vietos, privatumą ir pilietines laisves ⁽⁷⁴⁾. Šie leidžiami tikslai apima priemones, padedančias nustatyti grėsmes, kylančias dėl šnipinėjimo, terorizmo, masinio naikimo ginklų,

⁽⁶⁸⁾ Žr. ODNI pareiškimus (VI priedas), p. 3.

⁽⁶⁹⁾ Taip pat reiktų atkreipti dėmesį į tai, kad pagal E.O. 12333 2.4 skirsnį žvalgybos bendruomenės subjektai „naudoja mažiausiai ribojančius Jungtinėse Amerikos Valstijose prieinamus duomenų rinkimo būdus“. Dėl apribojimų, susijusių su visų masinio duomenų rinkimo operacijų pakeitimu tikslingo duomenų rinkimo operacijomis, žr. Nacionalinės mokslinių tyrimų tarybos vertinimo rezultatus, kuriuos paskelbė Europos Sąjungos pagrindinių teisių agentūra, „Žvalgybos tarnybų vykdoma stebėseną: pagrindinės teisės, apsaugos priemonės ir teisių gynimo būdai ES“ (angl. *Surveillance by intelligence services: fundamental rights, safeguards and remedies in the ES*) (2015 m.), p. 18.

⁽⁷⁰⁾ ODNI pareiškimai (VI priedas), p. 4.

⁽⁷¹⁾ Taip pat žr. PPD-28 5 skirsnio d punktą, kuriame Nacionalinės žvalgybos direktoriui pavedama, koordinuojant veiklą su atitinkamų žvalgybos bendruomenių subjektų vadovais ir Mokslo ir technologijų politikos biuru, teikti prezidentui „ataskaitą, kurioje būtų įvertintos galimybės sukurti programinę įrangą, leisiančią žvalgybos bendruomenei, užuot masiškai rinkus duomenis, lengviau imtis tikslingos informacijos rinkimo veiklos“. Iš viešai prieinamos informacijos matyti, kad šioje ataskaitoje padaryta išvada, jog „nėra jokios programine įranga pagrįstos alternatyvos, kuria būtų galima visiškai pakeisti masinio duomenų rinkimo veiklą siekiant nustatyti tam tikras grėsmes nacionaliniam saugumui“. Žr. signalų žvalgybos reformą, 2015 m. metinę ataskaitą.

⁽⁷²⁾ Žr. 68 išnašą.

⁽⁷³⁾ ODNI pareiškimai (VI priedas). Taip visų pirma sprendžiamas nacionalinių duomenų apsaugos institucijų nuomonėje dėl sprendimo dėl tinkamumo iškeltas klausimas. Žr. 29 straipsnio duomenų apsaugos darbo grupės nuomonę 01/2016 dėl ES ir JAV sprendimo dėl „privatumo skydo“ tinkamumo projekto (priimta 2016 m. balandžio 13 d.), p. 38, 47 punktas.

⁽⁷⁴⁾ Žr. PPD-28 2 skirsnį.

grėsmės kibernetiniam saugumui, ginkluotosioms pajėgoms ar kariuomenės personalui, taip pat tarpvalstybines nusikalstamos veiklos grėsmes, susijusias su kitais penkiais tikslais, ir su jomis kovoti, be to, šie tikslai bus peržiūrimi ne rečiau kaip kartą per metus. Iš JAV Vyriausybės pareiškimų matyti, kad žvalgybos bendruomenės subjektai, siekdami įvykdyti šiuos reikalavimus, sugriežtino analizės srityje galiojančią praktiką ir standartus, kurie taikomi teikiant užklausas dėl neišvertintų signalų žvalgybos duomenų; teikiant tikslingas užklausas „užtikrinama, kad analitikams būtų pateikti nagrinėti tik tie duomenys, kurie, kaip manoma, gali turėti žvalgybinę vertę“⁽⁷⁵⁾;

- (75) šie apribojimai yra ypač svarbūs perduodant asmens duomenis pagal ES ir JAV „privatumo skydą“, visų pirma tuo atveju, kai asmens duomenis ketinama rinkti už Jungtinių Amerikos Valstijų ribų, įskaitant duomenų tikrinimą juos perduodant transatlantiniais kabeliais iš Sąjungos į Jungtines Amerikos Valstijas. ODNI pareiškimuose JAV valdžios institucijos patvirtino, kad tokiam duomenų rinkimui taikomi juose, įskaitant PPD-28, nurodyti apribojimai ir apsaugos priemonės⁽⁷⁶⁾;
- (76) nors apribojimai nėra suformuluoti vartojant teisinius terminus, šiuose principuose įtvirtinti esminiai būtinumo ir proporcingumo principų aspektai. Akivaizdu, kad pirmenybė teikiama tikslingam duomenų rinkimui, o masinis duomenų rinkimas taikomas tik (išimtiniais) atvejais, kai duomenų tikslingai rinkti neįmanoma dėl techninių ar veiklos priežasčių. NET jeigu masinio duomenų rinkimo negalima išvengti, tolesnis tokių duomenų „naudojimas“ juos tikrinant griežtai ribojamas atsižvelgiant į konkrečius teisėtus nacionalinio saugumo tikslus⁽⁷⁷⁾;
- (77) kadangi šiuos reikalavimus direktyvos forma prezidentas priėmė kaip vykdomasis direktorius, jų privalo laikytis visa žvalgybos bendruomenė ir jie išsamiau apibūdinami agentūros taisyklėse ir procedūrose, kuriomis bendrieji principai perkeliama į konkrečias kasdinių operacijų instrukcijas. Be to, nors Kongresas pats nėra saistomas PPD-28, jis taip pat ėmėsi veiksmų, siekdamas užtikrinti, kad asmens duomenų rinkimas Jungtinėse Amerikos Valstijose ir prieiga prie jų būtų tikslinga, o ne užtikrinama „bendraisiais pagrindais“;
- (78) iš turimos informacijos, įskaitant iš JAV Vyriausybės gautus pareiškimus, matyti, kad, perdavus duomenis Jungtinėse Amerikos Valstijose esančioms ir pagal ES ir JAV „privatumo skydą“ autosertifikuotoms organizacijoms, JAV žvalgybos agentūros gali prašyti suteikti asmens duomenis tik⁽⁷⁸⁾ kai jų prašymas atitinka Užsienio žvalgybos stebėjimo aktą (FISA) arba jį Federalinis tyrimų biuras (FTB) pateikia pagal vadinamąjį raštą dėl nacionalinio saugumo (NSL)⁽⁷⁹⁾. FISA nustatyta keletas teisinių pagrindų, kuriais remiantis gali būti renkami (ir vėliau tvarkomi) ES duomenų subjektų asmens duomenys, perduoti pagal ES ir JAV „privatumo skydą“. Be FISA

⁽⁷⁵⁾ ODNI pareiškimai (VI priedas), p. 4. Taip pat žr. Žvalgybos bendruomenės direktyvą Nr. 203.

⁽⁷⁶⁾ ODNI pareiškimai (VI priedas), p. 2. Panašiai taikomi E.O. 12333 nustatyti apribojimai (pvz., poreikis užtikrinti, kad surinkta informacija atitiktų prezidento nustatytus žvalgybos prioritetus).

⁽⁷⁷⁾ Žr. *Schrems*, 93 punktas.

⁽⁷⁸⁾ Be to, FTB duomenis taip pat gali rinkti gavęs teisėsaugos institucijų leidimą (žr. šio sprendimo 3.2 skirsnį).

⁽⁷⁹⁾ Dėl išsamesnių paaiškinimų apie NSL naudojimą žr. ODNI pareiškimus (VI priedas), p. 13–14, 38 skirsnis. Kaip nurodyta tuose pareiškimuose, FTB gali remtis NSL tik prašydamas su turiniu nesusijusios informacijos, kuri yra svarbi atliekant sankcionuotą tyrimą dėl nacionalinio saugumo siekiant apsaugoti nuo tarptautinio terorizmo arba nelegalios žvalgybos veiklos. Kalbant apie duomenų perdavimą pagal ES ir JAV „privatumo skydą“, pažymėtina, kad svarbiausias teisinis leidimo pagrindas, atrodo, yra Elektroninių ryšių privatumo aktas (JAV kodekso 18 antraštinės dalies 2709 straipsnis), pagal kurį reikalaujama, kad kiekviename prašyme pateikti informaciją apie abonentinį arba įrašus apie sandorius turi būti naudojama „sąlyga, iš kurios galima aiškiai identifikuoti asmenį, subjektą, telefono numerį ar sąskaitą“.

104 straipsnio ⁽⁸⁰⁾, kuris taikomas tradiciniam individualiam elektroniniam stebėjimui, ir FISA 402 straipsnio ⁽⁸¹⁾ dėl renkamų numerių registratorių arba spąstų ir sekimo prietaisų naudojimo, dvi pagrindinės nuostatos – tai FISA 501 straipsnis (buvęs JAV patriotinio akto 215 straipsnis) ir FISA 702 straipsnis ⁽⁸²⁾;

(79) šiuo atžvilgiu 2015 m. birželio 2 d. priimtame JAV laisvės akte draudžiama masiškai rinkti įrašus remiantis FISA 402 straipsniu (renkamų numerių registratorių arba spąstų ir sekimo prietaisų naudojimas), FISA 501 straipsniu (buvęs JAV patriotinio akto 215 straipsnis) ⁽⁸³⁾ ir naudojant NSL, vietoje to, reikalaujama taikyti konkrečias „atrankos sąlygas“ ⁽⁸⁴⁾;

(80) nors FISA nustatyti papildomi teisiniai leidimai vykdyti nacionalinę žvalgybos veiklą, įskaitant signalų žvalgybą, Komisijos vertinimas parodė, kad, kiek tai susiję su asmens duomenimis, kurie turi būti perduodami pagal ES ir JAV „privatumo skydą“, šios institucijos lygiai taip pat riboja valstybės intervencinius veiksmus tikslingai renkant ir tikrinant duomenis;

(81) tai aiškiai matyti iš individualaus elektroninio stebėjimo pagal FISA 104 straipsnį ⁽⁸⁵⁾. FISA 702 straipsnyje nustatytas pagrindas tų dviejų svarbių žvalgybos programų, kurias vykdo JAV žvalgybos agentūros (PRISM, UPSTREAM), todėl paieškos atliekamos tikslingai naudojant individualius sekamus įrenginius, kuriais nustatomi konkreti ryšių infrastruktūra, pvz., sekamo asmens e. pašto adresas arba telefono numeris, tačiau ne raktiniai žodžiai ar net sekamų asmenų vardai ⁽⁸⁶⁾. Todėl, kaip nurodė Privatumo ir pilietinių laisvių priežiūros valdyba

⁽⁸⁰⁾ JAV kodekso 50 antraštinės dalies 1804 straipsnis. Nors pagal šią teisinę nuostatą reikalaujama „nurodyti faktus ir aplinkybes, kuriomis pareiškėjas grindžia savo įsitikinimą, kad A) elektroninio stebėjimo dalykas yra užsienio valstybės arba užsienio valstybės agentas“, kuriuo gali būti ir ne JAV asmenys, užsiimančys tarptautine terorizmo veikla arba platinantys masinio naikinimo ginklus (įskaitant parengiamuosius veiksmus) (JAV kodekso 50 antraštinės dalies 1801 straipsnio b dalies 1 punktas). Vis dėlto ryšys su pagal ES ir JAV „privatumo skydo“ nuostatas perduotais asmens duomenimis tėra teorinis, nes nurodytais faktais taip pat turi būti pagrindžiamas įsitikinimas, kad „kiekvieną objektą arba vietą, į kurią yra nukreipta elektroninio stebėjimo veikla, naudoja arba ketina naudoti užsienio valstybės arba užsienio valstybės atstovas“. Bet kuriuo atveju, naudojant šią priemonę, būtina teikti prašymą FISC, kuris, be kita ko, įvertins, ar, atsižvelgiant į nurodytą faktus, yra tikimybė, kad faktai atitinka tikrovę.

⁽⁸¹⁾ JAV kodekso 50 antraštinės dalies 1841 straipsnio 2 dalis ir 18 antraštinės dalies 3127 straipsnis. Ši priemonė nėra susijusi su ryšių turiniu, tiesą sakant, ji yra susieta su informacija apie paslauga besinaudojantį klientą arba abonentą (pvz., vardas, adresas, abonto numeris, gautos paslaugos trukmė/rūšis, mokėjimo šaltinis/būdas). Pagal ją reikalaujama, kad FISC (arba JAV magistrato teisėjas) priimtų sprendimą ir naudotų specialią atrankos sąlygą, kaip aprašyta 1841 straipsnio 4 dalyje, t. y. sąlygą, kurioje aiškiai nurodomas asmuo, sąskaita, ir pan., kurios paskirtis – kuo labiau pagrįstai riboti renkamos informacijos kiekį.

⁽⁸²⁾ Tuo tarpu FISA 501 straipsniu (buvęs JAV patriotinio akto 215 straipsnis) FTB leidžiama kreiptis į teismą, kad šis priimtų sprendimą dėl „materialių daiktų“ (visų pirma telefoninių metaduomenų ir verslo dokumentų) rinkimo užsienio žvalgybos tikslais. Pagal FISA 702 straipsnį JAV žvalgybos bendruomenės subjektams leidžiama Jungtinėse Amerikos Valstijose rinkti informaciją (įskaitant interneto ryšių turinį), susijusią su tam tikrais ne JAV asmenimis, esančiais už Jungtinių Amerikos Valstijų ribų.

⁽⁸³⁾ Remdamasis šia nuostata, FTB gali teikti prašymą dėl „materialių daiktų“ (pvz., įrašų, dokumentų, sutarčių), o toks prašymas gali būti grindžiamas Užsienio žvalgybos priežiūros teismui (FISC) pateiktais įrodymais, kuriais patvirtinama, kad esama pagrįstų priežasčių manyti, jog tokie materialūs daiktai yra svarbūs konkrečiam FTB tyrimui. Atlikdamas paiešką, FTB privalo taikyti FISC patvirtintas atrankos sąlygas, iš kurių matyti, kad esama „pagrįsto ir aiškaus įtariamo“, jog tokia sąlyga yra susijusi su viena arba daugiau užsienio valstybių arba jų agentų, užsiimančių terorizmo arba pasirengimo terorizmui veikla. Žr. PCLOB ataskaitos 215 skirsnį, p. 59, NSA CLPO, *Transparency Report: The USA Freedom Act Business Records FISA Implementation*, 2016 m. sausio 15 d., p. 4–6.

⁽⁸⁴⁾ ODNI pareiškimai (VI priedas), p. 13 (38 dalis).

⁽⁸⁵⁾ Žr. 81 išnašą.

⁽⁸⁶⁾ PCLOB ataskaitos 702 skirsnis, p. 32–33, įskaitant papildomas nuorodas. NSA privatumo biuro teigimu, NSA privalo patikrinti, ar tarp sekamo asmens ir sekamo įrenginio yra ryšys, dokumentuoti užsienio žvalgybos informaciją, kurią tikimasi gauti, šią informaciją turi peržiūrėti ir tvirtinti du vyresnieji NSA analitikai, o visas procesas bus stebimas, kad vėliau ODNI ir Teisingumo departamentas galėtų atlikti atitikties peržiūras. Žr. NSA CLPO, NSA užsienio žvalgybos akto 702 straipsnio įgyvendinimas, 2014 m. balandžio 16 d.

(PCLOB), stebėjimas pagal 702 straipsnį reiškia „visiškai tikslingą konkretaus [ne JAV] asmenų, dėl kurių buvo priimtas individualus sprendimas, sekimą“⁽⁸⁷⁾. Dėl laikino galiojimo sąlygos FISA 702 straipsnis turės būti peržiūrėtas 2017 m., o Komisija tuo metu turės pakartotinai įvertinti ES duomenų subjektams prieinamas apsaugos priemonės;

- (82) be to, savo pareiškimuose JAV Vyriausybė aiškiai patikino Europos Komisiją, kad JAV žvalgybos bendruomenė „neužsiima bet kokių asmenų, įskaitant Europos piliečius, masinio stebėjimo veikla“⁽⁸⁸⁾. Kalbant apie Jungtinėse Amerikos Valstijose surinktus asmens duomenis, pažymėtina, kad šį pareiškimą galima pagrįsti empiriniais įrodymais, iš kurių matyti, kad NSL forma pagal FISA atskirai ir bendrai pateikti prašymai suteikti prieigą prie asmens duomenų yra susiję tik su nedideliu skaičiumi sekamų asmenų, palyginti su bendru duomenų srautu internete⁽⁸⁹⁾;
- (83) kalbant apie prieigą prie surinktų duomenų ir duomenų saugumo, PPD-28 reikalaujama, kad prieiga „būtų suteikiama tik įgaliotam personalui, kuriam informacija reikalinga misijos vykdymo tikslais“, ir kad asmens duomenys „turi būti tvarkomi ir saugomi laikantis sąlygų, kuriomis užtikrinama tinkama apsauga ir užkertamas kelias neteisėtai prieigai, laikantis neskkelbtinai informacijai taikytinų apsaugos priemonių“. Žvalgybos personalas gauna tinkamą ir pakankamą mokymą apie PPD-28 nustatytus principus⁽⁹⁰⁾;
- (84) galiausiai, kalbant apie asmens duomenų, kuriuos apie ES duomenų subjektus surinko JAV žvalgybos institucijos saugojimą ir tolesnį platinimą, PPD-28 nustatyta, kad su visais asmenimis (įskaitant ne JAV asmenis) turėtų būti elgiamasi oriai ir pagarbiai, kad visi asmenys turi teisėtus privatumo interesus tvarkant jų asmens duomenis ir kad dėl šios priežasties žvalgybos bendruomenės subjektai turi sukurti politiką, kurioje būtų numatytos tinkamos apsaugos priemonės, kurios padėtų „pagrįstai užtikrinti kuo mažesnę jų platinimą ir trumpesnę saugojimą“⁽⁹¹⁾;

⁽⁸⁷⁾ PLCOB ataskaitos 702 skirsnis, p. 111. Taip pat žr. ODNI pareiškimus (VI priedas), p. 9 („duomenų rinkimas pagal [FISA] 702 straipsnį nėra vykdomas masiškai ir plačiu mastu, bet yra konkrečiai orientuotas į užsienio žvalgybos duomenų rinkimą iš atskirų nustatytų teisėtų taikinių“) ir p. 13, 36 punktas (įskaitant nuorodą į 2014 m. FISC nuomonę); NSA CLPO, NSA užsienio žvalgybos akto 702 straipsnio įgyvendinimas, 2014 m. balandžio 16 d. NET ir įgyvendindama UPSTREAM programą NSA gali tik prašyti perimti elektroninius ryšius į sekamą įrenginį, iš jo arba elektroninius ryšius, susijusius su veikiančiu įrenginiu.

⁽⁸⁸⁾ ODNI pareiškimai (VI priedas), p. 18. Taip pat žr. p. 6, kuriame nurodyta, kad pagal taikytinas procedūras „matyti aiškus išipareigojimas užkirsti kelią savavališkam ir masiškam signalų žvalgybos informacijos rinkimui, ir aukščiausiu Vyriausybės lygmeniu įgyvendinti pagrįstumo principą“.

⁽⁸⁹⁾ Žr. Statistinę skaidrumo ataskaitą apie nacionalinio saugumo valdžios institucijų naudojimą, 2015 m. balandžio 22 d. Dėl bendro duomenų srauto internete žr., pvz., Pagrindinių teisių agentūra, Žvalgybos tarnybų priežiūra: pagrindinių teisių apsauga ir teisių gynimo priemonės ES (2015 m.), p. 15–16. Kalbant apie UPSTREAM programą, pažymėtina, kad pagal išslaptintą 2011 m. FISC nuomonę daugiau nei 90 % elektroninių ryšių, perimtų pagal FISA 702 straipsnį, buvo stebimi pagal PRISM programą, o mažiau nei 10 % – pagal UPSTREAM programą. Žr. FISC, rekomendacinė nuomonė, 2011 m., WL 10945618 (FISA Ct., 2011 10 3), 21 punktas (skelbiama adresu <http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf>).

⁽⁹⁰⁾ Žr. PPD-28 4 skirsnio 2 dalies ii punktą. Taip pat žr. ODNI, Visų žmonių asmens duomenų apsauga: Padėties ataskaita apie Prezidento politinėje direktyvoje Nr. 28 nustatytų procedūrų plėtojimą ir įgyvendinimą, 2014 m. liepos mėn., p. 5, pagal kurią „žvalgybos bendruomenės subjektų politika turėtų būti stiprinama galiojanti analizės praktika ir standartai, kuriais analitikai siekia struktūrizuoti užklausas arba kitus paieškos terminus ir būdus, kad nustatytų žvalgybos informaciją, kuri yra svarbi vykdant dabartinę žvalgybos arba teisėsaugos užduotį; užklausas apie asmenis orientuoti į žvalgybos informacijos kategorijas, susijusias su žvalgybos arba teisėsaugos reikalavimu; ir tikrinti kuo mažiau asmens duomenų, nesusijusių su žvalgybos arba teisėsaugos reikalavimais“. Žr., pvz., CŽV, signalų žvalgybos veikla, p. 5, FTB, Prezidento politinė direktyva Nr. 28, politika ir procedūros, p. 3. Pagal 2016 m. pažangos ataskaitą apie signalų žvalgybos reformą žvalgybos bendruomenės subjektai (įskaitant FTB, CŽV ir NSA) ėmėsi priemonių savo darbuotojams supažindinti su PPD-28 reikalavimais ir šiuo tikslu sukūrė naują mokymo politiką arba pakeitė esamą.

⁽⁹¹⁾ Remiantis ODNI pareiškimais, šie apribojimai taikomi nepaisant to, ar informacija buvo surinkta masiškai, ar tikslingai renkant duomenis, ir nepriklausomai nuo asmens pilietybės.

- (85) JAV Vyriausybė paaiškino, jog šis pagrįstumo reikalavimas reiškia, kad žvalgybos bendruomenės subjektai neturės nustatyti „bet kurios teoriškai įmanomos priemonės“, tačiau turės „suderinti savo veiksmus su praktiniais signalų žvalgybos veiklos poreikiais, kad apsaugotų teisėtus su privatumu ir pilietinėmis laisvėmis susijusius interesus“⁽⁹²⁾. Šiuo atžvilgiu, remiantis generalinio prokuroro patvirtintomis procedūromis, su ne JAV asmenimis bus elgiama taip pat kaip ir su JAV asmenimis⁽⁹³⁾;
- (86) pagal šias taisykles duomenys paprastai saugomi ne ilgiau nei penkerius metus, išskyrus atvejus, kai įstatyme yra konkreti nuostata arba galioja aiškus Nacionalinės žvalgybos direktoriaus sprendimas, priimtas atidžiai įvertinus su privatumu susijusias aplinkybes (t. y. atsižvelgiant į ODNI pilietinių laisvių apsaugos pareigūno, taip pat agentūros privatumo ir pilietinių laisvių pareigūnų nuomones), kad nuolatinis duomenų saugojimas atitinka nacionalinio saugumo interesą⁽⁹⁴⁾. Duomenis platinti galima tik tais atvejais, kai informacija yra susijusi su pagrindiniu duomenų rinkimo tikslu, todėl atitinka teisėtą užsienio žvalgybos arba teisės saugos reikalavimą⁽⁹⁵⁾;
- (87) remiantis JAV Vyriausybės pateiktais patikinimais, asmeninė informacija negali būti platinama vien todėl, kad atitinkamas asmuo nėra JAV asmuo, ir „signalų žvalgybos duomenys apie įprastą užsieniečio veiklą nebūtų laikoma užsienio žvalgybos duomenimis, kuriuos būtų galima platinti arba saugoti nuolat atsižvelgiant vien į tą faktą, nebent jis kitais atžvilgiais atitinka galiojantį užsienio žvalgybos reikalavimą“⁽⁹⁶⁾;
- (88) remdamasi tuo, kas išdėstyta, Komisija daro išvadą, kad Jungtinėse Amerikos Valstijose galioja taisyklės, kuriomis ribojamas bet koks kišimasis į asmenų, kurių asmens duomenys perduodami iš Sąjungos į Jungtines Amerikos Valstijas pagal ES ir JAV „privatumo skydą“, pagrindines teises nacionalinio saugumo tikslais tiek, kiek tai griežtai būtina siekiant atitinkamo teisėto tikslo;
- (89) kaip matyti iš atliktos analizės, JAV teisėje užtikrinama, kad stebėjimo priemonės būtų naudojamos tik siekiant gauti užsienio žvalgybos informaciją, – o tai yra teisėtas politinis tikslas⁽⁹⁷⁾, – ir kad tokios priemonės būtų kuo

⁽⁹²⁾ Žr. ODNI pareiškimus (VI priedas).

⁽⁹³⁾ Žr. PPD-28 4 skirsnio a dalies i punktą ir E.O. 12333.

⁽⁹⁴⁾ PPD-28 4 skirsnio a dalies i punktas; ODNI pareiškimai (VI priedas), p. 7. Pavyzdžiui, renkant informaciją pagal FISA 702 straipsnį, taikomos NSA FISC patvirtintos minimalios informacijos procedūros, kuriose paprastai nustatyta, kad metaduomenys ir neįvertintas PRISM programos turinys saugomi ne ilgiau nei penkerius metus, o UPSTREAM duomenys saugomi ne ilgiau nei dvejus metus. NSA laikosi šių saugojimo terminų naudodamasi automatizuota procedūra – surinkti duomenys ištrinami pasibaigus atitinkamam saugojimo terminui. Žr. NSA FISA 702 straipsnį, minimalios informacijos procedūrų 7 straipsnį ir 6 straipsnio a dalies 1 punktą; NSA CLPO, NSA užsienio žvalgybos stebėjimo akto 702 straipsnio įgyvendinimas, 2014 m. balandžio 16 d. Panašiai saugojimas pagal FISA 501 straipsnį (buvęs JAV patriotinio akto 215 straipsnis) yra ribojamas iki penkerių metų, nebent asmens duomenys sudaro dalį tinkamai patvirtintos platinamos užsienio žvalgybos informacijos, arba jeigu DOJ raštu pataria NSA, kad įrašams saugojimo pareiga taikoma iki bus baigta nagrinėjama arba numatoma nagrinėti byla. Žr. NSA, CLOP, *Transparency Report: The USA Freedom Act Business Records FISA Implementation*, 2016 m. sausio 15 d.

⁽⁹⁵⁾ Visų pirma pagal FISA 501 straipsnį (buvęs JAV patriotinio akto 215 straipsnis) asmeninė informacija gali būti platinama tik kovos su terorizmu tikslais arba kaip nusikaltimo įrodymas, pagal FISA 702 straipsnį informacija gali būti platinama tik jeigu yra galiojantis užsienio žvalgybos arba teisės saugos tikslas. Plg. NSA CLPO, NSA užsienio žvalgybos stebėjimo akto 702 straipsnio įgyvendinimas, 2014 m. balandžio 16 d.; *Transparency Report: The USA Freedom Act Business Records FISA Implementation*, 2016 m. sausio 15 d. Taip pat žr. NSA pilietinių laisvių ir privatumo apsauga vykdančią tikslinę SIGINT veiklą pagal vykdomąją įsaką 12333, 2014 m. spalio 7 d.

⁽⁹⁶⁾ ODNI pareiškimai (VI priedas), p. 7 (pateikiama nuoroda į Žvalgybos bendruomenės direktyvą (ICD) Nr. 203).

⁽⁹⁷⁾ Teisingumo Teismas išaiškino, kad nacionalinis saugumas yra teisėtas politinis tikslas. Žr. *Schrems*, 88 punktas. Tai pat žr. Sprendimo *Digital Rights Ireland* ir kiti 42–44 ir 51 punktus, kuriuose Teisingumo Teismas nurodė, kad kovos su sunkiais nusikaltimais, visų pirma organizuotu nusikalstamumu ir terorizmu, sėkmė gali labai priklausyti nuo šiuolaikinių tyrimo priemonių naudojimo. Be to, kitaip nei baudžiamųjų tyrimų atveju, kurie paprastai yra susiję su atsakomybės ir kaltės už praityje padarytus veiksmus nustatymu, žvalgybos veikloje dažnai daugiausia dėmesio skiriama nacionalinių grėsmių prevencijai, kol dar tokios grėsmės nepadarė žalos. Todėl tokiuose tyrimuose dažnai gali dalyvauti platesnis dalyvių (sekamų asmenų) ratas ir jie gali būti vykdomi platesnėje geografinėje teritorijoje. Plg. EŽTT *Weber ir Saravia prieš Vokietiją*, 2006 m. birželio 29 d. sprendimas, paraškos Nr. 54934/00, 105–118 punktai (dėl vadinamosios „strateginės stebėsenos“).

labiau pritaikytos prie užsienio žvalgybos veiklos. Visų pirma masinis duomenų rinkimas bus leidžiamas tik išimtiniais atvejais, kai tikslingai rinkti duomenų neįmanoma, be to, masiškai renkant duomenis bus taikomos papildomos apsaugos priemonės, kurios padės kuo labiau sumažinti renkamų duomenų kiekį ir apriboti vėlesnę prieigą prie jų (tokia prieiga turės būti tikslinga ir suteikiama tik konkrečiais tikslais);

- (90) Komisijos manymu, tai atitinka Teisingumo Teismo Schrems byloje nustatytą standartą, pagal kurį teisės akte, kuriuo ribojamos Chartijos 7 ir 8 straipsniais garantuojamos pagrindinės teisės, turi būti nustatytos privalomos „būtinios apsaugos priemonės“⁽⁹⁸⁾ ir tokiam teisės akte „griežta būtinybe neribojamas toks reglamentavimas, kuris apskritai leidžia saugoti visų asmenų, kurių duomenys buvo perduoti iš Sąjungos į Jungtines Amerikos Valstijas, visus asmens duomenis nediferencijuojant, nenustatant jokių apribojimų arba išimčių pagal siekiamą tikslą ir nenumatant objektyvių kriterijų, leidžiančių nubrėžti ribas valstybės institucijų prieigai prie duomenų ir jų vėlesniam naudojimui konkrečiais, griežtai ribojamais ir galinčiais pateisinti apribojimą, taikomą tiek prieigai prie šių duomenų, tiek jų naudojimui, tikslais“⁽⁹⁹⁾. Be to, taip pat nebus renkami ir saugomi visų asmenų duomenys be jokių apribojimų ir nebus suteikiama neribota prieiga prie tokių duomenų. Be to, Komisijos pateiktuose pareiškimuose, įskaitant garantiją, kad JAV signalų žvalgybos veikla yra susijusi tik su dalimi interneto ryšių, atmetama galimybė suteikti „visuotinę“ prieigą⁽¹⁰⁰⁾ prie elektroninių ryšių turinio;

3.1.2. Veiksminga teisinė apsauga

- (91) Komisija įvertino Jungtinėse Amerikos Valstijose taikomus priežiūros mechanizmus, atsižvelgdama į bet kokią JAV žvalgybos institucijų kišimąsi tvarkant asmens duomenis, perduotus į Jungtines Amerikos Valstijas, ir būdus, kuriais ES duomenų subjektai gali naudotis gindami savo teises;

Priežiūra

- (92) JAV žvalgybos bendruomenei taikomi įvairūs peržiūros ir priežiūros mechanizmai, kuriuos taiko visos trys valdžios šakos. Šiuos mechanizmus taiko vidaus ir išorės vykdomosios valdžios įstaigos, įvairūs Kongreso komitetai, taip pat teisminę priežiūrą vykdančios institucijos, kurios visų pirma vadovaujasi Užsienio žvalgybos stebėsenos aktu;
- (93) pirma, JAV valdžios institucijų vykdomai žvalgybos veiklai taikoma plataus masto vykdomosios valdžios priežiūra;
- (94) pagal PPD-28 4 skirsnio a dalies iv punktą žvalgybos bendruomenės subjektų politikoje ir procedūrose „numatomos tinkamos priemonės, kuriomis palengvinama apsaugos priemonių, kuriomis apsaugoma asmeninė informacija, įgyvendinimo priežiūra“⁽¹⁰¹⁾;

⁽⁹⁸⁾ Schrems 91 punktą, įskaitant papildomas nuorodas.

⁽⁹⁹⁾ Schrems, 93 punktą.

⁽¹⁰⁰⁾ Plg. Schrems 94 punktą.

⁽¹⁰¹⁾ Žr. ODNI, Visų žmonių asmens duomenų apsauga: Padėties ataskaita apie Prezidento politinėje direktyvoje Nr. 28 nustatytų procedūrų plėtojamą ir įgyvendinimą. Žr., pvz., CŽV, signalų žvalgybos veikla, p. 6 (atitiktis) FTB, Prezidento politinė direktyva Nr. 28, politika ir procedūros, III skirsnio A dalies 4 punktas, B dalies 4 punktas; NSA, PPD-28 4 skirsnio procedūras, 2015 m. sausio 12 d., 8.1 skirsnis, 8.6 skirsnio c dalis.

- (95) šiuo atžvilgiu nustatyta keletas priežiūros lygmenų, įskaitant pilietinių laisvių ar privatumo pareigūnus, generalinius inspektorius, ODNI Pilietinių laisvių ir privatumo biurą, PCLOB ir Prezidento žvalgybos priežiūros valdybą. Šias priežiūros funkcijas padeda vykdyti visose agentūrose dirbantis personalas ⁽¹⁰²⁾;
- (96) kaip paaiškino JAV Vyriausybė ⁽¹⁰³⁾, pilietinių laisvių ar privatumo pareigūnai, turintys priežiūros pareigas, dirba įvairiuose departamentuose, kurie turi pareigų žvalgybos srityje, ir žvalgybos agentūrose ⁽¹⁰⁴⁾. Nors šių pareigūnų konkretūs įgaliojimai kai kuriais atžvilgiais gali skirtis priklausomai nuo leidimus nustatančio įstatymo, paprastai šie įgaliojimai apima procedūrų, kurių paskirtis – užtikrinti, kad atitinkamas departamentas (agentūra) tinkamai atsižvelgtų į privatumo ir pilietinių laisvių aspektus ir nustatytų tinkamas procedūras, kurias taikant nagrinėjami asmenų, manančių, kad jų privatumas arba pilietinės laisvės buvo pažeistos, priežiūrą (o kai kuriais atvejais, panašiai kaip ir ODNI, jos gali turėti savarankiškus įgaliojimus tirti skundus) ⁽¹⁰⁵⁾). Todėl departamento/agentūros direktorius turi užtikrinti, kad pareigūnas gautų visą informaciją ir jam būtų suteikta prieiga prie visos medžiagos, kuri reikalinga jo funkcijoms vykdyti. Pilietinių laisvių ir privatumo pareigūnai periodiškai atsiskaito Kongresui ir PCLOB, įskaitant ataskaitas apie departamento/agentūros gautų skundų skaičių ir pobūdį, ir tokių skundų dalyko santrauką, atliktas peržiūras ir išnagrinėtas užklaudas bei pareigūno vykdytos veiklos poveikį ⁽¹⁰⁶⁾. Remiantis nacionalinių duomenų apsaugos institucijų vertinimu, vidaus priežiūra, kurią vykdo pilietinių laisvių arba privatumo pareigūnai, gali būti laikoma „pakankamai patikima“, net jei mano, kad jie nėra pakankamai nepriklausomi ⁽¹⁰⁷⁾;
- (97) be to, kiekvienas žvalgybos bendruomenės subjektas turi savo generalinį inspektorių, kuris, be kita ko, turi pareigą prižiūrėti užsienio žvalgybos veiklą ⁽¹⁰⁸⁾. Tai reiškia, kad ODNI struktūroje veikia Generalinio inspektoriatas, turintis plačius įgaliojimus visos žvalgybos bendruomenės atžvilgiu ir leidimą tirti skundus arba informaciją, susijusią su kaltinimais neteisėtu elgesiu, piktnaudžiavimu tarnybine padėtimi, kiek tai susiję su ODNI ir (arba) žvalgybos bendruomenės programomis ir veikla ⁽¹⁰⁹⁾. Generaliniai inspektoriai pagal įstatymą yra nepriklausomi ⁽¹¹⁰⁾ padaliniai, atsakingi už auditą ir tyrimus, susijusius su atitinkamos agentūros vykdomomis programomis ir operacijomis nacionalinės žvalgybos tikslais, įskaitant piktnaudžiavimą teise ar jos pažeidimą ⁽¹¹¹⁾. Šie inspektoriai turi teisę susipažinti su visais įrašais, pranešimais, audito ataskaitomis, peržiūrų medžiaga, dokumentais, užrašais, rekomendacijomis ar kita svarbia medžiaga, įskaitant šiuo tikslu priimamą
-
- ⁽¹⁰²⁾ Pavyzdžiui, NSA Atitikties direktorate dirba daugiau nei 300 atitikties darbuotojų. Žr. ODNI pareiškimus (VI priedas), p. 7.
- ⁽¹⁰³⁾ Žr. ombudsmeno mechanizmo (III priedas) 6 straipsnio b dalies i–iii punktai.
- ⁽¹⁰⁴⁾ Žr. JAV kodekso 42 antraštinės dalies 2000ee-1 straipsnį. Tai, pvz., apima Valstybės departamentą, Teisingumo departamentą (įskaitant FTB), Vidaus saugumo departamentą, Gynybos departamentą, NSA, CŽV ir ODNI.
- ⁽¹⁰⁵⁾ Pasak JAV Vyriausybės, jeigu ODNI Pilietinių laisvių ir privatumo biuras gauna skundą, jis savo veiklą koordinuos ir su kitais žvalgybos bendruomenės subjektais, kad nustatytų, kaip žvalgybos bendruomenės subjektas turėtų toliau nagrinėti tą skundą. Žr. ombudsmeno mechanizmo (III priedas) 6 straipsnio b dalies ii punktą.
- ⁽¹⁰⁶⁾ Žr. JAV kodekso 42 antraštinės dalies 2000ee-1 straipsnio f dalies 1 ir 2 punktus.
- ⁽¹⁰⁷⁾ 29 straipsnio duomenų apsaugos darbo grupės nuomonė Nr. 01/2016 dėl ES ir JAV sprendimo dėl „privatumo skydo“ tinkamumo projekto (priimta 2016 m. balandžio 13 d.), p. 41.
- ⁽¹⁰⁸⁾ ODNI pareiškimai (VI priedas), p. 7. Žr., pvz., NSA, PPD-28 4 skirsnio procedūras, 2015 m. sausio 12 d., 8.1 skirsnį: CŽV, signalų žvalgybos veiklą, p. 7 (pareigos).
- ⁽¹⁰⁹⁾ Šį generalinį inspektorių (IG) (kurio pareigybė įsteigta 2010 m. spalio mėn.), skiria prezidentas pritarus Senatui, o iš pareigų jį gali atleisti tik prezidentas, bet ne DNI.
- ⁽¹¹⁰⁾ Šių generalinių inspektorių pareigybės yra nepriklausomoms ir juos atleisti gali tik prezidentas, kuris privalo Kongresui raštu nurodyti bet kurio tokio atleidimo priežastis. Tai nebūtinai reiškia, kad jie gali visiškai nepaisyti instrukcijų. Tam tikrais atvejais departamento direktorius gali drausti generaliniam inspektoriui inicijuoti, vykdyti arba užbaigti auditą arba tyrimą, kai manoma, kad tai būtina siekiant apsaugoti svarbius nacionalinius (saugumo) interesus. Tačiau Kongresą privaloma informuoti apie pasinaudojimą šiuo įgaliojimu ir šiuo pagrindu atitinkamas direktorius gali būti laikomas atsakingu. Žr., pvz., 1978 m. Generalinio inspektoriatas akto 8 straipsnį (Gynybos departamento generalinis inspektorius); 8E straipsnį (DOJ generalinis inspektorius); 8G straipsnio d dalies 2 punkto A, B papunkčius (NSA generalinis inspektorius); JAV kodekso 50 antraštinės dalies 403q straipsnio b dalis (CŽV generalinis inspektorius); 2010 fiskalinių metų Žvalgybos autorizavimo akto 405 straipsnio f dalis (žvalgybos bendruomenės generalinis inspektorius). Nacionalinių duomenų apsaugos institucijų vertinimu, generaliniai inspektoriai, tikėtina atitiks organizacinio nepriklausomumo kriterijus, kuriuos apibrėžė ESTT ir Europos Žmogaus Teisių Teismas (EŽTT), bent jau nuo to momento, kai visiems generaliniams inspektoriams bus taikoma nauja paskyrimo tvarka. Žr. 29 straipsnio duomenų apsaugos darbo grupės nuomonę Nr. 01/2016 dėl ES ir JAV sprendimo dėl „privatumo skydo“ tinkamumo projekto (priimta 2016 m. balandžio 13 d.), p. 40.
- ⁽¹¹¹⁾ Žr. ODNI pareiškimus (VI priedas), p. 7. Taip pat žr. 1978 m. Generalinio inspektoriatas aktą, 2014 m. liepos 7 d. Oficialusis leidinys Nr. 113–126.

administracinę potvarkį, be to, jie gali duoti parodymus⁽¹¹²⁾. Nors generaliniai inspektoriai gali priimti tik neprivalomo pobūdžio rekomendacijas dėl taisomųjų veiksmų, jų ataskaitos, įskaitant tolesnius veiksmus (arba jų nebuvimą), skelbiamos viešai, be to, siunčiamos Kongresui, kuris šiuo pagrindu gali vykdyti savo priežiūros funkciją⁽¹¹³⁾;

- (98) be to, Privatumo ir pilietinių laisvių priežiūros valdyba – nepriklausoma vykdomosios valdžios agentūra⁽¹¹⁴⁾, kurią sudaro Senato pritarimu prezidento šešerių metų kadencijai paskirta dvipartinė penkių narių valdyba⁽¹¹⁵⁾, – turi pareigų kovos su terorizmu politikos ir jos įgyvendinimo srityje privatumo ir pilietinių laisvių apsaugos požiūriu. Peržiūrėdama žvalgybos bendruomenės veiksmus, ji gali susipažinti su visais svarbiais agentūros įrašais, ataskaitomis, audito medžiaga, peržiūrų medžiaga, dokumentais, užrašais ir rekomendacijomis, įskaitant konfidencialią informaciją, rengti pokalbius ir išklausti parodymus. Ji gauna ataskaitas iš kelių federalinių departamentų (agentūrų) pilietinių laisvių ir privatumo pareigūnų⁽¹¹⁶⁾, gali teikti jiems rekomendacijas ir reguliarias ataskaitas Kongreso komitetams ir prezidentui⁽¹¹⁷⁾. PCLOB, atsižvelgiant į jos įgaliojimus, taip pat pavesta užduotis parengti PPD-28 įgyvendinimo vertinimo ataskaitą;
- (99) galiausiai pirmiau minėtus priežiūros mechanizmus papildo Prezidento patariamojoje žvalgybos valdyboje veikianti Žvalgybos priežiūros valdyba, kuri prižiūri, kaip JAV žvalgybos institucijos laikosi Konstitucijos ir visų taikomų taisyklių;
- (100) siekdami palengvinti priežiūrą, žvalgybos bendruomenės subjektai raginami kurti informacines sistemas, kurios leistų stebėti, įrašyti ir peržiūrėti užklausas arba kitas asmeninės informacijos paieškas⁽¹¹⁸⁾. Priežiūros ir atitikties įstaigos periodiškai tikrins praktiką, kurios žvalgybos bendruomenės subjektai laikosi saugodami asmeninę informaciją, esančią signalų žvalgyboje, ir jos atitiktį šioms procedūroms⁽¹¹⁹⁾;
- (101) be to, šios priežiūros funkcijos papildomos išsamiais ataskaitų teikimo reikalavimais, susijusiais su neatitiktimi. Visų pirma agentūroje taikomomis procedūromis turi būti užtikrinama, kad tais atvejais, kai kyla svarbus atitikties klausimas, susijęs su bet kurio asmens asmenine informacija, nepaisant jo pilietybės, surinktos naudojant signalų žvalgybą, apie tokį klausimą nedelsiant turi būti pranešama žvalgybos bendruomenės subjekto vadovui, kuris atitinkamai informuoja Nacionalinės žvalgybos direktorių, kuris pagal PPD-28 nustato, ar reikia imtis kokių nors taisomųjų veiksmų⁽¹²⁰⁾. Be to, pagal E.O. 12333 visi žvalgybos bendruomenės subjektai turi pareigą pranešti Žvalgybos priežiūros valdybai apie reikalavimų nesilaikymo incidentus⁽¹²¹⁾. Šiais mechanizmais

⁽¹¹²⁾ Žr. 1978 m. Generalinio inspektoriaus aktą, 6 straipsnis.

⁽¹¹³⁾ Žr. ODNI pareiškimus (VI priedas), p. 7. Taip pat žr. 1978 m. Generalinio inspektoriaus aktą, 4 straipsnio 5 dalis, 5 straipsnis. Pagal 2010 fiskalinių metų Žvalgybos autorizavimo akto 405 straipsnio b dalies 3, 4 punktus, 2010 m. spalio 7 d. Oficialusis leidinys Nr. 111–259, žvalgybos bendruomenės generalinis inspektorius informuos DNI ir Kongresą apie taisomųjų veiksmų būtinybę ir pažangą.

⁽¹¹⁴⁾ Remiantis nacionalinių duomenų apsaugos institucijų vertinimu, PCLOB praeityje „įrodė, kad ji įgaliojimais naudojasi nepriklausomai“. Žr. 29 straipsnio duomenų apsaugos darbo grupės nuomonę Nr. 01/2016 dėl ES ir JAV sprendimo dėl „privatumo skydo“ tinkamumo projekto (priimta 2016 m. balandžio 13 d.), p. 42.

⁽¹¹⁵⁾ Be to, PCLOB dirba apytiksliai 20 nuolatinių darbuotojų. Žr. <https://www.pclob.gov/about-us/staff.html>.

⁽¹¹⁶⁾ Tai apima bent jau Teisingumo departamentą, Gynybos departamentą, Vidaus saugumo departamentą, Nacionalinės žvalgybos direktorių ir Centrinę žvalgybos agentūrą, taip pat bet kurią kitą departamentą, agentūrą arba vykdomosios valdžios subjektą, kurį PCLOB paskyrė kaip tinkamą veikti tam tikroje teritorijoje.

⁽¹¹⁷⁾ Žr. JAV kodekso 42 antraštinės dalies 2000ee straipsnį. Taip pat žr. ombudsmeno mechanizmą (III priedas), 6 straipsnio b dalies IV punktą. Be kita ko, reikalaujama, kad PCLOB praneštų, kai vykdomosios valdžios agentūra atsisako vadovautis jos rekomendacijomis.

⁽¹¹⁸⁾ Žr. ODNI, Visų žmonių asmens duomenų apsauga: padėties ataskaita apie Prezidento politinėje direktyvoje Nr. 28 nustatytų procedūrų plėtojimą ir įgyvendinimą.

⁽¹¹⁹⁾ Ten pat, p. 8. Taip pat žr. ODNI pareiškimus (VI priedas), p. 9.

⁽¹²⁰⁾ Žr. ODNI, Visų žmonių asmens duomenų apsauga: Padėties ataskaita apie Prezidento politinėje direktyvoje Nr. 28 nustatytų procedūrų plėtojimą ir įgyvendinimą. Žr., pvz., NSA, PPD-28 4 skirsnio procedūras, 2015 m. sausio 12 d., 7.3 skirsnį, 8.7 skirsnio c, d punktus; FTB, Prezidento politinės direktyvą Nr. 28, politiką ir procedūras, III skirsnio A dalies 4 punktą, B dalies 4 punktą; CŽV, signalų žvalgybos veiklą, p. 6 (atitiktis) ir p. 8 (pareigos).

⁽¹²¹⁾ Žr. E.O. 12333 1.6 skirsnio c dalį.

užtikrinama, kad klausimas žvalgybos bendruomenėje būtų sprendžiamas aukščiausiu lygmeniu. Jeigu klausimas susijęs su ne JAV asmeniu, Nacionalinės žvalgybos direktorius, pasikonsultavęs su valstybės sekretoriumi ir pranešimą pateikęs departamentui arba agentūros direktoriumi, nustato, ar reikėtų imtis atitinkamos užsienio Vyriausybės informavimo veiksmų, suderinamų su šaltinių ir metodų, ir JAV personalo apsauga ⁽¹²²⁾;

- (102) antra, be šių vykdomosios valdžios priežiūros mechanizmų, JAV Kongresas, t. y. Atstovų Rūmų ir Senato žvalgybos ir teismų komitetai, turi pareigą prižiūrėti visą JAV užsienio žvalgybos veiklą, įskaitant JAV signalų žvalgybą. Pagal Nacionalinio saugumo aktą „prezidentas užtikrina, kad Kongreso žvalgybos komitetai būtų išsamiai ir nuolat informuojami apie Jungtinių Amerikos Valstijų žvalgybos veiklą, įskaitant visus numatomus svarbius žvalgybos veiksmus, kaip reikalaujama pagal šį poskirsnį“ ⁽¹²³⁾. Be to, „prezidentas užtikrina, kad apie bet kurią neteisėtą žvalgybos veiklą nedelsiant būtų pranešama Kongreso žvalgybos komitetams, taip pat būtų pranešama apie visus taisomuosius veiksmus, kurių buvo imtasi arba kurių planuojama imtis dėl tokios neteisėtos veiklos“ ⁽¹²⁴⁾. Šių komitetų nariai turi prieigą prie išlaptintos informacijos, taip pat žvalgybos metodų ir programų ⁽¹²⁵⁾;

- (103) vėliau priimtuose įstatymuose ataskaitų teikimo reikalavimai buvo praplėsti ir patikslinti tiek dėl žvalgybos bendruomenės subjektų, tiek dėl atitinkamų generalinių inspektorių ir generalinio prokuroro. Pavyzdžiui, FISA reikalaujama, kad generalinis prokuroras išsamiai informuotų Senato ir Atstovų Rūmų žvalgybos ir teismų komitetus apie Vyriausybės veiklą pagal tam tikrus FISA straipsnius ⁽¹²⁶⁾. Jame taip pat reikalaujama, kad Vyriausybė teiktų Kongreso komitetams „visų Užsienio žvalgybos stebėjimo teismo arba Apeliacinio užsienio žvalgybos stebėjimo teismo sprendimų, nutarimų ar nuomonių kopijas arba sprendimų, nutarimų ir nuomonių, kuriose pateikiamas svarbus FISA nuostatų aiškinimas, kopijas“. Visų pirma kalbant apie priežiūrą pagal FISA 702 straipsnį, ji vykdoma žvalgybos ir teismų komitetams teikiant įstatyme nustatytas ataskaitas, taip pat reguliariai rengiant trumpus informacinius susitikimus ir posėdžius. Tai apima kas pusę metų generalinio prokuroro teikiamas ataskaitas, kuriose aprašomas FISA 702 straipsnio taikymas ir prie kurių pridedami patvirtinamieji dokumentai, visų pirma Teisingumo departamento ir ODNI atitikties ataskaitos, bet kokių reikalavimų nesilaikymo incidentų aprašymus ⁽¹²⁷⁾ ir atskirą kas pusę metų generalinio prokuroro teikiamą vertinimą ir DNI dokumentaciją dėl sekamų asmenų nustatymo ir minimalios informacijos procedūrų, kurių paskirtis – užtikrinti, kad duomenys būtų renkami teisėtu užsienio žvalgybos tikslu, atitikties ⁽¹²⁸⁾. Kongresas taip pat gauna generalinių inspektorių, turinčių įgaliojimus vertinti, kaip agentūros laikosi sekamų asmenų nustatymo ir minimalios informacijos procedūrų ir generalinio prokuroro gairių, ataskaitas;

- (104) pagal 2015 m. JAV laisvės aktą JAV Vyriausybė kasmet privalo atskleisti Kongresui (ir visuomenei) prašymų dėl FISA nutarimų ir direktyvų ir patenkintų prašymų skaičių, taip pat JAV ir ne JAV asmenų, kurie yra stebimi, apytikslį skaičių ⁽¹²⁹⁾. Akte taip pat reikalaujama teikti papildomą viešą informaciją apie išduotų NSL dėl JAV ir ne

⁽¹²²⁾ PPD-28 skirsnį, 4 skirsnio a dalies iv punktą.

⁽¹²³⁾ Žr. 501 straipsnio a dalies 1 punktą (JAV kodekso 50 antraštinės dalies 413 straipsnio a dalies 1 punktą). Šioje nuostatoje įtvirtinti bendrieji reikalavimai, susiję su Kongreso vykdoma priežiūra nacionalinio saugumo srityje.

⁽¹²⁴⁾ Žr. 501 straipsnio b dalies (JAV kodekso 50 antraštinės dalies 413 straipsnio b dalis).

⁽¹²⁵⁾ Plg. 501 straipsnio d dalį (JAV kodekso 50 antraštinės dalies 413 straipsnio d dalis).

⁽¹²⁶⁾ Žr. JAV kodekso 50 antraštinės dalies 1808, 1846, 1862, 1871 ir 1881f straipsnius.

⁽¹²⁷⁾ Žr. JAV kodekso 50 antraštinės dalies 1881f straipsnį.

⁽¹²⁸⁾ Žr. JAV kodekso 50 antraštinės dalies 1881a straipsnio l dalies 1 punktą.

⁽¹²⁹⁾ Žr. 2015 m. JAV laisvės aktą, Oficialusis leidinys Nr. 114–23, 602 straipsnio a punktas. Be to, pagal 402 straipsnį „Nacionalinės žvalgybos direktorius, pasikonsultavęs su generaliniu prokuroru, atlieka kiekvieno Užsienio žvalgybos stebėjimo teismo arba Apeliacinio užsienio žvalgybos stebėjimo teismo priimto sprendimo, nutarties arba nuomonės, kurioje pateikiamas svarbus bet kurios teisės nuostatos vertinimas arba aiškinimas, įskaitant bet kokią naują ar svarbų sąvokos „konkreči atrankos sąlyga“ vertinimą arba aiškinimą, išslaptinimo peržiūrą (kaip apibrėžta 601 straipsnio e dalyje) ir, atsižvelgdamas į šios peržiūros rezultatus, kiekvieną tokį sprendimą, nutartį ar nuomonę skelbia viešai ir kuo išsamiau“.

JAV asmenų skaičių (kartu FISA nutarčių ir pažymėjimų gavėjams, taip pat NSL prašymams išduoti skaidrumo ataskaitas tam tikromis sąlygomis) ⁽¹³⁰⁾;

- (105) trečia, FISA pagrįsta JAV valdžios institucijų žvalgybos veikla leidžia FISA teismui (FISC) ⁽¹³¹⁾, t. y. nepriklausomam teismui ⁽¹³²⁾, kurio sprendimus galima ginčyti Apeliaciniame užsienio žvalgybos teisme (FISCR) ⁽¹³³⁾ ir galiausiai Jungtinių Amerikos Valstijų Aukščiausiąjame Teisme ⁽¹³⁴⁾, peržiūrėti priemones ir tam tikrais atvejais iš anksto duoti joms leidimą. Jeigu prašoma suteikti išankstinį leidimą, prašančiosios institucijos (FTB, NSA, CŽV ir pan.) turės Teisingumo departamento Nacionalinio saugumo departamento teisininkams pateikti prašymo projektą, o šie atidžiai patikrins jį ir prireikus paprašys pateikti papildomos informacijos ⁽¹³⁵⁾. Parengtą galutinį prašymą turės patvirtinti generalinis prokuroras, jo pavaduotojas arba nacionalinio saugumo generalinio prokuroro padėjėjas ⁽¹³⁶⁾. Tuomet Teisingumo departamentas pateiks prašymą FISC, kuris įvertins prašymą ir pateiks preliminarias rekomendacijas dėl tolesnių veiksmų ⁽¹³⁷⁾. Jeigu rengiamas posėdis, FISC turi įgaliojimus priimti parodymus, įskaitant, be kita ko, eksperto konsultaciją ⁽¹³⁸⁾;

- (106) FISC (ir FISCR) padeda nuolatinė penkių asmenų, turinčių kompetenciją spręsti nacionalinio saugumo ir su pilietinėmis laisvėmis susijusius klausimus, komisija ⁽¹³⁹⁾. Iš šios komisijos teismas paskiria asmenį, kuris veikia kaip *amicus curiae* ir padeda nagrinėti bet kokią paraišką dėl nutarties arba peržiūros, kurioje, teismo manymu, pateikiamas naujas arba svarbus teisės aiškinimas, išskyrus atvejus, kai teismas nustato, kad paskirti tokį asmenį nėra tikslinga ⁽¹⁴⁰⁾. Taip visų pirma užtikrinama, kad privatumo klausimai būtų tinkamai aptarti teismo vertinime. Teismas taip pat gali paskirti asmenį arba organizaciją, kuris (-i) veiktų kaip *amicus curiae*, įskaitant techninės konsultacijos teikimą, kai tai yra tinkama, arba paprašius suteiktų asmeniui arba organizacijai laiko *amicus curiae* laišku pateikti ⁽¹⁴¹⁾;

⁽¹³⁰⁾ JAV laisvės akto 602 straipsnio a punktas, 603 straipsnio a punktas.

⁽¹³¹⁾ Tam tikrų rūšių stebėjimo veiklą kitais atvejais gali vykdyti JAV magistrato teisėjas, kurį viešai paskyrė Jungtinių Amerikos Valstijų vyriausiasis teisėjas ir kuris gali turėti įgaliojimus nagrinėti prašymus ir priimti nutartis.

⁽¹³²⁾ FISC sudaro vienuolika Jungtinių Amerikos Valstijų vyriausiojo teisėjo paskirtų teisėjų iš JAV apygardų teismų teisėjų, kuriuos anksčiau paskyrė prezidentas ir patvirtino Senatas. Teisėjai, kurie į pareigas skiriami iki gyvos galvos ir gali būti atleisti tik dėl pagrįstos priežasties, FISC pareigas eina septynerius metus. FISA reikalaujama, kad teisėjai būtų atrinkti bent jau iš septynių skirtingų JAV teisminių apygardų. Žr. FISA 103 straipsnį (JAV kodekso 50 antraštinės dalies 1803 straipsnio a dalis; PCLOB ataskaitos 215 skirsnį, p. 174–187. Teisėjams padeda patyrę teismų raštinės darbuotojai, kurie veikia kaip teismo teisinis personalas ir rengia teisines analizes dėl prašymų rinkti duomenis. Žr. PCLOB ataskaitos 215 skirsnį, p. 178; JAV užsienio žvalgybos stebėjimo teismo pirmininko Reggie B. Waltonio laišką JAV Senato Teismų komiteto pirmininkui Patrickui J. Leahy (2013 m. liepos 29 d.) (Waltono laiškas), p. 2–3.

⁽¹³³⁾ FISCR sudaro trys Jungtinių Amerikos Valstijų vyriausiojo teisėjo paskirti teisėjai, parinkti iš JAV teismų ar apeliacinių teismų ir einantys pareigas nepertraukiamą septynerių metų terminą. Žr. FISA 103 straipsnį (JAV kodekso 50 antraštinės dalies 1803 straipsnio b punktas).

⁽¹³⁴⁾ Žr. JAV kodekso 50 antraštinės dalies 1803 straipsnio b punktą, 1861 straipsnio a dalies f punktą, 1881 straipsnio a dalies h punktą, 1881 straipsnio a dalies i punkto 4 papunktį.

⁽¹³⁵⁾ Pavyzdžiui, papildomi faktiniai duomenys apie stebėjimo objektą, techninė informacija apie metodiką arba patikrinimai dėl to, kaip gauta informacija bus naudojama ir platinama. Žr. PCLOB ataskaitos 215 skirsnį, p. 177.

⁽¹³⁶⁾ JAV kodekso 50 antraštinės dalies 1804 straipsnio a dalis, 1801 straipsnio g dalis.

⁽¹³⁷⁾ FISC gali patvirtinti paraišką, prašymą pateikti papildomą informaciją, nustatyti, ar būtina rengti posėdį, arba nurodyti galimą paraiškos atmetimo priežastį. Remdamasi šiuo preliminarium sprendimu, Vyriausybė pateiks galutinę paraišką. Joje, atsižvelgiant į teisėjo preliminarį pastabas, gali būti padaryti esminiai pradinės paraiškos pakeitimai. Nors FISCR patvirtina didelę galutinių paraiškų dalį (skaiciuojant procentais), daugumoje šių paraiškų būna padaryti esminiai pakeitimai, palyginti su pradinėmis paraiškomis, pvz., 24 % patvirtintų paraiškų 2013 m. liepos–rugsėjo mėn. Žr. PCLOB ataskaitos 215 skirsnį, p. 179, Waltonio raštą, p. 3.

⁽¹³⁸⁾ PCLOB ataskaitos 215 skirsnį, p. 179, Nr. 619.

⁽¹³⁹⁾ JAV kodekso 50 antraštinės dalies 1803 straipsnio i dalies 1 punktas ir 3 punkto A papunktis. Šiuo nauju teisės aktu įgyvendintos PCLOB rekomendacijos sutelkti būrį privatumo ir pilietinių laisvių ekspertų, kurie veiktų kaip *amicus curiae* ir iš anksto pateiktų teismui teisinius argumentus, susijusius su privatumu ir pilietinėmis laisvėmis. Žr. PCLOB ataskaitos 215 skirsnį, p. 183–187.

⁽¹⁴⁰⁾ JAV kodekso 50 antraštinės dalies 1803 straipsnio i dalies 2 punkto A papunktis. Remiantis ODNĮ pateikta informacija, tokie pareigūnai jau paskirti. Žr. signalų žvalgybos reformą, 2016 m. pažangos ataskaitą.

⁽¹⁴¹⁾ JAV kodekso 50 antraštinės dalies 1803 straipsnio i dalies 2 punkto B papunktis.

- (107) kalbant apie du teisinius leidimus vykdyti stebėjimą pagal FISA, kurie yra svarbiausi duomenų perdavimo pagal ES ir JAV „privatumo skydą“, FISC vykdoma priežiūra yra skirtinga;
- (108) pagal FISA 501 straipsnį ⁽¹⁴²⁾, kuriuo leidžiama rinkti „bet kokius materialius daiktus (įskaitant knygas, užrašus, dokumentus ir kitus daiktus)“, FISC pateiktame prašyme turi būti nurodomi faktai, iš kurių pagrįstai galima manyti, kad ieškomi daiktai yra susiję su sankcionuotu tyrimu (išskyrus grėsmės vertinimą), kuris atliktas siekiant gauti užsienio žvalgybos informaciją apie JAV asmenį arba apsisaugoti nuo tarptautinio terorizmo arba neteisėtos žvalgybos veiklos. Be to, taikant FISA būtina išvardyti generalinio prokuroro patvirtintas minimalios informacijos procedūras, susijusias su surinktų žvalgybos duomenų saugojimu ir platinimu ⁽¹⁴³⁾;
- (109) priešingai, pagal FISA 702 straipsnį ⁽¹⁴⁴⁾ FISC neleidžia taikyti individualių stebėjimo priemonių; tiesą sakant, jis suteikia leidimus įgyvendinti stebėjimo programas (pvz., PRISM, UPSTREAM) remdamasis metiniais pažymėjimais, kuriuos parengė generalinis prokuroras ir Nacionalinės žvalgybos direktorius. Pagal FISA 702 straipsnį leidžiama sekti asmenis, kurie, kaip pagrįstai manoma, yra už Jungtinių Amerikos Valstijų ribų, kad įgytų užsienio žvalgybos informacijos ⁽¹⁴⁵⁾. Tokį sekimą NSA vykdo dviem etapais. Pirma, analitikai nustatys ne JAV asmenis, esančius užsienyje, kurių stebėjimas, atsižvelgiant į analitiko vertinimą, reikš atitinkamą užsienio žvalgybą, nurodomą pažymėjime. Antra, nustačius šiuos konkrečius asmenis ir, pritaikius išsamias peržiūros NSA procedūras ⁽¹⁴⁶⁾, patvirtinus jų sekimą, bus pradėta naudoti (t. y. parengta ir įjungta) sekimo įranga (pvz., e. pašto adresai) ⁽¹⁴⁷⁾. Kaip nurodyta, pažymėjimuose, kuriuos tvirtins FISC, nėra informacijos apie individualius asmenis, kurie bus sekami, vietoj to nustatomos užsienio žvalgybos informacijos kategorijos ⁽¹⁴⁸⁾. Nors FISC, atsižvelgdamas į pagrįstą tikimybę arba kitą standartą, nevertina, ar asmenys tinkamai sekami siekiant gauti užsienio žvalgybos informacijos ⁽¹⁴⁹⁾, vykdydamas kontrolę jis vadovaujasi sąlyga, kad „svarbus sekimo tikslas – gauti užsienio žvalgybos informacijos“ ⁽¹⁵⁰⁾. Tiesą sakant, pagal FISA 702 straipsnį NSA leidžiama rinkti duomenis apie ne JAV asmenų, esančių užsienyje, ryšius tik jeigu galima pagrįstai manyti, kad atitinkamos ryšio priemonės naudojamos užsienio žvalgybos informacijai perduoti (pvz., su tarptautiniu terorizmu, branduolinių ginklų platinimu arba priešiškomis elektroninėmis atakomis susijusi informacija). Šiuo atžvilgiu priimtiems sprendimams gali būti taikoma teisminė peržiūra ⁽¹⁵¹⁾. Pažymėjimuose taip pat reikia aptarti asmenų sekimo ir minimalios informacijos procedūras ⁽¹⁵²⁾. Generalinis prokuroras ir Nacionalinės žvalgybos direktorius tikrina, kaip laikomasi

⁽¹⁴²⁾ JAV kodekso 50 antraštinės dalies 1861 straipsnis.

⁽¹⁴³⁾ JAV kodekso 50 antraštinės dalies 1861 straipsnio b punktas.

⁽¹⁴⁴⁾ JAV kodekso 50 antraštinės dalies 1881 straipsnis.

⁽¹⁴⁵⁾ JAV kodekso 50 antraštinės dalies 1881a straipsnio a punktas.

⁽¹⁴⁶⁾ PCLOB ataskaitos 702 skirsnis, p. 46.

⁽¹⁴⁷⁾ JAV kodekso 50 antraštinės dalies 1881a straipsnio h punktas.

⁽¹⁴⁸⁾ JAV kodekso 50 antraštinės dalies 1881a straipsnio g punktas. Pagal PCLOB šios kategorijos iš esmės yra susijusios su tarptautiniu terorizmu ir tokiomis temomis kaip masinio naikinimo ginklų įsigijimas. Žr. PCLOB ataskaitos 702 skirsnį, p. 25.

⁽¹⁴⁹⁾ PCLOB ataskaitos 702 skirsnis, p. 27.

⁽¹⁵⁰⁾ JAV kodekso 50 antraštinės dalies 1881a straipsnis.

⁽¹⁵¹⁾ *Liberty and Security in a Changing World*, Prezidento peržiūros grupės dėl žvalgybos ir ryšių technologijų ataskaita ir rekomendacijos, 2013 m. gruodžio 12 d., p. 152.

⁽¹⁵²⁾ JAV kodekso 50 antraštinės dalies 1881a straipsnio i dalis.

reikalavimų, o agentūros turi pareigą pranešti apie visus neatitikties incidentus FISC ⁽¹⁵³⁾ (taip pat Kongresui ir Prezidento žvalgybos priežiūros valdybai), kuris šiuo pagrindu gali daryti leidimo pakeitimus ⁽¹⁵⁴⁾;

- (110) be to, siekdama didinti FISC vykdomos priežiūros veiksmingumą, JAV Administracija nutarė įgyvendinti PCLOB rekomendaciją teikti FISC dokumentaciją, susijusią su pagal 702 straipsnį priimtais sprendimais dėl asmenų sekimo, įskaitant atsitiktinę užduočių lapų atranką, kad FISC būtų sudarytos sąlygos įvertinti, kaip užsienio žvalgybos tikslo reikalavimo laikomasi praktikoje ⁽¹⁵⁵⁾. Kartu JAV Administracija sutiko su priemonėmis ir jų ėmėsi, kad peržiūrėtų NSA asmenų sekimo procedūras ir geriau dokumentuotų sprendimų dėl asmenų sekimo užsienio žvalgybos tikslais motyvus ⁽¹⁵⁶⁾;

Individualios teisių gynimo priemonės

- (111) pagal JAV teisę ES duomenų subjektai gali pasinaudoti įvairiomis priemonėmis, jei mano, kad JAV žvalgybos bendruomenės subjektai tvarko (renka, tikrina ir pan.) jų asmens duomenis, ir, jeigu taip, ar laikosi JAV teisėje nustatytų apribojimų. Šios priemonės iš esmės taikomos trijose srityse: intervencija pagal FISA; neteisėta, tyčinė prieiga prie asmens duomenų, už kurią atsako Vyriausybės pareigūnai, ir prieiga prie informacijos pagal Informacijos laisvės aktą (FOIA) ⁽¹⁵⁷⁾;
- (112) pirma, Užsienio žvalgybos stebėjimo akte nustatytos įvairios teisių gynimo priemonės, kuriomis taip pat gali pasinaudoti ne JAV asmenys, kad ginčytų neteisėtą elektroninį stebėjimą. ⁽¹⁵⁸⁾ Tai reiškia asmenų galimybę pareikšti civilinį ieškinį Jungtinėms Amerikos Valstijoms dėl materialinių nuostolių atlyginimo, jeigu informacija apie juos buvo neteisėtai ir tyčia naudojama arba atskleista ⁽¹⁵⁹⁾; iškelti bylą JAV Vyriausybės pareigūnams, kaip asmenims, (pagal statutinę teisę) dėl materialinių nuostolių atlyginimo ⁽¹⁶⁰⁾, ir ginčyti stebėjimo teisėtumą (bei siekti panaikinti informaciją), jeigu JAV Vyriausybė ketina naudoti arba atskleisti bet kokią informaciją, gautą arba perimtą vykdant elektroninį asmens stebėjimą Jungtinėse Amerikos Valstijose nagrinėjamoje teisminėje arba administracinėje byloje ⁽¹⁶¹⁾;
- (113) antra, JAV Vyriausybė nurodė Komisijai įvairius papildomus būdus, kuriais ES duomenų subjektai galėtų pasinaudoti, siekdami teisinėmis priemonėmis apsiginti nuo Vyriausybės pareigūnų neteisėtos prieigos prie

⁽¹⁵³⁾ Pagal FISC darbo tvarkos taisyklių 13 taisyklės b punktą reikalaujama, kad Vyriausybė teismui pateiktų rašytinį pranešimą ir tai padarytų iš karto, kai tik nustato, kad bet kuris teismo suteiktas leidimas ar patvirtinimas buvo įgyvendintas nesilaikant teismo leidimo ar patvirtinimo, arba taikytinos teisės. Joje taip pat reikalaujama, kad Vyriausybė raštu praneštų faktus ir aplinkybes, susijusias su tokia neatitiktimi. Paprastai Vyriausybė galutinį pranešimą pagal 13 taisyklės a punktą pateikia iš karto, kai sužino atitinkamus faktus ir sunaikina bet kokius neteisėtai gautus duomenis. Žr. Walton'o laišką, p. 10.

⁽¹⁵⁴⁾ JAV kodekso 50 antraštinės dalies 1881 straipsnio I dalis. Taip pat žr. PCLOB ataskaitos 702 skirsnį, p. 66–76; NSA, CLPO, NSA Užsienio žvalgybos stebėjimo akto 702 straipsnio įgyvendinimas, 2014 4 16. Asmens duomenų rinkimui žvalgybos tikslais pagal FISA 702 skirsnį taikoma vykdomosios valdžios vykdoma vidaus ir išorės priežiūra. Be kita ko, atliekant vidaus priežiūrą, vadovaujamasi atitikties programomis, kurių paskirtis – įvertinti ir prižiūrėti, kaip laikomasi sekamų asmenų nustatymo ir minimalios informacijos procedūrų; ODNI, Teisingumo departamentui, Kongresui ir FISC pranešama apie vidinius ir išorės reikalavimų nesilaikymo incidentus ir šioms įstaigoms siunčiamos metinės peržiūros. Kalbant apie išorės priežiūrą, pažymėtina, kad ją iš esmės sudaro sekamų asmenų nustatymo ir minimalios informacijos peržiūros, kurias atlieka Kongresui ir FISC atskaitingi ODNI, DOJ ir generaliniai inspektoriai, įskaitant informavimą apie reikalavimų nesilaikymo incidentus. Apie svarbius reikalavimų nesilaikymo incidentus būtina nedelsiant pranešti FISC, o apie kitus incidentus teikiamos ketvirčio ataskaitos. Žr. PCLOB ataskaitos 702 skirsnį, p. 66–77.

⁽¹⁵⁵⁾ PCLOB, rekomendacijų vertinimo ataskaita, 2015 m. sausio 29 d., p. 20.

⁽¹⁵⁶⁾ PCLOB, rekomendacijų vertinimo ataskaita, 2015 m. sausio 29 d., p. 16.

⁽¹⁵⁷⁾ Be to, įslaptintos informacijos procedūrų įstatymo 10 straipsnyje nustatyta, kad bet kuriame baudžiamojo persekiojimo procese, kuriame Jungtinės Amerikos Valstijos privalo nustatyti, ar medžiaga prilygsta įslaptintai informacijai (pvz., dėl to, kad ji turi būti apsaugota nuo neteisėto atskleidimo dėl nacionalinio saugumo priežasčių), Jungtinės Amerikos Valstijos informuoja atsakovą apie medžiagos dalis, kuriomis, jos pagrįstu manymu, ieškovas remsis reikalaudamas nustatyti įslaptintos informacijos elementą.

⁽¹⁵⁸⁾ Šiuo atžvilgiu taip pat žr. ODNI pareiškimus (VI priedas), p. 16.

⁽¹⁵⁹⁾ JAV kodekso 18 antraštinės dalies 2712 straipsnis.

⁽¹⁶⁰⁾ JAV kodekso 50 antraštinės dalies 1810 straipsnis.

⁽¹⁶¹⁾ JAV kodekso 50 antraštinės dalies 1806 straipsnis.

asmens duomenų arba jų naudojimo, įskaitant tariamus nacionalinio saugumo tikslus (t. y. Kompiuterinio sukčiavimo ir piktnaudžiavimo aktas ⁽¹⁶²⁾; Elektroninių ryšių privatumo aktas ⁽¹⁶³⁾ ir Teisės į finansinį privatumą aktas ⁽¹⁶⁴⁾). Visi šie ieškinio pagrindai yra susiję su konkrečiais duomenimis, prieigos tikslais ir (arba) rūšimi (pvz., nuotolinė prieiga iš kompiuterio per internetą) ir yra taikomi tik tam tikromis sąlygomis (pvz., sąmoningas ar tyčinis elgesys, elgesys veikiant kaip privačiam asmeniui, patirta žala) ⁽¹⁶⁵⁾. Administracinių procedūrų akte (JAV kodekso 5 antraštinės dalies 702 straipsnis) nustatyta bendresnio pobūdžio galimybė ginti teises, pagal kurią „kiekvienas asmuo, kuris dėl institucijos veikimo patyrė teisinių padarinių arba nukentėjo nuo institucijos veikimo ar dėl tokio veikimo jo padėtis pablogėjo“, turi teisę kreiptis į teismą. Tai apima galimybę prašyti, kad teismas „institucijos veiksmus, nuomones ir išvadas, kurios <...> yra savavališkos, neteisingos, susijusios su piktnaudžiavimu įgaliojimais ar kitaip prieštarauja įstatymui, pripažintų neteisėtomis ir panaikintų“ ⁽¹⁶⁶⁾;

- (114) galiausiai JAV Vyriausybė nurodė, kad FOIA ne JAV asmenys gali naudotis kaip priemone, siekdami gauti prieigą prie esamų federalinių agentūros įrašų, įskaitant atvejus, kai juose yra asmens duomenų ⁽¹⁶⁷⁾. Atsižvelgiant į FOIA taikymo sritį, FOIA nenumatyti individualūs teisių gynimo nuo asmens duomenų ribojimo būdai, net jeigu tai iš esmės galėtų suteikti asmenims galimybę susipažinti su atitinkama informacija, kurią turi nacionalinės žvalgybos agentūros. NET ir šiuo atžvilgiu, atrodo, galimybės yra ribotos, nes agentūros gali nuslėpti informaciją, kuriai taikomos tam tikros išvardytos išimtys, įskaitant prieigą prie išlaptintos nacionalinio saugumo informacijos ir informacijos, susijusios su teisėsaugos tyrimais ⁽¹⁶⁸⁾. Todėl asmenys, kurie siekia administracinės ir teisminės peržiūros, gali ginčyti tai, kaip tokias išimtis naudoja nacionalinės žvalgybos agentūros;
- (115) todėl nors asmenys, įskaitant ES duomenų subjektus, gali pasinaudoti įvairiais teisių gynimo būdais, jei tapo neteisėto (elektroninio) stebėjimo nacionalinio saugumo tikslais aukomis, lygiai taip pat aišku, kad bent jau kai kurie teisiniai pagrindai, kuriuos JAV žvalgybos institucijos gali naudoti (pvz., E.O. 12333), nėra taikomi. Be to, net jeigu galimybėmis pasinaudoti teisminėmis teisių gynimo priemonėmis iš esmės gali pasinaudoti ir ne JAV asmenys, pvz., stebėjimas pagal FISA, prieinami ieškinio pareiškimo pagrindai yra riboti ⁽¹⁶⁹⁾, o asmenų (įskaitant JAV asmenis) pareikšti ieškiniai bus paskelbti nepriimtinais, jeigu negalima įrodyti jų pagrįstumo ⁽¹⁷⁰⁾, todėl galimybė kreiptis į bendrosios kompetencijos teismus yra ribota ⁽¹⁷¹⁾;
- (116) siekdama suteikti galimybę pasinaudoti papildomu teisių gynimo būdu, kuris būtų prieinamas visiems ES duomenų subjektams, JAV Vyriausybė nusprendė sukurti naują instituciją – ombudsmeną, kaip nustatyta JAV valstybės sekretoriaus rašte Komisijai, kuris prie šio sprendimo pridedamas kaip III priedas. Šiai institucijai pagal PPD-28 vadovauja Valstybės departamente (sekretoriaus pavaduotojo lygmeniu) paskirtas vyresnysis koordinatorius, kuris veikia kaip kontaktinis centras, ne tik sprendžiantis užsienio Vyriausybių iškeltus klausimus dėl JAV signalų žvalgybos veiklos, bet ir vykdamas daug įvairesnę veiklą, palyginti su pradine jo samprata;

⁽¹⁶²⁾ JAV kodekso 18 antraštinės dalies 1030 straipsnis.

⁽¹⁶³⁾ JAV kodekso 18 antraštinės dalies 2701–2712 straipsniai.

⁽¹⁶⁴⁾ JAV kodekso 12 antraštinės dalies 3417 straipsnis.

⁽¹⁶⁵⁾ ODNI pareiškimai (VI priedas), p. 17.

⁽¹⁶⁶⁾ JAV kodekso 5 antraštinės dalies 706 straipsnio 2 punkto A papunktis.

⁽¹⁶⁷⁾ JAV kodekso 5 antraštinės dalies 552 straipsnis. Panašūs įstatymai galioja valstijos lygmeniu.

⁽¹⁶⁸⁾ Tokiu atveju asmuo paprastai gauna tik standartinį atsakymą, kuriame agentūra atsisako patvirtinti arba paneigti bet kokių įrašų egzistavimo faktą. Žr. *ACLU v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

⁽¹⁶⁹⁾ Žr. ODNI pareiškimus (VI priedas), p. 16. Pagal pateiktus paaiškinimus ieškinius galima pareikšti dėl *nuostolių* (JAV kodekso 18 antraštinės dalies 2712 straipsnis; JAV kodekso 50 antraštinės dalies 1810 straipsnis) arba įrodžius, kad *Vyriausybė ketina naudoti arba atskleisti informaciją*, gautą arba perimtą elektroninėmis priemonėmis stebint atitinkamą asmenį prieš tą asmenį Jungtinėse Amerikos Valstijose nagrinėjamoje *teisminėje arba administracinėje byloje* (JAV kodekso 50 antraštinės dalies 1806 straipsnis). Tačiau, kaip ne kartą pažymėjo Teisingumo Teismas, siekiant nustatyti, ar pagrindinė teisė į privatumą ribojama, neturi reikšmės, ar atitinkamas asmuo patyrė kokių nors neigiamų pasekmių dėl tokio ribojimo. Žr. *Schrems*, 89 punktą, įskaitant papildomas nuorodas.

⁽¹⁷⁰⁾ Šis priimtinumų kriterijus kyla iš JAV Konstitucijos III straipsnyje nustatyto „bylos arba ginčo“ reikalavimo.

⁽¹⁷¹⁾ Žr. *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1144 (2013). Kalbant apie NSL naudojimą, pažymėtina, jog JAV laisvės akte (502 straipsnio f dalis – 503 straipsnis) nustatyta, kad neatskleidimo reikalavimai turi būti periodiškai peržiūrimi ir kad NSL *gavėjai* turi būti informuojami, kai nustoja galioti faktai, dėl kurių informacija neatskleidžiama (žr. ODNI pareiškimus (VI priedas), p. 13). Tačiau tai nereiškia, kad ES duomenų subjektas iš tikrųjų turėtų būti informuojamas, kad tapo tyrimo objektu.

- (117) visų pirma, atsižvelgdamas į JAV Vyriausybės įsipareigojimus, ombudsmenas užtikrins, kad individualūs skundai būtų tinkamai tiriami ir sprendžiami, ir kad asmenys gautų nepriklausomą patvirtinimą, jog JAV įstatymų buvo laikomasi, arba, jeigu tokie įstatymai buvo pažeisti, patvirtinimą, kad dėl įstatymų nesilaikymo susidariusi padėtis buvo ištaisyta⁽¹⁷²⁾. Ombudsmeno instituciją sudaro „privatumo skydo“ ombudsmenas, t. y. sekretoriaus pavaduotoja ir kiti darbuotojai, taip pat kitos priežiūros įstaigos, turinčios kompetenciją prižiūrėti įvairių žvalgybos bendruomenės subjektų veiklą, su kuriomis „privatumo skydo“ ombudsmenas bendradarbiaus nagrinėdamas skundus. Visų pirma tais atvejais, kai asmens prašymas yra susijęs su stebėjimo atitiktimi JAV teisei, „privatumo skydo“ ombudsmenas galės kliautis nepriklausomomis priežiūros institucijomis, kurios turi tyrimo įgaliojimus (pvz., generaliniai inspektoriai arba PCLOB). Kiekvienu atveju valstybės sekretorius užtikrina, kad ombudsmenas turėtų priemones, kurios leistų atsakymus į atskirų asmenų prašymus pagrįsti visa reikalinga informacija;
- (118) dėl šios sudėtinės struktūros ombudsmeno institucija garantuoja nepriklausomą priežiūrą ir individualų teisių gynimą. Be to, bendradarbiavimas su kitomis priežiūros institucijomis atveria galimybes pasinaudoti reikalinga patirtimi. Galiausiai „privatumo skydo“ ombudsmenui nustatyta pareiga užtikrinti reikalavimų laikymąsi arba ištaisyti su reikalavimų nesilaikymu susijusią padėtį, atspindi JAV Vyriausybės įsipareigojimą iš esmės nagrinėti ir spręsti ES asmenų skundus;
- (119) pirma, kitaip nei išimtinai Vyriausybių tarpusavio mechanizmas, „privatumo skydo“ ombudsmenas gaus individualius skundus ir atsakys į juos. Tokie skundai gali būti adresuojami valstybių narių priežiūros institucijoms, turinčioms kompetenciją prižiūrėti nacionalinio saugumo tarnybas ir (arba) asmens duomenų tvarkymą valdžios institucijose, kurios perduos juos centralizuotai ES institucijai, iš kurios jie bus persiųsti „privatumo skydo“ ombudsmenui⁽¹⁷³⁾. Tai, tiesą sakant, bus naudinga ES asmenims, kurie gimtąja kalba gali kreiptis į netoli jų gyvenamosios vietos esančią nacionalinę instituciją. Tokios institucijos pareiga bus padėti asmeniui pateikti prašymą „privatumo skydo“ ombudsmenui, kuriame nurodoma pagrindinė informacija, todėl skundas gali būti laikomas „išsamiu“. Asmuo neturi įrodyti, jog JAV Vyriausybė, vykdydama signalų žvalgybos veiklą, iš tikrųjų tikrino jo asmens duomenis;
- (120) antra, JAV Vyriausybė įsipareigoja užtikrinti, kad, vykdydamas savo funkcijas „privatumo skydo“ ombudsmenas galės kliautis bendradarbiavimu su kitomis pagal JAV teisę įkurtomis priežiūros ir atitikties peržiūros institucijomis. Kartais tai reikš bendradarbiavimą su nacionalinėmis žvalgybos institucijomis, visų pirma nustačius, kad prašyme pagal Informacijos laisvės aktą prašoma leisti susipažinti su dokumentais. Kitais atvejais, visų pirma, kai prašymai yra susiję su stebėjimo atitiktimi JAV teisei, bendradarbiaujama bus su nepriklausomomis priežiūros institucijomis (pvz., generaliniais inspektoriais), kurie atsako už tyrimų vykdymą ir turi įgaliojimus šioje srityje (visų pirma susipažindami su dokumentais ir prašydami pateikti informaciją ir padaryti pareiškimus), ir spręsti reikalavimų nesilaikymo bylas⁽¹⁷⁴⁾. Be to, „privatumo skydo“ ombudsmenas galės perduoti bylas PCLOB, kad ši jas išnagrinėtų⁽¹⁷⁵⁾. Jeigu reikalavimų nesilaikymo atvejį nustatė kuri nors iš šių priežiūros institucijų, atitinkamas žvalgybos bendruomenės subjektas (pvz., žvalgybos agentūra) turės ištaisyti su tuo susijusią padėtį, nes tik taip ombudsmenas, atsižvelgdamas į šiuo tikslu duotą JAV Vyriausybės įsipareigojimą, galės pateikti teigiamą

⁽¹⁷²⁾ Jeigu skundo pareiškėjas siekia susipažinti su JAV valdžios institucijų turimais dokumentais, taikomos Informacijos laisvės akte nustatytos taisyklės ir procedūros. Tai reiškia galimybę ginti savo teises teisme (o ne nepriklausomoje priežiūros institucijoje), jeigu prašymas pagal FOIA išdėstytas sąlygas atmetamas.

⁽¹⁷³⁾ Pagal ombudsmeno mechanizmo (III priedas) 4 skirsnio f dalį „privatumo skydo“ ombudsmenas tiesiogiai susisieks su ES individualių skundų nagrinėjimo įstaiga, kuri turės pareigą susisiekti su prašymą pateikiančiu asmeniu. Jeigu tiesioginiai ryšiai yra „pagrindinių procesų“ sudedamoji dalis, kuriuos taikant galima panaudoti prašomą teisių gynimo priemonę (pvz., FOIA prašymas leisti susipažinti su duomenimis, žr. 5 skirsnį), tie ryšiai bus palaikomi pagal taikytinas procedūras.

⁽¹⁷⁴⁾ Žr. ombudsmeno mechanizmo (III priedas) 2 dalies a punktą. Taip pat žr. (96)–(97) konstatuojamąsias dalis.

⁽¹⁷⁵⁾ Žr. ombudsmeno mechanizmo (III priedas) 2 dalies c punktą. Pagal JAV Vyriausybės pateiktus paaiškinimus PCLOB nuolat peržiūri už kovą su terorizmu atsakingų JAV valdžios institucijų politiką ir procedūras, taip pat tai, kaip jos įgyvendinamos, kad nustatytų, ar jų veiksmais „tinkamai apsaugomas privatumas ir pilietinės laisvės ir jie dera su taikomais įstatymais, taisyklėmis ir politika, susijusia su privatumu ir pilietinėmis laisvėmis“. Jis taip pat „gauna ir peržiūri atskaitas ir kitą informaciją iš privatumo pareigūnų ir pilietinių laisvių pareigūnų ir, kai tinkama, teikia jiems rekomendacijas dėl jų veiklos“.

atsakymą asmeniui (t. y. atsakymą, kuriame nurodoma, kad ištaisyta bet kokia su reikalavimų nesilaikymu susijusi padėtis). Be to, bendradarbiavimo srityje „privatumo skydo“ ombudsmenas bus informuojamas apie tyrimo rezultatus ir jam bus suteiktos priemonės, padėsiančios užtikrinti, kad jis gautų visą informaciją, kuri yra būtina atsakymui pateikti;

- (121) galiausiai „privatumo skydo“ ombudsmenas veiks nepriklausomai, todėl nesivadovaus JAV žvalgybos bendruomenės instrukcijomis⁽¹⁷⁶⁾. Tai yra labai svarbu, nes ombudsmenas turės patvirtinti, kad i) skundas buvo tinkamai ištirtas ir ii) kad atitinkamas JAV įstatymas, visų pirma įskaitant VI priede nustatytus apribojimus ir apsaugos priemones, buvo laikomasi arba, jeigu teisės nebuvo laikomasi, kad toks pažeidimas buvo ištaisytas. Kad turėtų galimybę teikti tą nepriklausomą patvirtinimą, „privatumo skydo“ ombudsmenas turės gauti būtiną informaciją, susijusią su tyrimu, kad galėtų įvertinti atsakymo į skundą tikslumą. Be to, valstybės sekretorius įsipareigojo užtikrinti, kad sekretoriaus pavaduotoja veiks kaip „privatumo skydo“ ombudsmenas ir tai darys nepriklausomai ir nepaisydamas jokios netinkamos įtakos, kuri gali daryti poveikį ombudsmeno sprendimui;
- (122) apskritai šiuo mechanizmu užtikrinama, kad asmenų skundai būtų išsamiai tiriami ir išsprendžiami, ir kad bent jau priežiūros srityje dalyvautų nepriklausomos priežiūros institucijos, turinčios reikalingą patirtį ir tyrimo įgaliojimus, ir ombudsmenas, kuris savo funkcijas galės vykdyti nepriklausomai nuo netinkamos, visų pirma politinės įtakos. Be to, asmenys skundus galės pateikti net ir neįrodę, kad jie buvo stebimi, arba tiesiog nurodę stebėjimo požymius⁽¹⁷⁷⁾. Atsižvelgdama į šias aplinkybes, Komisija yra įsitikinusi, kad šiuo atveju galioja tinkamos ir veiksmingos apsaugos nuo piktnaudžiavimo garantijos;
- (123) remdamasi tuo, kas išdėstyta, Komisija daro išvadą, kad Jungtinės Amerikos Valstijos užtikrina veiksmingą teisinę apsaugą nuo žvalgybos institucijų kišimosi į asmenų, kurių duomenys perduoti iš Sąjungos į Jungtines Amerikos Valstijas pagal ES ir JAV „privatumo skydą“, pagrindines teises;
- (124) šiuo atžvilgiu Komisija atkreipia dėmesį į Teisingumo Teismo sprendimą Schrems byloje, pagal kurį „reglamentavimu, nenumatančiu asmeniui jokios galimybės pasinaudoti teisių gynimo priemonėmis tam, kad gautų prieigą prie su juo susijusių asmens duomenų arba galėtų juos taisyti ar ištrinti, nepaisoma Chartijos 47 straipsnyje įtvirtintos pagrindinės teisės į veiksmingą teisminę gynybą esmės“⁽¹⁷⁸⁾. Atlikusi vertinimą, Komisija patvirtina, kad Jungtinėse Amerikos Valstijose galioja tokios teisinės teisių gynimo priemonės, įskaitant priemones, kurios taikomos sukūrus ombudsmeno instituciją. Ombudsmeno institucija vykdo nepriklausomą priežiūrą ir naudojasi tyrimo įgaliojimais. Atsižvelgiant į tai, kad Komisija nuolat stebi „privatumo skydą“, įskaitant bendrą metinę peržiūrą, kurioje taip pat dalyvauja ombudsmenas, šio mechanizmo veikimas bus dar kartą įvertintas;

3.2. JAV valdžios institucijų prieiga prie duomenų ir jų naudojimas teisėsaugos tikslais

- (125) kalbant apie asmens duomenų, perduotų pagal ES ir JAV „privatumo skydo“ sistemą teisėsaugos tikslais, perėmimą, pažymėtina, kad JAV Vyriausybė (per Teisingumo departamentą) pateikė patikinimą dėl taikomų apribojimų ir apsaugos priemonių, kurios, Komisijos vertinimu, užtikrina tinkamą apsaugos lygį;

⁽¹⁷⁶⁾ Žr. *Roman Zakharov prieš Rusiją*, 2015 m. gruodžio 4 d. sprendimas (Didžioji kolegija), paraiškos Nr. 47143/06, 275 punktas („nors iš esmės pageidautina priežiūros kontrolę pavesti teisėjui, neteisminių institucijų priežiūra gali būti laikoma suderinama su šia Konvencija, jeigu priežiūros institucija yra nepriklausoma nuo stebėjimo veiklą vykdančių institucijų ir jeigu jai suteikiami pakankami ir veiksmingi priežiūros įgaliojimai“).

⁽¹⁷⁷⁾ Žr. *Kennedy prieš Jungtinę Karalystę*, 2010 m. gegužės 18 d. sprendimas, paraiškos Nr. 26839/05, 167 punktas.

⁽¹⁷⁸⁾ *Schrems*, 95 punktas. Kaip aiškiai matyti iš sprendimo 91 ir 96 punktų, 95 punktas yra susijęs su apsaugos lygiu, kuris garantuojamas pagal Sąjungos teisinę tvarką, kurioje nustatyta, kad trečiosios šalies apsaugos lygis turi būti „iš esmės lygiavertis“. Pagal sprendimo 73 ir 74 punktus tai reiškia, kad apsaugos lygis arba priemonės, kuriomis gali pasinaudoti trečioji šalis, nebūtinai turi būti identiškos, tačiau naudojamų priemonių praktinis veiksmingumas turi būti įrodytas.

- (126) remiantis šia informacija, pagal JAV Konstitucijos Ketvirtąją pataisą ⁽¹⁷⁹⁾ teisėsaugos institucijos gali ieškoti asmenų ir juos areštuoti ⁽¹⁸⁰⁾ iš esmės remdamosi teismo išduotu orderiu ir įrodžiusios „pagrįstą tikimybę“. Keliais konkrečiai nustatytais ir išimtiniais atvejais, kai reikalavimas dėl orderio netaikomas ⁽¹⁸¹⁾, teisėsaugos institucijoms taikomas „pagrįstumo“ testas ⁽¹⁸²⁾. Paieškos arba arešto pagrįstumas „nustatomas, viena vertus, vertinant kišimosi į asmens privatumą mastą ir, kita vertus, laipsnį, kuriuo reikia užtikrinti teisėtų Vyriausybės interesų gynimą“ ⁽¹⁸³⁾. Tiksliau tariant, Ketvirtąją pataisą garantuojamas privatumas, orumas ir apsaugoma nuo savavališkų ir invazinių Vyriausybės pareigūnų veiksmų ⁽¹⁸⁴⁾. Šiomis koncepcijomis apibendrinama Sąjungoje taikoma būtinumo ir proporcingumo koncepcija. Kai tik teisėsaugos institucijai nebereikia naudoti areštuotų daiktų kaip įrodymų, jie turėtų būti grąžinami ⁽¹⁸⁵⁾;
- (127) nors teisė remtis Ketvirtąją pataisa netaikoma ne JAV asmenims, kurie negyvena Jungtinėse Amerikos Valstijose, tačiau jie vis tiek netiesiogiai naudojami šioje pataisoje nustatytais apsaugos priemonėmis, atsižvelgiant į tai, kad JAV bendrovės saugo asmens duomenis, o teisėsaugos institucijos bet kuriuo atveju turi gauti teismo leidimą (arba bent jau paisyti pagrįstumo reikalavimo) ⁽¹⁸⁶⁾. Papildomas apsaugos priemonės nustato specialios valdžios institucijos; šios priemonės taip pat nustatytos Teisingumo departamento gairėse, kuriomis teisėsaugos institucijų prieiga prie duomenų ribojama būtinumui ir proporcingumui lygiaverčiais pagrindais (pvz., reikalaujama, kad FTB naudotų kuo mažiau ribojančius įmanomus metodus ir atsižvelgtų į poveikį privatumui ir pilietinėms laisvėms) ⁽¹⁸⁷⁾. Pagal JAV Vyriausybės pateiktus pareiškimus ta pati arba didesnė apsauga taikoma teisėsaugos tyrimams, atliekamiems valstybės lygmeniu (dėl tyrimų, kurie atliekami pagal valstybės įstatymus) ⁽¹⁸⁸⁾;
- (128) išankstinis teismo arba didžiosios prisiekusiųjų žiuri (teisme naudojama tyrimo priemonė, kurią išrenka teisėjas arba magistratas) leidimas visais atvejais nėra reikalingas ⁽¹⁸⁹⁾, tačiau administraciniai potvarkiai priimami tik konkrečiais atvejais ir jiems gali būti taikoma nepriklausoma teisminė peržiūra, bent jau tais atvejais, kai Vyriausybė siekia vykdymo teisme ⁽¹⁹⁰⁾;

⁽¹⁷⁹⁾ Pagal Ketvirtąją pataisą „asmens teisė, kad būtų užtikrinta jų asmens, būsto, dokumentų ir turto apsauga nuo nepagrįstos kratos ar arešto, negali būti pažeidžiama, ir jokie orderiai, išskyrus pakankamu pagrindu pagrįstus orderius, pagrįsti priesaika arba patvirtinimu, ypač orderiai, kuriuose aprašoma apieškoma vieta ir asmenys arba areštuotini daiktai, negali būti išduodami“. Kratos orderius gali išduoti tik (magistrato) teisėjai. Federaliniai orderiai dėl elektroniniu būdu saugomos informacijos kopijavimo išduodami pagal Federalinių baudžiamojo proceso taisyklių 41 taisyklę.

⁽¹⁸⁰⁾ Aukščiausiasis Teismas ne kartą pabrėžė, kad krata be orderio gali būti atliekama tik „išimtiniais atvejais“. Žr., pvz., *Johnson v. United States*, 333 U.S. 10, 14 (1948); *McDonald v. United States*, 335 U.S. 451, 453 (1948); *Camara v. Municipal Court*, 387 U.S. 523, 528–29 (1967); *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 352–53, 355 (1977). Be to, Aukščiausiasis Teismas reguliariai pabrėžia, kad „šioje srityje galioja pagrindinė konstitucinė taisyklė, pagal kurią su teismo byla nesusijusios kratos, atliktos be išankstinio teisėjo arba magistrato leidimo, pačios savaime yra nepagrįstos pagal Ketvirtąją pataisą, išskyrus keletą konkrečių ir aiškiai apibrėžtų išimčių“. Žr., pvz., *Coolidge v. New Hampshire*, 403 U.S. 443, 454–55 (1971); *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 352–53, 358 (1977).

⁽¹⁸¹⁾ *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).

⁽¹⁸²⁾ PCLOB 215 skirsnis, p. 107, kuriame pateikiama nuoroda į bylą *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).

⁽¹⁸³⁾ PCLOB 215 skirsnis, p. 107, kuriame pateikiama nuoroda į bylą *Samson v. California*, 547 U.S. 843, 848 (2006).

⁽¹⁸⁴⁾ *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010), 2627.

⁽¹⁸⁵⁾ Žr., pvz., *United States v. Wilson*, 540 F.2d 1100 (D.C. Cir. 1976).

⁽¹⁸⁶⁾ Plg. *Roman Zakharov prieš Rusiją*, 2015 m. gruodžio 4 d. sprendimas (Didžioji kolegija), paraiškos Nr. 47143/06, 269 punktas, pagal kurį „reikalavimas ryšių paslaugų teikėjui prieš gaunant prieigą prie asmens ryšių parodyti leidimą perimti ryšius yra viena iš svarbiausių apsaugos nuo teisėsaugos institucijų piktnaudžiavimo priemonių, kuria užtikrinama, kad visais ryšių perėmimo atvejais būtų gaunamas tinkamas leidimas“.

⁽¹⁸⁷⁾ DOJ pareiškimai (VII priedas), p. 4, įskaitant papildomas nuorodas.

⁽¹⁸⁸⁾ DOJ pareiškimai (VII priedas), 2 dalis.

⁽¹⁸⁹⁾ Remiantis Komisijos gauta informacija ir nepaisant konkrečių sričių, kurios, tikėtina, nėra svarbios duomenų perdavimui pagal ES ir JAV „privatumo skydą“ (pvz., tyrimai dėl sukčiavimo sveikatos priežiūros srityje, vaiko išnaudojimo arba kontroliuojamų medžiagų bylos), minėti leidimai iš esmės yra susiję su tam tikrais pagal Elektroninių ryšių privatumo įstatymą (ECPA) suteiktais įgaliojimais, t. y. prašymai pateikti pagrindinę informaciją apie abonentą, ryšio seansus ir sąskaitas (JAV kodekso 18 antraštinės dalies 2703 straipsnio c dalies 1 ir 2 punktai, pvz., adresas, paslaugos rūšis ir (arba) trukmė) ir dėl senesnių nei 180 dienų e. laiško turinio atskleidimo (JAV kodekso 18 antraštinės dalies 2703 straipsnio a ir b dalys). Tačiau pastaruoju atveju atitinkamą asmenį reikia informuoti, todėl jis turi galimybę prašymą ginčyti teisme. Taip pat žr. DOJ apžvalgą, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 3 skyrius Saugomų ryšių aktas, p. 115–138.

⁽¹⁹⁰⁾ Pagal JAV Vyriausybės pareiškimus administracinių potvarkių gavėjai gali juos ginčyti teisme remdamiesi tuo, kad jie yra nepagrįsti, t. y. pertekliniai, neįvykdomi arba sukeliantys per didelę našą. Žr. DOJ pareiškimus (VII priedas), p. 2.

- (129) tą patį galima pasakyti apie administracinius potvarkius, priimamus atsižvelgiant į viešąjį interesą. Be to, pagal JAV Vyriausybės pareiškimus panašūs esminiai apribojimai taikomi tais atvejais, kai institucijos gali tik siekti gauti duomenis, susijusius su jų kompetencijai priklausančiais klausimais, ir privalo paisyti pagrįstumo standarto;
- (130) be to, JAV teisėje nustatyti įvairūs asmenims prieinami teisminiai teisių gynimo būdai, padedantys apsaugoti nuo asmens duomenis tvarkančios valdžios institucijos arba vieno iš jos pareigūnų. Būdais, kurie visų pirma nustatyti Administracinių procedūrų akte (APA), Informacijos laisvės akte (FOIA) ir Elektroninių ryšių privatumo akte (ECPA), gali pasinaudoti visi asmenys, nepaisant jų pilietybės ir atsižvelgiant į taikytinas sąlygas;
- (131) paprastai pagal Administracinių procedūrų aktą⁽¹⁹¹⁾, kiekvienas asmuo, kuris dėl institucijos veikimo patyrė teisinių padarinių arba nukentėjo nuo institucijos veikimo ar dėl tokio veikimo jo padėtis pablogėjo, turi teisę kreiptis į teismą⁽¹⁹²⁾. Tai apima galimybę prašyti, kad teismas „institucijos veiksmus, nuomones ir išvadas, kurios <...> yra savavališkos, neteisingos, susijusios su piktnaudžiavimu įgaliojimais ar kitaip prieštarauja įstatymui, pripažintų neteisėtomis ir panaikintų“⁽¹⁹³⁾;
- (132) konkrečiau, Elektroninių ryšių privatumo akto⁽¹⁹⁴⁾ II antraštinėje dalyje įtvirtinta įstatymu nustatytų privatumo teisių sistema, pagal kurią iš esmės reglamentuojama teisėsaugos institucijų prieiga prie laidinių, žodinių arba elektroninių ryšių turinio, kurį saugo trečiosios šalys paslaugų teikėjai⁽¹⁹⁵⁾. Šiuo aktu kriminalizuojama neteisėta (t. y. teismo nesankcionuota arba kitais būdais neleistina) prieiga prie tokių ryšių, o nukentėjusiam asmeniui suteikiama galimybė pareikšti civilinį ieškinį JAV federaliniame teisme dėl faktinių ir baudinių nuostolių, taip pat lygiavertės arba deklaratyvaus pobūdžio teisių gynimo priemonės taikymo Vyriausybės pareigūno, kuris sąmoningai įvykdė tokius neteisėtus veiksmus, arba Jungtinių Amerikos Valstijų atžvilgiu;
- (133) be to, pagal Informacijos laisvės aktą (FOIA, JAV kodekso 5 antraštinės dalies 552 straipsnis) kiekvienas asmuo turi teisę susipažinti su federalinės institucijos įrašais ir, išnaudojus administracines teisių gynimo priemones, įgyvendinti tokią teisę teisme, išskyrus atvejus, kai tokie įrašai nuo visuomenės saugomi taikant išimtį arba specialią teisėsaugos sąlygą⁽¹⁹⁶⁾;

⁽¹⁹¹⁾ JAV kodekso 5 antraštinės dalies 702 straipsnis.

⁽¹⁹²⁾ Paprastai teisminė peržiūra taikoma tik galutiniam institucijos veiksmui, o ne preliminarium, procesiniam ar tarpiniam veiksmui. Žr. JAV kodekso 5 antraštinės dalies 704 straipsnį.

⁽¹⁹³⁾ JAV kodekso 5 antraštinės dalies 706 straipsnio 2 punkto A papunktis.

⁽¹⁹⁴⁾ JAV kodekso 18 antraštinės dalies 2701–2712 straipsniai.

⁽¹⁹⁵⁾ ECPA apsaugomi ryšiai, kuriuos saugo dviejų apibūdintų klasių tinklo paslaugų teikėjai, t. y.: i) elektroninių ryšių, pvz., telefonijos arba e. pašto, paslaugų teikėjai, ii) nuotolinio duomenų apdorojimo paslaugų teikėjai, pvz., kompiuterinio saugojimo arba duomenų tvarkymo paslaugos.

⁽¹⁹⁶⁾ Vis dėlto šios išimtys yra konkrečios. Pavyzdžiui, pagal JAV kodekso 5 antraštinės dalies 552 straipsnio b dalies 7 punktą FOIA nustatytos teisės negalioja „teisėsaugos tikslais sudarytiems įrašams arba informacijai, išskyrus atvejus, kai tokių teisėsaugos įrašų ar informacijos sudarymas A) galėtų būti pagrįstai laikomas kaip trukdantis nagrinėti teisėsaugos bylą, B) atimtų asmeniui teisę į sąžiningą bylos nagrinėjimą arba nepriklausomą klausimo sprendimą teisme, C) galėtų būti pagrįstai laikomas neteisėtu kišimusi į asmens privatų gyvenimą, D) galėtų būti pagrįstai laikomas kaip atskleidžiančiu konfidencialaus informacijos šaltinio, įskaitant valstybės, vietos ar užsienio agentūrą ar instituciją arba bet kurią konfidencialią informaciją pateikusią privačią instituciją, tapatybę ir, jeigu įrašą arba informaciją parengė baudžiamosios justicijos institucija vykdydama baudžiamąjį tyrimą arba agentūra, kuri atlieka teisėtą nacionalinio saugumo žvalgybos tyrimą, konfidencialaus šaltinio pateiktą informaciją, E) atskleistų teisėsaugos tyrimų ar baudžiamojo persekiojimo būdus ir procedūras, arba atskleistų teisėsaugos tyrimų ir baudžiamojo persekiojimo rekomendacijas, jeigu pagrįstai tikėtina, kad toks informacijos atskleidimas galėtų būti naudingas apeinant įstatymus, arba F) galėtų būti pagrįstai laikomas kaip keliantis pavojų bet kurio asmens gyvybei arba fiziniam saugumui“. Be to, „kai pateikiamas prašymas leisti susipažinti su įrašais [kurių rengimas gali būti pagrįstai laikomas kaip kenkiantis teisėsaugos bylai] ir – A) tyrimas arba byla yra susijęs su galimu baudžiamosios teisės pažeidimu, ir B) yra pagrindas manyti, kad i) tyrimo arba bylos adresatas nežino apie vykstantį tyrimą arba bylą, ir ii) atskleidus informaciją apie sudarytą įrašą galima pagrįstai tikėtis, kad bus pakenkta teisėsaugos bylai, agentūra gali, jeigu neišnyksta minėtos aplinkybės, įrašams netaikyti šio straipsnio reikalavimų“. JAV kodekso 5 antraštinės dalies 552 straipsnio c dalies 1 punktas.

- (134) be to, keliuose kituose įstatymuose asmenims suteikiama teisė pareikšti ieškinį JAV valdžios institucijai arba pareigūnui dėl jų asmens duomenų tvarkymo; tai, pvz., pasakytina apie Slapto pokalbių pasiklausymo aktą ⁽¹⁹⁷⁾, Kompiuterinio sukčiavimo ir piktnaudžiavimo aktą ⁽¹⁹⁸⁾, Federalinį deliktinių reikalavimų aktą ⁽¹⁹⁹⁾, Teisės į finansinį privatumą aktą ⁽²⁰⁰⁾ ir Sąžiningo kreditinių ataskaitų sudarymo aktą ⁽²⁰¹⁾;
- (135) todėl Komisija daro išvadą, kad Jungtinėse Amerikos Valstijose galioja taisyklės, kuriomis ribojamas bet koks kišimasis į asmenų, kurių asmens duomenys perduodami iš Sąjungos į Jungtines Amerikos Valstijas pagal ES ir JAV „privatumo skydą“, pagrindines teises teisėsaugos ⁽²⁰²⁾ arba kito viešojo intereso tikslais tiek, kiek tai griežtai būtina siekiant atitinkamo teisėto tikslo, ir kad užtikrina veiksmingą teisinę apsaugą nuo tokio kišimosi;

4. TINKAMAS APSAUGOS LYGIS PAGAL ES IR JAV „PRIVATUMO SKYDĄ“

- (136) atsižvelgdama į šias išvadas, Komisija mano, kad Jungtinės Amerikos Valstijos užtikrina tinkamą asmens duomenų, kuriuos pagal ES ir JAV „privatumo skydą“ Sąjunga perdavė Jungtinių Amerikos Valstijų autosertifikuotoms organizacijoms, apsaugos lygį;
- (137) visų pirma Komisija mano, kad JAV komercijos departamento nustatytais privatumo principais iš tikrųjų užtikrinamas asmens duomenų apsaugos lygis, kuris iš esmės yra lygiavertis apsaugos lygiui, užtikrinamam Direktyvoje 95/46/EB nustatytais pagrindiniais principais;
- (138) be to, veiksmingas privatumo principų taikymas garantuojamas Komercijos departamento išipareigojimų skaidrumu ir „privatumo skydo“ sistemos administravimu;
- (139) Komisija taip pat mano, kad, atsižvelgiant į visas aplinkybes, „privatumo skydo“ sistemoje užtikrinama priežiūra ir nurodytos teisių gynimo institucijos sudaro sąlygas nustatyti „privatumo skydo“ organizacijų padarytus privatumo principų pažeidimus ir taikyti praktines bausmes bei suteikti teises teisių gynimo priemones duomenų subjektui, kad jis galėtų susipažinti su savo asmens duomenimis ir galiausiai panaikinti arba ištrinti tokius duomenis;
- (140) galiausiai, remdamasi prieinama informacija apie JAV teisinę tvarką, įskaitant JAV Vyriausybės pareiškimus ir išipareigojimus, Komisija mano, kad bet kokia išimtis, kurią JAV valdžios institucijos, siekdamos nacionalinio saugumo, teisėsaugos ar kitų viešojo intereso tikslų, taiko asmenų, kurių duomenys perduodami iš Sąjungos į Jungtines Amerikos Valstijas pagal „privatumo skydą“, pagrindinėms teisėms, ir iš to išplaukiantys autosertifikuotoms organizacijoms nustatyti privalomi apribojimai, susiję su privatumo principų laikymusi, galios tik tiek, kiek tai yra griežtai būtina siekiant atitinkamo teisėto tikslo ir jeigu taikant tokias išimtis galioja veiksminga teisinė apsauga;

⁽¹⁹⁷⁾ JAV kodekso 18 antraštinės dalies 2510 ir kiti straipsniai. Pagal Slapto pokalbių pasiklausymo aktą (JAV kodekso 18 antraštinės dalies 2520 straipsnis) asmuo, kurio laidiniai, žodiniai arba elektroniniai ryšiai perimami, atskleidžiam arba sąmoningai naudojami, gali pareikšti ieškinį dėl Slapto pokalbių pasiklausymo akto pažeidimo, įskaitant tam tikras aplinkybes, susijusias su atskiru Vyriausybės pareigūnu arba Jungtinėmis Amerikos Valstijomis. Dėl informacijos apie adresus ir kitos su turiniu nesusijusios informacijos (pvz., IP adresas, e. pašto adresas) rinkimo taip pat žr. 18 antraštinės dalies skyrių dėl renkamų numerių registratorių arba spąstų ir sekimo prietaisų (JAV kodekso 18 antraštinės dalies 3121–3127 straipsniai, o dėl civilinių ieškinių žr. 2707 straipsnį).

⁽¹⁹⁸⁾ JAV kodekso 18 antraštinės dalies 1030 straipsnis. Pagal Kompiuterių sukčiavimo ir piktnaudžiavimo aktą asmuo gali pareikšti ieškinį bet kuriam asmeniui dėl tyčinės neteisėtos prieigos (arba perteklinės neteisėtos prieigos), siekiant gauti informacijos iš finansų įstaigos, JAV Vyriausybės kompiuterinės sistemos arba kito konkretaus kompiuterio, įskaitant tokią prieigą tam tikromis aplinkybėmis, susijusiomis su atskiru Vyriausybės pareigūnu.

⁽¹⁹⁹⁾ JAV kodekso 28 antraštinės dalies 2671 ir kiti straipsniai. Pagal Federalinį deliktinių reikalavimų aktą asmuo tam tikromis aplinkybėmis gali pareikšti ieškinį Jungtinėms Amerikos Valstijoms dėl „bet kurio Vyriausybės pareigūno aplaidaus arba neteisėto veikimo arba neveikimo einant valstybės tarnautojo pareigas arba dirbant pagal darbo sutartį“.

⁽²⁰⁰⁾ JAV kodekso 12 antraštinės dalies 3401 ir kiti straipsniai. Pagal Teisės į finansinį privatumą aktą asmuo tam tikromis aplinkybėmis gali pareikšti ieškinį Jungtinėms Amerikos Valstijoms dėl saugomų finansinių įrašų gavimo arba atskleidimo pažeidžiant įstatymą. Vyriausybės prieiga prie saugomų finansinių įrašų paprastai draudžiama, išskyrus atvejus, kai Vyriausybė, remdamasi teisėtų potvarkiu arba kratos orderiu, pateikia prašymą arba, atsižvelgiant į tam tikrus apribojimus, pateikia oficialų rašytinį prašymą, o asmuo, kurio informacijos prašoma, gauna pranešimą apie tokį prašymą.

⁽²⁰¹⁾ JAV kodekso 15 antraštinės dalies 1681–1681x straipsniai. Pagal Sąžiningo kreditinių ataskaitų sudarymo aktą asmuo gali pareikšti ieškinį bet kuriam asmeniui, kuris nesilaiko reikalavimų (visų pirma reikalavimo turėti teisėtą leidimą), susijusių su vartotojo kredito ataskaitų rinkimu, skleidimu ir naudojimu, arba tam tikromis sąlygomis toks ieškinys gali būti pareikštas Vyriausybės įstaigai.

⁽²⁰²⁾ Teisingumo Teismas pripažino, kad teisėsaugos užtikrinimas yra teisėtas politinis tikslas. Žr. sujungtas bylas C-293/12 ir C-594/12, *Digital Rights Ireland ir kiti*, ES:C:2014:238, 42 punktą. Taip pat žr. EŽTK 8 straipsnio 2 dalį ir Europos Žmogaus Teisių Teismo sprendimą byloje *Weber ir Saravia prieš Vokietiją*, paraiškos Nr. 54934/00, 104 punktą.

- (141) Komisija daro išvadą, kad tai atitinka Direktyvos 95/46/EB 25 straipsnio standartus, kaip juos, atsižvelgdamas į Europos Sąjungos pagrindinių teisių chartiją, išaiškino Teisingumo Teismas, visų pirma Schrems sprendime;

5. DUOMENŲ APSAUGOS INSTITUCIJŲ VEIKSMAI IR KOMISIJAI TEIKIAMA INFORMACIJA

- (142) Schrems sprendime Teisingumo Teismas paaiškino, kad Komisija neturi jokios kompetencijos riboti DAI įgaliojimų, suteiktų pagal Direktyvos 95/46/EB 28 straipsnį (įskaitant įgaliojimą sustabdyti duomenų perdavimą), kai asmuo, pagal tą nuostatą pateikęs prašymą, nurodo aplinkybes, galinčias sukelti abejonių dėl Komisijos sprendimo dėl tinkamumo suderinamumo su pagrindine teise į privatumą ir duomenų apsaugą ⁽²⁰³⁾;
- (143) siekdamas užtikrinti veiksmingą „privatumo skydo“ veikimą, valstybės narės turėtų informuoti Komisiją apie susijusius DAI veiksmus;
- (144) be to, Teisingumo Teismas nurodė, kad pagal Direktyvos 95/46/EB 25 straipsnio 6 dalies antrą pastraipą valstybės narės ir jų institucijos privalo imtis priemonių, kurios yra būtinos siekiant užtikrinti atitiktį Sąjungos institucijų aktams, nes iš esmės tariama, kad Sąjungos institucijų teisės aktai yra teisėti, todėl sukelia teisinių pasekmių, kol nėra pripažinti netekusiais galios, panaikinti patenkinus ieškinį dėl panaikinimo, paskelbti negaliojančiais išnagrinėjus prašymą priimti prejudicinį sprendimą arba pareiškus prieštaravimą dėl teisėtumo. Todėl Komisijos sprendimas dėl tinkamumo, kurį ji priėmė pagal Direktyvos 95/46/EB 25 straipsnio 6 dalį, yra privalomas visoms valstybių narių, kurioms jis skirtas, institucijoms, įskaitant šių valstybių narių nepriklausomas priežiūros institucijas ⁽²⁰⁴⁾. Kai tokia valdžios institucija gauna skundą, kuriame klausiama, ar Komisijos sprendimas dėl tinkamumo atitinka pagrindinės teisės į privatumą ir duomenų apsaugą užtikrinimą, ir mano, kad pateikti prieštaravimai yra pagrįsti, nacionalinėje teisėje turi būti numatytos teisių gynimo priemonės, kad šie prieštaravimai būtų perduoti nacionaliniam teismui, kuris, kilus abejonėms, privalo sustabdyti bylą ir Teisingumo Teismui pateikti prašymą priimti prejudicinį sprendimą ⁽²⁰⁵⁾;

6. IŠVADOS DĖL TINKAMUMO PERIODINĖ PERŽIŪRA

- (145) atsižvelgdama į tai, kad JAV teisės tvarkoje užtikrinamas apsaugos lygis gali keistis, Komisija, vadovaudamasi šiuo priimtu sprendimu, periodiškai tikrins, ar išvados dėl Jungtinių Amerikos Valstijų pagal ES ir JAV „privatumo skydo“ sistemą užtikrinamos apsaugos lygio tinkamumo vis dar yra faktiškai ir teisiškai pagrįstos. Toks patikrinimas turi būti atliekamas visais atvejais, kai Komisija gauna informacijos, dėl kurios jai šiuo atžvilgiu gali kilti pagrįsta abejonė ⁽²⁰⁶⁾;
- (146) todėl Komisija nuolat stebės bendrą asmens duomenų, sukurtų pagal ES ir JAV „privatumo skydą“, perdavimo sistemą, taip pat tai, kaip JAV valdžios institucijos laikosi prie šio sprendimo pridėtuose dokumentuose pateiktų pareiškimų ir įsipareigojimų. Kad palengvintų šį procesą, JAV įsipareigojo informuoti Komisiją apie esminius pokyčius JAV teisėje, kai jie yra susiję su „privatumo skydo“ duomenų apsaugos nuostatomis, ir valdžios institucijų prieigai prie asmens duomenų taikomus apribojimus ir apsaugos priemones. Be to, šiam sprendimui bus taikoma bendros metinės peržiūros procedūra, per kurią bus aptariami visi ES ir JAV „privatumo skydo“ veikimo aspektai, įskaitant nacionalinio saugumo ir teisės saugos išimčių taikymą privatumo principams. Be to, kadangi išvada dėl tinkamumo įtakos gali turėti Sąjungos teisės teisiniai pokyčiai, Komisija „privatumo skydu“ užtikrinamos apsaugos lygį įvertins pradėjusi taikyti BDAR;
- (147) kad atliktų bendrą metinę peržiūrą, nurodytą I, II ir VI prieduose, Komisija susitiks su Komercijos departamentu ir FPK, o prireikus – su kitų departamentų ir agentūrų, dalyvaujančių įgyvendinant „privatumo skydo“ sistemą, taip pat atsakingų už nacionalinio saugumo klausimus, atstovais, taip pat ODNI atstovais, kitais žvalgybos bendruomenės subjektais ir ombudsmenu. Šiame susitikime galės dalyvauti ES DAI ir 29 straipsnio darbo grupės atstovai;

⁽²⁰³⁾ Schrems, 40 ir kiti punktai, 101–103 punktai.

⁽²⁰⁴⁾ Schrems, 51, 52 ir 62 punktai.

⁽²⁰⁵⁾ Schrems, 65 punktas.

⁽²⁰⁶⁾ Schrems, 76 punktas.

- (148) atlikdama bendrą metinę peržiūrą, Komisija prašys Komercijos departamento pateikti išsamią informaciją apie visus su ES ir JAV „privatumo skydo“ sistemos veikimu susijusius aspektus, įskaitant Komercijos departamento iš DAI gautas bylas ir ex officio atitikties peržiūros rezultatus. Komisija taip pat prašys pateikti paaiškinimus dėl visų klausimų, susijusių su ES ir JAV „privatumo skydu“ ir jo veikimu, kurių gali kilti susipažinus su bet kuria prieinama informacija, įskaitant skaidrumo ataskaitas, kurias leidžiama teikti pagal JAV laisvės aktą, viešas ataskaitas, kurias rengia JAV nacionalinės žvalgybos institucijos, DAI ar privatumo grupių pateikta informacija, žiniasklaidos ataskaitomis arba informacija iš kitų prieinamų šaltinių. Be to, siekdamas palengvinti Komisijos užduotį šiuo atžvilgiu, valstybės narės turėtų informuoti Komisiją apie bylas, kuriose už privatumo principų laikymosi Jungtinėse Amerikos Valstijose užtikrinimą atsakingų institucijų veiksmais neužtikrinama atitiktis ir yra bet kokių požymių, kad JAV valdžios institucijų, atsakingų už nacionalinį saugumą arba nusikalstamų veikų prevenciją, tyrimą, atskleidimą ar baudžiamąjį persekiojimą, veiksmais neužtikrinamas reikalaujamas apsaugos lygis;
- (149) remdamasi metine bendra peržiūra, Komisija parengs viešą ataskaitą, kurią teiks Europos Parlamentui ir Tarybai;

7. SPRENDIMO DĖL TINKAMUMO SUSTABDYMAS

- (150) jeigu Komisija, remdamasi patikrinimų rezultatais arba bet kuria kita prieinama informacija, padaro išvadą, kad „privatumo skydu“ užtikrinamos apsaugos lygis nebegali būti laikomas iš esmės lygiaverčiu Sąjungoje užtikrinamam apsaugos lygiui, arba kad yra akivaizdžių požymių, jog Jungtinėse Amerikos Valstijose nebegalima užtikrinti veiksmingos atitikties privatumo principams arba kad JAV valdžios institucijų, atsakingų už nacionalinį saugumą arba nusikalstamų veikų prevenciją, tyrimą, atskleidimą ar baudžiamąjį persekiojimą, veiksmais neužtikrinamas reikalaujamas apsaugos lygis, ji apie tai informuoja Komercijos departamentą ir prašo imtis tinkamų priemonių, kad per konkretų ir protingą terminą būtų skubiai pašalinta bet kokia galimo privatumo principų nesilaikymo rizika. Jeigu pasibaigus konkrečiam terminui JAV valdžios institucijos tinkamai neįrodo, kad ES ir JAV „privatumo skydo“ sistema toliau garantuojama veiksminga atitiktis ir tinkamas apsaugos lygis, Komisija inicijuoja procedūrą dėl dalies ar viso šio sprendimo sustabdymo arba panaikinimo ⁽²⁰⁷⁾; Kitu atveju Komisija gali siūlyti iš dalies pakeisti šį sprendimą, pvz., nustatydama, kad išvada dėl tinkamumo galioja tik papildomas sąlygas atitinkančioms duomenų perdavimo operacijoms;
- (151) Komisija sustabdymo arba panaikinimo procedūrą visų pirma inicijuoja tuo atveju, kai:
- a) yra požymių, kad JAV valdžios institucijos nesilaiko prie šio sprendimo pridėtuose dokumentuose pateiktų pareiškimų ir įsipareigojimų, įskaitant pareiškimus ir įsipareigojimus, susijusius su sąlygomis ir apribojimais, taikomais JAV valdžios institucijų prieigai prie asmens duomenų, perduotų pagal „privatumo skydą“, teisėsaugos, nacionalinio saugumo ir kitais viešojo intereso tikslais;
 - b) nesugebama veiksmingai nagrinėti ES duomenų subjektų skundų; šiuo atžvilgiu Komisija atsižvelgia į visas aplinkybes, kurios daro poveikį ES duomenų subjektų galimybei įgyvendinti savo teises, įskaitant visų pirma autosertifikuotų JAV bendrovių savanorišką įsipareigojimą bendradarbiauti su duomenų apsaugos institucijomis ir paisyti jų rekomendacijų, arba
 - c) „privatumo skydo“ ombudsmenas laiku nepateikia tinkamų atsakymų į ES duomenų subjektų pateiktus prašymus;
- (152) Komisija taip pat nagrinėja galimybę pradėti procedūrą dėl šio sprendimo pakeitimo, sustabdymo arba panaikinimo, jeigu, atlikusi bendrą metinę ES ir JAV „privatumo skydo“ peržiūrą ar pritaikiusi kitokią procedūrą, nustato, kad Komercijos departamentas arba kiti departamentai ar agentūros, dalyvaujantys įgyvendinant „privatumo skydą“, arba už nacionalinio saugumo klausimų sprendimą atsakingi JAV žvalgybos bendruomenės atstovai arba ombudsmenas neteikia informacijos ar paaiškinimų, kurie yra būtini norint įvertinti, kaip laikomasi

⁽²⁰⁷⁾ Nuo Bendrojo duomenų apsaugos reglamento taikymo dienos Komisija pasinaudos savo įgaliojimais tinkamai pagrįstais skubiais atvejais priimti įgyvendinimo aktą, kuriuo bus sustabdomas dabartinis sprendimas ir kuris taikomas iš karto, nepateikiant jo atitinkamam komitologijos komitetui, ir galios ne ilgiau nei šešis mėnesius.

privatumo principų, skundų nagrinėjimo procedūrų veiksmingumą, arba JAV nacionalinės žvalgybos institucijos savo veiksmais sumažina reikalaujamą apsaugos lygį, visų pirma tai padaro rinkdamos ir (arba) tikrindamos daugiau asmens duomenų, nei yra griežtai būtina ir proporcinga. Šiuo atveju Komisija atsižvelgs į tai, kiek atitinkamos informacijos ji gali gauti iš kitų šaltinių, įskaitant autosertifikuotų JAV bendrovių ataskaitas, kaip tai leidžiama pagal JAV laisvės aktą;

- (153) pagal Direktyvos 95/46/EB 29 straipsnio nuostatas įkurta Darbo grupė asmenų apsaugai tvarkant asmens duomenis paskelbė savo nuomonę dėl apsaugos lygio, kuri suteikia ES ir JAV „privatumo skydas“ ⁽²⁰⁸⁾, į kurią buvo atsižvelgta rengiant šį sprendimą;
- (154) Europos Parlamentas priėmė rezoliuciją dėl transatlantinių duomenų srautų ⁽²⁰⁹⁾;
- (155) šiame sprendime nustatytos priemonės atitinka pagal Direktyvos 95/46/EB 31 straipsnio 1 dalį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

- Atsižvelgdamos į Direktyvos 95/46/EB 25 straipsnio 2 dalį, Jungtinės Amerikos Valstijos užtikrina tinkamą asmens duomenų, kuriuos pagal ES ir JAV „privatumo skydą“ Sąjunga perdavė Jungtinių Amerikos Valstijų organizacijoms, apsaugos lygį.
- ES ir JAV „privatumo skydą“ sudaro 2016 m. liepos 7 d. JAV komercijos departamento paskelbti privatumo principai, kurie išdėstyti II priede ir oficialiuose pareiškimuose ir išsipareigojimuose, kurie pateikti I, III–VII prieduose nurodytuose dokumentuose.
- Pagal šio straipsnio 1 dalį asmens duomenys perduodami pagal ES ir JAV „privatumo skydą“ tais atvejais, kai jie iš Sąjungos perduodami Jungtinių Amerikos Valstijų organizacijoms, įrašytoms į „privatumo skydo“ sąrašą, kuri pagal II priede išdėstytų privatumo principų I ir III skirsnius tvarko ir viešai skelbia JAV komercijos departamentas.

2 straipsnis

Šis sprendimas neturi jokios įtakos Direktyvos 95/46/EB nuostatų, visų pirma 4 straipsnio, taikymui, išskyrus 25 straipsnio 1 dalį, kuri yra susijusi su asmens duomenų tvarkymu valstybėse narėse.

3 straipsnis

Kai valstybių narių kompetentingos institucijos įgyvendina savo įgaliojimus pagal Direktyvos 95/46/EB 28 straipsnio 3 dalį ir dėl šios priežasties sustabdomi arba neribotam laikui uždraudžiami duomenų srautai į Jungtinių Amerikos Valstijų organizaciją, kuri įrašyta į „privatumo skydo“ sąrašą pagal II priedo I ir III skirsniuose nustatytus privatumo principus, kad apsaugotų asmenis atsižvelgiant į jų asmens duomenų tvarkymą, atitinkama valstybė narė nedelsdama informuoja Komisiją.

4 straipsnis

- Siekdama įvertinti, ar Jungtinės Amerikos Valstijos toliau užtikrina tinkamą asmens duomenų, kurie iš Sąjungos pagal ES ir JAV „privatumo skydą“ perduodami Jungtinių Amerikos Valstijų organizacijoms, apsaugą, Komisija nuolat stebi, kaip veikia ES ir JAV „privatumo skydas“.

⁽²⁰⁸⁾ 2016 m. balandžio 13 d. priimta nuomonė Nr. 01/2016 dėl ES ir JAV sprendimo dėl „privatumo skydo“ tinkamumo projekto.

⁽²⁰⁹⁾ 2016 m. gegužės 26 d. Europos Parlamento rezoliucija dėl transatlantinių duomenų srautų (2016/2727(RSP)).

2. Valstybės narės ir Komisija informuoja viena kitą apie atvejus, kai atrodo, kad Jungtinių Amerikos Valstijų Vyriausybės įstaigos, naudodamosi įstatymu suteiktais įgaliojimais užtikrinti II priede nustatytą privatumo principų laikymąsi nenustato veiksmingų nustatymo ir priežiūros mechanizmų, leidžiančių praktiškai identifikuoti privatumo principų pažeidimus ir už juos skirti bausmes.

3. Valstybės narės ir Komisija informuoja viena kitą apie bet kokius požymius, iš kurių matyti, kad JAV valdžios institucijos, atsakingos už nacionalinį saugumą, teisėsaugą ar kitus viešuosius interesus, asmenų teises į jų asmens duomenų apsaugą riboja viršydamos griežto būtinumo sąlygas ir (arba) kad nėra jokių veiksmingų teisių gynimo priemonių nuo tokio ribojimo.

4. Per vienus metus nuo pranešimo apie šį sprendimą valstybėms narėms ir vėliau kasmet Komisija vertina 1 straipsnio 1 dalies išvadą remdamasi visa prieinama informacija, įskaitant informaciją, gautą atliekant I, II ir VI prieduose nurodytą bendrą metinę peržiūrą.

5. Komisija apie visas susijusias išvadas informuoja pagal Direktyvos 95/46/EB 31 straipsnį įsteigtą komitetą.

6. Vadovaudamasi Direktyvos 95/46/EB 31 straipsnio 2 dalyje nustatyta procedūra, Komisija teiks priemonių projektus, kad sustabdytų, pakeistų arba panaikintų šį sprendimą arba apribotų jo taikymo sritį, be kita ko, kai yra požymių, kad:

- JAV valdžios institucijos nesilaiko prie šio sprendimo pridėtuose dokumentuose pateiktų pareiškimų ir išipareigojimų, įskaitant pareiškimus ir išipareigojimus, susijusius su sąlygomis ir apribojimais, taikomais JAV valdžios institucijų prieigai prie asmens duomenų, perduotų pagal „privatumo skydą“, teisėsaugos, nacionalinio saugumo ir kitais viešojo intereso tikslais,
- sistemiškai vengiama veiksmingai nagrinėti ES duomenų subjektų skundus arba
- „privatumo skydo“ ombudsmenas sistemiškai neteikė laiku tinkamų atsakymų į ES duomenų subjektų prašymus pagal savo funkcijas, kaip to reikalaujama pagal III priedo 4 dalies e punktą.

Komisija tokius priemonių projektus taip pat nustatys, jeigu dėl ES ir JAV „privatumo skydo“ veikimo užtikrinimą Jungtinėse Amerikos Valstijose užtikrinančių įstaigų netinkamo bendradarbiavimo Komisija negali nustatyti, ar daromas poveikis 1 straipsnio 1 dalyje nustatyta išvada.

5 straipsnis

Valstybės narės imasi visų priemonių, reikalingų šiam sprendimui įgyvendinti.

6 straipsnis

Šis sprendimas skirtas valstybėms narėms.

Priimta Briuselyje 2016 m. liepos 12 d.

Komisijos vardu
Věra JOUROVÁ
Komisijos narė

I PRIEDAS

JAV prekybos sekretoriaus Penny Pritzkerio raštas

2016 m. liepos 7 d.

Vėrai Jourovái,
už teisingumą, vartotojų reikalus ir lyčių lygybę atsakingai Komisijos narei
Europos Komisija
Rue de la Loi/Westraat 200
1049 Briuselis
Belgija

Gerbiama Komisijos nare V. Jourová,

džiaugiuosi galėdamas Jungtinių Amerikos Valstijų vardu kartu su šiuo raštu perduoti Jums ES ir JAV „privatumo skydo“ medžiagos dokumentus, kuriuos per dvejus metus trukusias rezultatyvias diskusijas parengė mūsų darbo grupės. Šis dokumentų rinkinys, įskaitant kitą Komisijai viešuose šaltiniuose prieinamą informaciją, – itin patikimas Europos Komisijos naujos išvados dėl tinkamumo pagrindas ⁽¹⁾.

Abi pusės turėtų didžiuotis atliktais sistemos patobulinimais. „Privatumo skydas“ grindžiamas principais, dėl kurių tvirtai sutariama abiejose Atlanto pusėse, be to, mes pradėjome griežčiau juos taikyti. Dirbdami drauge turime realią galimybę pagerinti privatumo apsaugą visame pasaulyje.

„Privatumo skydo“ dokumentų rinkinį, be kita ko, sudaro „privatumo skydo“ principai, taip pat programą administruojančios Komercijos departamento Tarptautinės prekybos administracijos (TPA) raštas (pridedamas kaip 1 priedas), kuriame aprašomi mūsų departamento priimti išipareigojimai siekiant užtikrinti, kad „privatumo skydo“ sistema būtų veiksminga. Dokumentų rinkinyje taip pat yra 2 priedas, kuriame aprašyti kiti Komercijos departamento išipareigojimai, susiję su naujai sukurtu „privatumo skydo“ arbitražo modeliu.

Savo darbuotojams nurodžiau skirti visus reikalingus išteklius, kad „privatumo skydo“ sistema būtų įgyvendinta greitai ir visapusiškai, ir užtikrinti, kad 1 ir 2 prieduose nurodyti išipareigojimai būtų laiku įgyvendinti.

„Privatumo skydo“ dokumentų rinkinį taip pat sudaro kitų Jungtinių Amerikos Valstijų agentūrų dokumentai, t. y.:

- Federalinės prekybos komisijos (FPK) raštas, kuriame aprašoma, kaip ji užtikrins „privatumo skydo“ veikimą,
- Transporto departamento raštas, kuriame aprašoma, kaip jis užtikrins „privatumo skydo“ veikimą,
- Nacionalinės žvalgybos direktoriaus biuro (ODNI) parengti du raštai dėl apsaugos priemonių ir JAV nacionalinio saugumo institucijoms taikomų apribojimų,
- Valstybės departamento raštas ir pridedamas memorandumas, kuriuose aprašomas Valstybės departamento išipareigojimas įsteigti naują „privatumo skydo“ ombudsmeno įstaigą, kuriai būtų teikiamos užklausos dėl Jungtinių Amerikos Valstijų signalų žvalgybos praktikos, ir
- Teisingumo departamento parengtas raštas dėl apsaugos priemonių ir JAV Vyriausybei taikomų apribojimų leidžiant susipažinti su duomenimis teisėsaugos ir viešojo intereso tikslais.

Galiu patikinti, kad Jungtinės Amerikos Valstijos rimtai vertina šiuos išipareigojimus.

⁽¹⁾ Jeigu Komisijos sprendimas dėl ES ir JAV „privatumo skydo“ suteikiamos apsaugos tinkamumo taikomas Islandijai, Lichtenšteinui ir Norvegijai, „privatumo skydo“ dokumentų rinkinys bus taikomas tiek Europos Sąjungai, tiek šioms trimis šalims.

Per 30 dienų nuo galutinio sprendimo dėl tinkamumo patvirtinimo visas „privatumo skydo“ dokumentų rinkinys bus perduotas *Federaliniam registrui*, kad šis jį paskelbtų.

Nekantraujame toliau su jumis bendradarbiauti įgyvendinant „privatumo skydo“ nuostatas ir kartu pereinant prie kito šio proceso etapo.

Pagarbiai
Penny Pritzkeris

1 priedas

Laikiniai einančio pareigas Tarptautinės prekybos sekretoriaus Keno Hyatt raštas

Gerbiamai Vėrai Jourovái,
už teisingumą, vartotojų reikalus ir lyčių lygybę atsakingai Komisijos narei
Europos Komisija
Rue de la Loi/Westraat 200
1049 Briuselis
Belgija

Gerbiama Komisijos nare V. Jourová,

džiaugiuosi galėdamas Tarptautinės prekybos administracijos vardu pranešti apie sustiprintą asmens duomenų apsaugą, kuri užtikrinama ES ir JAV „privatumo skydo“ sistema (toliau – „privatumo skydas“ arba sistema), ir Komercijos departamento (toliau – Departamentas) priimtus išipareigojimus siekiant užtikrinti „privatumo skydo“ sistemos veiksmingumą. Šio istorinio susitarimo užbaigimas – svarbiausias laimėjimas privatumo srityje, kuris bus naudingas abiejose Atlanto pusėse veikiančioms įmonėms. Todėl ES fiziniai asmenys galės būti tikri dėl savo duomenų apsaugos ir neabejoti, kad bet kokioms kilusioms problemoms išspręsti galės pasinaudoti teisinėmis teisių gynimo priemonėmis. Šiuo susitarimu sukuriamas užtikrintumas, kuris padės augti transatlantinei ekonomikai, nes tūkstančiai Europos ir Amerikos įmonių toliau galės nebijodamos investuoti ir vykdyti verslą abiejose Atlanto pusėse. „Privatumo skydas“ – tai dvejų metų sunkaus darbo ir bendradarbiavimo su Jumis ir mūsų kolegomis Europos Komisijoje (toliau – Komisija) rezultatas. Tikimės toliau dirbti su Komisija ir užtikrinti, kad „privatumo skydas“ veiktų kaip numatyta.

Kartu su Komisija dirbome kurdami „privatumo skydą“, kad Jungtinėse Amerikos Valstijose įsikūrusios organizacijos galėtų užtikrinti atitiktį ES teisėje nustatytiems duomenų apsaugos tinkamumo reikalavimams. Naujoji sistema fiziniams asmenims ir įmonėms bus naudinga keliais aspektais. Pirmia, šioje sistemoje nustatytas svarbus ES fizinių asmenų duomenų privatumo apsaugos priemonių rinkinys. Šioje sistemoje iš dalyvaujančių JAV organizacijų reikalaujama: sukurti atitinkamą privatumo politiką; viešai išipareigoti laikytis „privatumo skydo“ principų, kad išipareigojimas taptų vykdytinas pagal JAV teisę; kasmet teikti Komercijos departamentui reikalavimų laikymosi patvirtinimą; užtikrinti galimybę ES fiziniams asmenims nemokamai kreiptis į nepriklausomą ginčų sprendimo instituciją ir paklusti JAV federalinės prekybos komisijos (FPK), Transporto departamento (angl. *Department of Transportation*, toliau – DOT) ar kitos teisės saugos institucijos nurodymams. Antra, „privatumo skydas“ leis tūkstančiams Jungtinių Amerikos Valstijų bendrovių ir Jungtinėse Amerikos Valstijose veikiančių Europos bendrovių filialų gauti iš Europos Sąjungos asmens duomenis, kad būtų palengvinti transatlantinę prekybą skatinantys duomenų srautai. Transatlantiniai ekonominiai santykiai pagal apimtį jau yra didžiausi pasaulyje, nes sudaro pusę pasaulinės ekonomikos produkcijos, kurios prekių ir paslaugų vertė – beveik vienas trilijonas JAV dolerių, be to, šie santykiai yra daugybės darbo vietų abiejose Atlanto pusėse garantas. Transatlantiniais duomenų srautais naudojasi visų pramonės sektorių įmonės, įskaitant pagrindines „Fortune 500“ bendroves, taip pat daugybę mažųjų ir vidutinių įmonių (MVĮ). Dėl transatlantinių duomenų srautų JAV organizacijos gali tvarkyti duomenis, kurių reikia Europos fiziniams asmenims siūlant prekes, paslaugas ir įsidarbinimo galimybes. „Privatumo skydo“ sistemoje skatinama laikytis bendrų privatumo principų, pašalinti mūsų teisinių sistemų skirtumus ir toliau siekti Europos ir Jungtinių Amerikos Valstijų prekybos ir ekonominių tikslų.

Bendrovės sprendimus dėl šios sistemos autosertifikavimo priims savanoriškai, tačiau bendrovės viešas išipareigojimas dalyvauti „privatumo skydo“ sistemoje tampa vykdytinas pagal JAV teisę, o jo vykdymą užtikrina Federalinė prekybos komisija arba Transporto departamentas; tai priklauso nuo to, kuri institucija turi jurisdikciją „privatumo skydo“ organizacijos atžvilgiu.

„Privatumo skydo“ principų patobulinimai

Sukurtas „privatumo skydas“ padeda užtikrinti geresnę privatumo apsaugą, nes:

- pagal pranešimo principą reikalaujama pateikti papildomą informaciją fiziniams asmenims, įskaitant deklaraciją dėl organizacijos dalyvavimo „privatumo skydo“ sistemoje, pareiškimą dėl fizinio asmens teisės susipažinti su asmens duomenimis ir atitinkamos nepriklausomos ginčų sprendimo įstaigos nurodymą,
- sugriežtinama asmens duomenų, kuriuos „privatumo skydo“ organizacija perduoda trečiosios šalies duomenų valdytojui, apsauga – reikalaujama, kad šalys sudarytų sutartį, kurioje nustatytų, kad tokie duomenys gali būti tvarkomi tik ribotais ir konkrečiais tikslais, atitinkančiais fizinio asmens duoto sutikimo sąlygas, ir kad duomenų gavėjas užtikrins tokį pat duomenų apsaugos lygį, koks užtikrinamas pagal privatumo principus,

- sugriežtinama asmens duomenų, kuriuos „privatumo skydo“ organizacija perduoda trečiosios šalies atstovui, apsauga, be kita ko, reikalaujama, kad „privatumo skydo“ organizacija: imtųsi pagrindų ir tinkamų priemonių, kuriomis užtikrintų, kad atstovas veiksmingai tvarkytų asmeninę informaciją, kuri buvo perduota laikantis organizacijos įsipareigojimų, susijusių su privatumo principais; gavusi pranešimą, imtųsi pagrindų ir tinkamų priemonių, kad sustabdytų neteisėtą duomenų tvarkymą ir atitaisytų su tuo susijusius pažeidimus ir Departamento prašymu pateiktų atitinkamų savo sutarties su tuo atstovu privatumo nuostatų santrauką arba patvirtintą kopiją,
- nustatoma, kad „privatumo skydo“ organizacija atsako už pagal „privatumo skydo“ nuostatas gautos asmeninės informacijos tvarkymą ir vėlesnį jos perdavimą trečiajai šaliai, kuri jos vardu veikia kaip atstovas, ir kad „privatumo skydo“ organizacija pagal privatumo principus toliau atsako, jeigu jos atstovas tokią asmeninę informaciją tvarko su privatumo principais nesuderinamu būdu, nebent organizacija įrodo, kad ji neatsako už įvykį, dėl kurio buvo padaryta žala,
- paaiškinama, kad „privatumo skydo“ organizacijos privalo tvarkyti tik tvarkymo tikslus atitinkančią asmeninę informaciją,
- reikalaujama, kad organizacija kasmet teiktų Departamentui patvirtinimą, jog įsipareigoja informacijai, kurią gavo dalyvaudama „privatumo skydo“ sistemoje, toliau taikyti privatumo principus, jeigu nustoja dalyvauti „privatumo skydo“ sistemoje ir nusprendžia toliau saugoti tokius duomenis,
- reikalaujama, kad fiziniam asmeniui būtų sudarytos sąlygos nemokamai pasinaudoti nepriklausomomis teisių gynimo institucijomis,
- reikalaujama, kad organizacijos ir jų pasirinktos nepriklausomos teisių gynimo institucijos greitai reaguotų į Departamento pateiktas užklausas ir prašymus pateikti informaciją „privatumo skydo“ užtikrinimo klausimais,
- reikalaujama, kad organizacijos greitai reaguotų į skundus dėl privatumo principų nesilaikymo, kuriuos ES valstybės narės valdžios institucijos perdavė per Departamentą, ir
- reikalaujama, kad „privatumo skydo“ organizacija viešai skelbtų visus su „privatumo skydu“ susijusius FPK pateiktų atitikties arba vertinimo ataskaitų skirsnius, jeigu ji privalo laikytis FPK arba teismo sprendimo, priimto byloje dėl reikalavimų nesilaikymo.

Komercijos departamento įgyvendinamo „privatumo skydo“ programos administravimas ir priežiūra

Departamentas pakartoja, kad įsipareigoja tvarkyti ir viešai skelbti patikimą JAV organizacijų, kurios pateikė Departamentui autosertifikavimo pažymėjimą ir pareiškė įsipareigojančios laikytis privatumo principų, sąrašą (toliau – „privatumo skydo“ sąrašas). Departamentas nuolat atnaujins „privatumo skydo“ sąrašą, išbraukdamas organizacijas, kurios savanoriškai pasitraukė, nesilaikė Departamento nustatytų metinių pakartotinio sertifikavimo procedūrų arba nustatyta, kad jos nuolat nesilaikė reikalavimų. Departamentas taip pat tvarkys ir viešai skelbs patikimą JAV organizacijų, kurios anksčiau pateikė Departamentui autosertifikavimo pažymėjimą, tačiau buvo išbrauktos iš „privatumo skydo“ sąrašo, registrą, kuriame, be kita ko, bus rodomos iš sąrašo išbrauktos organizacijos, kurios nuolat nesilaikė privatumo principų. Departamentas nurodys kiekvienos organizacijos išbraukimo iš sąrašo priežastį.

Be to, Departamentas įsipareigoja stiprinti „privatumo skydo“ administravimą ir priežiūrą. Tiksliau tariant, Departamentas imsis toliau išvardytų veiksmų.

„Privatumo skydo“ svetainėje skelbs papildomą informaciją

- Tvarkys „privatumo skydo“ sąrašą, taip pat organizacijų, kurios anksčiau pateikė autosertifikavimo pažymėjimą dėl principų laikymosi, tačiau nebesinaudoja „privatumo skydo“ teikiamais privalumais, registrą.
- Gerai matomoje vietoje pateiks paaiškinimą, kuriame nurodys, kad visos iš „privatumo skydo“ sąrašo išbrauktos organizacijos, kurios nebesinaudoja „privatumo skydo“ teikiamais privalumais, vis tiek privalo toliau taikyti privatumo principus asmeninei informacijai, gautai tuo metu, kai dalyvavo „privatumo skydo“ sistemoje, ir tai daryti tol, kol saugos tokią informaciją, ir
- pateiks nuorodą į FPK svetainėje skelbiamą FPK bylų, susijusių su „privatumo skydu“, sąrašą.

Tikrins, kaip laikomasi autosertifikavimo reikalavimų

- Prieš pasibaigiant organizacijos autosertifikavimo (arba metinio pakartotinio sertifikavimo) procedūrai ir ištraukiant organizaciją iš „privatumo skydo“ sąrašą, tikrins, ar organizacija:
 - pateikė reikalaujamus organizacijos kontaktus,
 - aprašė organizacijos veiklą, susijusią su asmenine informacija, gaunama iš ES,
 - nurodė, kokiai asmeninei informacijai bus taikoma jos autosertifikavimo procedūra,
 - jeigu organizacija turi viešą svetainę, tikrins, ar ji nurodė svetainės adresą, kuriame skelbiama privatumo politika, ir ar privatumo politika skelbiama nurodytu svetainės adresu, arba, jeigu organizacija neturi viešos svetainės, tikrins, ar visuomenė turi galimybę susipažinti su privatumo politika;
 - į savo atitinkamą privatumo politiką įtraukė pareiškimą, kad ji laikosi privatumo principų, ir, jeigu privatumo politika skelbiama internete, tikrins, ar pateikiamas saitas į Departamento „privatumo skydo“ svetainę,
 - nurodė konkrečią valstybinę įstaigą, turinčią jurisdikciją nagrinėti bet kokius skundus prieš organizaciją dėl galimų nesąžiningų ar apgaulingų veiksmų ir privatumo teisės aktų ar taisyklių pažeidimų (kai šie teisės aktai ar taisyklės yra įtraukti į privatumo principus arba būsimą privatumo principų priedą),
 - jeigu organizacija nusprendžia teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principo (a)(i) ir (a)(iii) punktuose nurodytus reikalavimus įvykdyti išpareigodama bendradarbiauti su atitinkamomis ES duomenų apsaugos institucijomis (DAI), nurodė savo ketinimą bendradarbiauti su DAI tiriant ir sprendžiant su „privatumo skydu“ susijusius skundus, visų pirma atsakyti į DAI užklausas, kai ES duomenų subjektai skundus pateikė tiesiogiai savo nacionalinėms DAI,
 - nurodė privatumo programų, kurioje dalyvauja organizacija, pavadinimą,
 - nurodė metodą, kurį taiko tikrindama, ar laikomasi privatumo principų (pvz., vidaus arba trečiųjų šalių kontrolė),
 - savo pareiškime dėl autosertifikavimo ir privatumo politikoje nurodė nepriklausomą teisių gynimo instituciją, į kurią galima kreiptis norint ištirti ir išspręsti skundus;
 - savo atitinkamoje privatumo politikoje, jeigu ji skelbiama internete, pateikė saitą į nepriklausomos teisių gynimo institucijos, į kurią galima kreiptis norint ištirti neišspręstus skundus, svetainę arba skundų pateikimo formą, ir
 - jeigu organizacija nurodė ketinanti gauti žmoniškųjų išteklių informaciją, perduotą iš ES, ir ją naudoti įdarbinimo tikslais, tikrinama, ar ji išpareigojo bendradarbiauti su DAI ir laikytis jų rekomendacijų, kad būtų išspręsti skundai dėl jos veiklos tvarkant tokius duomenis, pateikė Departamentui savo žmoniškųjų išteklių politikos kopiją ir nurodė, kur jos darbuotojai gali susipažinti su privatumo politika.
- Dirba su nepriklausomomis teisių gynimo institucijomis, kad patikrintų, ar organizacijos iš tikrųjų yra registruotos atitinkamos institucijos, nurodytos jų pareiškimuose dėl autosertifikavimo, naudotojos, kai tokia registracija yra privaloma.

Stengiasi toliau bendradarbiauti su organizacijomis, kurios buvo išbrauktos iš „privatumo skydo“ sąrašo

- Praneša organizacijoms, kurios iš „privatumo skydo“ sąrašo buvo išbrauktos dėl „nuolatinio reikalavimų nesilaikymo“, kad jos neturi teisės saugoti pagal „privatumo skydo“ nuostatas surinktos informacijos, ir
- organizacijoms, kurių autosertifikavimo terminas pasibaigė arba kurios savanoriškai nustojo dalyvauti „privatumo skydo“ sistemoje, nusiunčia klausimyną, kuris padeda nustatyti, ar organizacija grąžino ar ištrynė asmens duomenis, kuriuos gavo dalyvaudama „privatumo skydo“ sistemoje, ar toliau tokiems duomenims taiko privatumo principus, o jeigu asmens duomenys turi būti saugomi, – nustatyti asmenį, kuris organizacijoje bus atsakingas už visų su „privatumo skydu“ susijusių klausimų sprendimą.

Atlieka klaidingų pareiškimų dėl dalyvavimo paiešką ir užkerta kelią tokiems pareiškimams

- Peržiūri organizacijos, kuri anksčiau dalyvavimo „privatumo skydo“ sistemoje, tačiau buvo išbraukta iš „privatumo skydo“ sąrašo, privatumo politiką, kad išsiaiškintų, ar nėra kokių nors klaidingų pareiškimų dėl dalyvavimo „privatumo skydo“ sistemoje.
- Reguliariai, kai organizacija: a) nustoja dalyvauti „privatumo skydo“ sistemoje, b) pakartotinai nepatvirtina savo įsipareigojimo laikytis privatumo principų arba c) pašalinama iš „privatumo skydo“ sistemos, visų pirma dėl „nuolatinio reikalavimų nesilaikymo“, įsipareigoja *ex officio* tikrinti, ar organizacija iš bet kurios susijusios privatumo politikos pašalino visas nuorodas į „privatumo skydą“, iš kurių būtų galima numanyti, kad organizacija toliau aktyviai dalyvauja „privatumo skydo“ sistemoje ir turi teisę naudotis jos teikiama privalumais. Departamentas, jeigu nustato, kad tokios nuorodos nebuvo pašalintos, įspėja organizaciją, kad, kai tinkama, perduos klausimus atitinkamai agentūrai, kad ji imtųsi vykdymo veiksmų, jeigu organizacija toliau darys pareiškimus, kad ji dalyvauja „privatumo skydo“ sistemoje. Jeigu organizacija nepašalina nuorodų ir, taikydama autosertifikavimo procedūrą, nepatvirtina, kad laikysis „privatumo skydo“ nuostatų, Departamentas *ex officio* perduoda klausimą FPK, TD arba kitai atitinkamai vykdymo agentūrai arba atitinkamai atvejais imasi veiksmų, kad užtikrintų tinkamą „privatumo skydo“ sertifikavimo ženklo naudojimą.
- Imasi kitų veiksmų, kad nustatytų klaidingus pareiškimus dėl dalyvavimo „privatumo skydo“ sistemoje ir netinkamo „privatumo skydo“ sertifikavimo ženklo naudojimo atvejus, įskaitant paiešką internete, siekiant nustatyti, kuriose vietose rodomos „privatumo skydo“ sertifikavimo ženklų piktogramos ir kurioje organizacijos privatumo politikos vietoje pateikiamos nuorodos į „privatumo skydą“.
- Nedelsdamas sprendžia visus klausimus, kuriuos Departamentas nustato *ex officio* stebėdamas, ar nėra klaidingų pareiškimų dėl dalyvavimo ir netinkamo sertifikavimo ženklo naudojimo atvejų, įskaitant organizacijų, kurios klaidingai informuoja apie savo dalyvavimą „privatumo skydo“ sistemoje, perspėjimą, kaip aprašyta pirmiau.
- Imasi kitų tinkamų taisomųjų veiksmų, įskaitant visas teises priemones, kurias gali taikyti Departamentas, ir klausimų perdavimą FPK, TD arba kitai atitinkamai vykdymo agentūrai, ir
- nedelsdamas peržiūri ir nagrinėja gautus skundus dėl klaidingų pareiškimų apie dalyvavimą.

Departamentas atlieka organizacijos privatumo politikos peržiūrą, kad veiksmingiau nustatytų klaidingus pareiškimus dėl dalyvavimo „privatumo skydo“ sistemoje ir užkirstų jiems kelią. Tiksliau tariant, Departamentas peržiūrės organizacijų, kurių autosertifikavimo terminas baigėsi dėl to, kad jos pakartotinai nepatvirtino, jog laikosi privatumo principų, privatumo politiką. Departamentas šios rūšies peržiūrą atliks siekdamas patikrinti, ar tokios organizacijos iš visos paskelbtos privatumo politikos pašalino bet kokias nuorodas, iš kurių būtų galima numanyti, kad organizacijos toliau aktyviai dalyvauja „privatumo skydo“ sistemoje. Atlikę šias peržiūras, nustatysime organizacijas, kurios nepašalino tokių nuorodų, ir nusiųsime joms Departamento Generalinio advokato biuro vardu pasirašytą raštą, kuriame įspėsime apie galimus vykdymo veiksmus, jeigu nuorodos nebus pašalintos. Departamentas imsis tolesnių veiksmų, siekdamas užtikrinti, kad organizacijos pašalintų netinkamas nuorodas arba pakartotinai patvirtintų, kad laikosi privatumo principų. Be to, Departamentas imsis priemonių, kad nustatytų klaidingus pareiškimus apie dalyvavimą „privatumo skydo“ sistemoje, kuriuos pateikė „privatumo skydo“ sistemoje niekada nedalyvavusios organizacijos, ir imsis panašių taisomųjų veiksmų tokių organizacijų atžvilgiu.

Ex officio atlieka periodines atitikties peržiūras ir programos vertinimus

- Nuolat stebi, ar iš tikrųjų laikomasi reikalavimų, įskaitant išsamių klausimynų siuntimą dalyvaujančioms organizacijoms, kad nustatytų klausimus, dėl kurių gali prireikti imtis tolesnių veiksmų. Tokia atitikties peržiūra visų pirma atliekama, kai: a) Departamentas gauna konkrečius pagrįstus skundus dėl to, kaip organizacija laikosi privatumo principų; b) organizacijos atsakymai į Departamento užklausas dėl informacijos, susijusios su „privatumo skydu“, yra netinkami arba c) yra patikimų įrodymų, kad organizacija nesilaiko savo įsipareigojimų pagal „privatumo skydo“ sistemą. Departamentas, kai tinkama, konsultuojasi su kompetentingomis duomenų apsaugos institucijomis dėl tokių atitikties peržiūrų ir
- periodiškai įvertina „privatumo skydo“ programos administravimą ir priežiūrą, siekdamas užtikrinti, kad būtų imtasi tinkamų stebėsenos veiksmų ir išspręsti nauji klausimai.

Departamentas padidino išteklis, kurie bus skirti „privatumo skydo“ programos administravimui ir priežiūrai, įskaitant dvigubai didesnę darbuotojų, atsakingų už programos administravimą ir priežiūrą, skaičių. Toliau skirsime pakankamai išteklių tokiems veiksams, kad užtikrintume veiksmingą programos stebėseną ir administravimą.

Pritaikyti „privatumo skydo“ svetainę prie tikslinės auditorijos poreikių

Departamentas pritaikys „privatumo skydo“ svetainę, kad ji atitiktų trijų grupių tikslinės auditorijos – ES fizinių asmenų, ES įmonių ir JAV įmonių – poreikius. Tiesiogiai ES fiziniams asmenims ir ES įmonėms skirtos medžiagos pateikimas padės užtikrinti didesnę skaidrumą įvairiais aspektais. Svetainėje bus pateikiama ES fiziniams asmenims skirta aiški informacija apie: 1) teises, kurios ES fiziniams asmenims suteikiamos „privatumo skydo“ sistemoje; 2) teisių gynimo institucijas, į kurias gali kreiptis ES fiziniai asmenys, manantys, kad organizacija pažeidė savo įsipareigojimą laikytis privatumo principų; ir 3) tai, kaip rasti informacijos, susijusios su organizacijos „privatumo skydo“ autosertifikavimu. Svetainėje ES įmonės galės lengviau patikrinti: 1) ar organizacija teisėtai naudoja „privatumo skydo“ teikiamaais privalumais; 2) informacijos, kuriai taikoma organizacijos „privatumo skydo“ autosertifikavimo procedūra, rūšį; 3) privatumo politiką, kuri taikoma tvarkomai informacijai; ir 4) metodą, kurį organizacija naudoja siekdama laikytis privatumo principų.

Didesnis bendradarbiavimas su DAI

Siekdamas didinti bendradarbiavimo su DAI galimybes, Departamentas įsteigs specialų kontaktinį centrą, kuris veiks kaip ryšių palaikymo su DAI institucija. Jeigu DAI mano, kad organizacija nesilaiko privatumo principų, įskaitant iš ES fizinio asmens gautą skundą, ji gali kreiptis į specialų Departamento kontaktinį centrą, kad perduotų organizacijos bylą tolesnei peržiūrai. Kontaktiniam centrui taip pat bus perduodamos bylos dėl organizacijų, kurios klaidingai teigė dalyvaujančios „privatumo skydo“ sistemoje, nors niekada netaikė autosertifikavimo procedūros dėl privatumo principų laikymosi. Kontaktinis centras padės DAI ieškoti informacijos, susijusios su konkrečios organizacijos autosertifikavimu arba ankstesniu dalyvavimu programoje, be to, kontaktinis centras atsakys į DAI užklausas dėl konkrečių „privatumo skydo“ programos reikalavimų įgyvendinimo. Antra, Departamentas teiks DAI medžiagą apie „privatumo skydą“, kuri bus skelbiama DAI svetainėje siekiant didesnio skaidrumo ES fizinių asmenų ir ES įmonių atžvilgiu. Didesnis informuotumas apie „privatumo skydą“ ir su juo susijusias teises bei pareigas turėtų padėti lengviau nustatyti kylančius klausimus ir tinkamai juos išspręsti.

Palengvinti skundų dėl reikalavimų nesilaikymo sprendimą

Departamentas per specialų kontaktinį centrą gaus DAI jam perduotus skundus dėl to, kad „privatumo skydo“ organizacija nesilaiko privatumo principų. Departamentas dės visas pastangas, kad palengvintų skundų dėl „privatumo skydo“ organizacijos sprendimą. Per 90 dienų nuo skundo gavimo Departamentas pateiks DAI naujausią informaciją. Kad palengvintų tokių skundų pateikimą, Departamentas sukurs DAI skirtą standartinę formą, kurią jos naudos perduodamos skundus specialiam Departamento kontaktiniam centrui. Specialus kontaktinis centras stebės visas DAI perduotas bylas, kurias gavo Departamentas, o metinėje peržiūroje (aprašyta toliau) Departamentas pateiks ataskaitą, kurioje galima rasti apibendrintą kasmet gautų skundų analizę.

Nustato arbitražo procedūras ir, pasikonsultavęs su Komisija, atranka arbitrus

Departamentas įgyvendina savo įsipareigojimus pagal I priedą ir skelbia procedūras, dėl kurių buvo pasiektas susitarimas.

„Privatumo skydo“ veikimo bendras peržiūros mechanizmas

Komercijos departamentas, FPK ir, kai tinkama, kitos agentūros rengs metinius susitikimus su Komisija, suinteresuotomis DAI ir atitinkamais 29 straipsnio darbo grupės atstovais, kuriuose Departamentas pateiks naujausią informaciją apie „privatumo skydo“ programą. Per metinį susitikimą bus aptariami einamieji klausimai, susiję su „privatumo skydo“ veikimu, įgyvendinimu, priežiūra ir užtikrinimu, taip pat Departamento iš DAI gautos bylos, *ex officio* atitikties peržiūros, be to, gali būti aptariami ir atitinkami teisės pakeitimai. Per pirmąją metinę peržiūrą ir vėlesnes peržiūras, kai tinkama, bus aptariamasi kitos temos, pvz., susijusios su automatizuotu sprendimų priėmimu, įskaitant aspektus, susijusius su ES ir JAV požiūrių panašumais ir skirtumais.

Įstatymų atnaujinimas

Departamentas imsis tinkamų veiksmų, kad informuotų Komisiją apie esminius Jungtinių Amerikos Valstijų teisės pokyčius, susijusius su „privatumo skydo“ nuostatomis, kuriomis reglamentuojama duomenų privatumo apsauga ir JAV valdžios institucijų galimybei susipažinti su asmens duomenimis ir vėliau juos naudoti taikomi apribojimai ir apsaugos priemonės.

Nacionalinio saugumo išimtis

Kalbant apie nacionalinio saugumo tikslais taikomus „privatumo skydo“ principų laikymosi apribojimus, atkreipiame dėmesį į Jums persiųstus du Nacionalinės žvalgybos direktoriaus biuro Generalinio advokato Roberto Litto raštus, adresuotus Komercijos departamento darbuotojams Justinui Antonipillai ir Tedui Deanui. Šiuose raštuose, be kitų klausimų, išsamiai aptariama politika, apsaugos priemonės ir apribojimai, kurie taikomi JAV vykdomai signalų žvalgybos veiklai. Be to, juose aprašomos skaidrumo priemonės, kurias šiems klausimams taiko žvalgybos bendruomenė. Komisija šiuo metu dar vertina „privatumo skydo“ sistemą, todėl šiuose raštuose pateikta informacija patikinama, kad „privatumo skydas“ veiks tinkamai pagal jame nustatytus principus. Suprantame, kad galite rinkti žvalgybos bendruomenės viešai paskelbtą informaciją, įskaitant kitą informaciją, kuria ateityje galėsite remtis atlikdami metinę „privatumo skydo“ sistemos peržiūrą.

Remdamiesi „privatumo skydo“ principais ir pridedamais raštais bei medžiaga, įskaitant Departamento įsipareigojimus, susijusius su „privatumo skydo“ sistemos administravimu ir priežiūra, tikimės, kad Komisija patvirtins, jog ES ir JAV „privatumo skydo“ sistema užtikrinama tinkama apsauga, atitinkanti ES teisės reikalavimus, ir kad duomenys iš Europos Sąjungos toliau bus perduodami „privatumo skydo“ sistemoje dalyvaujančioms organizacijoms.

Pagarbiai
Kenas Hyattas

2 priedas

Arbitražinis modelis

I PRIEDAS

Šiame I priede pateikiamos sąlygos, kuriomis „privatumo skydo“ organizacijos įpareigojamos pagal teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principą arbitražo tvarka nagrinėti reikalavimus. Toliau aprašyta arbitražo sąlyga taikoma tam tikriems neįvykdytiems reikalavimams, susijusiems su duomenimis, kuriems galioja ES ir JAV „privatumo skydo“ apsauga. Šios arbitražo sąlygos paskirtis – sukurti operatyvų, nepriklausomą ir sąžiningą mechanizmą, kurį pasirinkę fiziniai asmenys galėtų pašalinti tariamus privatumo principų pažeidimus, kurie nebuvo išspręsti naudojant kurį nors kitą „privatumo skydo“ mechanizmą.

A. Taikymo sritis

Šia arbitražo alternatyva asmenys gali pasinaudoti, kad, atsižvelgdami į neįvykdytus reikalavimus, nustatytų, ar „privatumo skydo“ organizacija pažeidė savo įsipareigojimus pagal privatumo principus dėl to asmens ir ar bet kuris toks pažeidimas lieka visiškai arba iš dalies neištaisytas. Arbitražu galima pasinaudoti tik minėtais tikslais. Ši alternatyva nėra prieinama, pvz., dėl privatumo principo išimčių ⁽¹⁾ arba dėl teiginių, susijusių su „privatumo skydo“ tinkamumu.

B. Prieinamos teisių gynimo priemonės

Pagal šią arbitražo alternatyvą „privatumo skydo“ komisija (kurią sudaro vienas arba trys arbitrai, tai priklauso nuo šalių sutarimo) turi įgaliojimus nustatyti su konkrečiu asmeniu susijusias nepinigines lygiavertes teisių gynimo priemones (pvz., prieiga prie atitinkamų asmens duomenų, šių duomenų taisymas, trynimasis arba grąžinimas), kurios yra būtinos siekiant ištaisyti privatumo principų pažeidimą tik to asmens atžvilgiu. Šiais įgaliojimais arbitražo komisija gali naudotis tik dėl teisių gynimo priemonių. Nagrinėdama teisių gynimo priemones, arbitražo komisija turi apsvarstyti kitas teisių gynimo priemones, kurios jau privalomai taikomos pagal kitus „privatumo skydo“ mechanizmus. Netaikomas žalos, išlaidų ar mokesčių atlyginimas ar kitos teisių gynimo priemonės. Kiekviena šalis sumoka savo advokato mokesčius.

C. Reikalavimai, kuriuos reikia įvykdyti iki arbitražo

Asmuo, kuris nusprendžia naudotis šia arbitražo alternatyva, prieš perduodamas reikalavimą arbitražui privalo atlikti šiuos veiksmus: 1) pareikšti reikalavimą dėl tariamo pažeidimo tiesiogiai organizacijai ir suteikti jai galimybę išspręsti klausimą per privatumo principų III.11 skirsnio d dalies i punkte nustatytą terminą; 2) pasinaudoti nepriklausoma ir nemokama teisių gynimo institucija pagal privatumo principus; ir 3) klausimą per duomenų apsaugos instituciją perduoti Komercijos departamentui ir suteikti jam galimybę visomis pastangomis išspręsti klausimą nemokamai per Komercijos departamento Tarptautinės prekybos administracijos rašte nustatytus terminus.

Šia arbitražo alternatyva negalima remtis, jeigu tas pats asmens reikalavimas dėl tariamo privatumo principų pažeidimų 1) buvo anksčiau nagrinėtas arbitražo tvarka ir dėl jo buvo priimtas įpareigojantis sprendimas, 2) buvo priimtas galutinis teismo sprendimas teismo byloje, kurioje asmuo dalyvavo kaip šalis, arba 3) šalys išsprendė jį anksčiau. Be to, šia alternatyva negalima naudotis, jeigu ES duomenų apsaugos institucija 1) turi įgaliojimus pagal privatumo principų III.5 arba III.9 skirsnį; arba 2) turi įgaliojimus pašalinti tariamą pažeidimą tiesiogiai organizacijoje. DAI įgaliojimai nagrinėti tą patį reikalavimą dėl ES duomenų valdytojo patys savaime nepanaikina galimybės remtis šia arbitražo alternatyva kitame juridiniame asmenyje, kuris nėra pavaldus DAI įgaliojimams.

D. Privalomas sprendimų pobūdis

Asmens sprendimas remtis šia privaloma arbitražo alternatyva yra visiškai savanoriškas. Arbitražo sprendimai bus privalomi visoms arbitražo šalims. Pradėjus arbitražo procedūrą, asmuo netenka galimybės kitame teisme ginti savo teisių dėl to paties tariamo pažeidimo, išskyrus tai, kad jeigu lygiavertė nepiniginė teisių gynimo priemonė nepadėjo visiškai ištaisyti tariamo pažeidimo, asmens pradėta arbitražo procedūra nepanaikins galimybės reikalauti atlyginti nuostolius, kuriuos kitu atveju būtų galima prisieisti teisme.

⁽¹⁾ Privatumo principų I.5 skirsnis.

E. Peržiūra ir reikalavimų užtikrinimas

Asmenys ir „privatumo skydo“ organizacijos galės siekti, kad arbitražiniai sprendimai būtų peržiūrimi teisme ir vykdomi pagal JAV teisę, t. y. Federalinį arbitražo aktą⁽¹⁾. Visos tokios bylos turi būti iškeltos federaliniame apygardos teisme, kurio teritorinė veiklos sritis apima pagrindinę „privatumo skydo“ organizacijos verslo vietą.

Ši arbitražo alternatyva ketinama išspręsti individualius ginčus, o arbitražiniais sprendimais neketinama sukurti atgrasančio arba privalomo precedento bylose, susijusiose su kitomis šalimis, įskaitant būsimą arbitražą arba ES ir JAV teismuose, arba FPK bylose.

F. Arbitražo komisija

Šalys arbitrus pasirenka iš toliau aptarto arbitrų sąrašo.

Laikydami taikytinos teisės, JAV komercijos departamentas ir Europos Komisija sudaro ne mažiau kaip 20 arbitrų, atrinktų atsižvelgiant į jų nepriklausomumą, sąžiningumą ir patirtį, sąrašą. Šiam procesui taikomos toliau nurodytos nuostatos:

Arbitrai:

- 1) bus įtraukti į sąrašą 3 metų terminui, kuris, išskyrus išimtines aplinkybes arba pagrįstą priežastį, atnaujinamas papildomam 3 metų terminui;
- 2) nesivadovauja jokiais kurios nors šalies instrukcijomis arba nėra susiję su kuria nors iš šalių arba bet kuria „privatumo skydo“ organizacija, arba JAV, ES ar bet kuria ES valstybe nare ar bet kuria kita Vyriausybine institucija, valdžios institucija arba teisės saugos institucija arba
- 3) turi turėti teisę verstis advokato praktika JAV ir būti JAV privatumo teisės ekspertais ir turėti žinių apie ES duomenų apsaugos teisę.

G. Arbitražo procedūros

Laikydami taikytinos teisės per 6 mėnesius nuo sprendimo dėl tinkamumo priėmimo Komercijos departamentas ir Europos Komisija sutars priimti galiojančių išsamių JAV arbitražo procedūrų rinkinį (pvz., AAA arba JAMS), kad užtikrintų arbitražo procedūrų reglamentavimą „privatumo skydo“ komisijoje, ir atsižvelgs į toliau nurodytas aplinkybes.

1. Asmuo gali inicijuoti privalomą arbitražą, jeigu įvykdyti pirmiau nurodyti prieš arbitražo procedūrą taikomi reikalavimai, įteikdamas pranešimą organizacijai. Pranešime pateikiama priemonių, kurių pagal C punktą buvo imtasi siekiant įvykdyti reikalavimą, santrauka, tariamo pažeidimo aprašymas ir asmens pasirinkimu – bet kurie patvirtinamieji dokumentai, medžiaga ir (arba) teisės aiškinimas, susijęs su tariamu reikalavimu.

⁽¹⁾ Federalinio arbitražo akto (FAA) 2 skyriuje nustatyta, kad „susitarimas dėl arbitražo arba arbitražo sprendimas atitinkamai sudarytas arba priimtas dėl teisinių santykių, nepaisant to, ar tai sutartiniai, ar nesutartiniai santykiai, kurie laikomi komerciniais, įskaitant sandorį, sutartį arba susitarimą, aprašytą [FAA 2 straipsnyje], patenka į [1958 m. birželio 10 d.] Konvencijos [dėl užsienio arbitražo sprendimų pripažinimo ir vykdymo taikymo sritį, 21 U.S.T. 2519, T.I.A.S. Nr. 6997 („Niujorko konvencija“)]“. JAV kodekso 9 antraštinės dalies 202 straipsnis. FAA taip pat nustatyta, kad „iš tokių santykių, kurie išimtinai yra susiję su Jungtinių Amerikos Valstijų piliečiais, kylantis susitarimas arba arbitražo sprendimas nepatenka į [Niujorko] Konvencijos taikymo sritį, išskyrus atvejus, kai tie santykiai yra susiję su užsienyje esančiu turtu, pagal juos užsienyje turi būti atliekami veiksmai ar vykdomos pareigos, arba jis kitais atžvilgiais yra iš esmės susijęs su viena arba daugiau užsienio valstybių“. Ten pat. Pagal 2 skyrių „bet kuri arbitražo šalis gali kreiptis į bet kurį pagal šį skyrių jurisdikciją turintį teismą, kad šis priimtų patvirtinamąją nutartį dėl arbitražo sprendimo bet kurios kitos arbitražo šalies atžvilgiu. Teismas patvirtina arbitražo sprendimą, nebent nustato vieną iš [Niujorko] Konvencijoje nurodytų arbitražo sprendimo atsisakymo, pripažinimo atidėjimo arba vykdymo pagrindų.“ Ten pat, 207 straipsnis. 2 skyriuje taip pat nustatyta, kad „Jungtinių Amerikos Valstijų apygardos teismai <...> turi dalykinę jurisdikciją nagrinėti <...> ieškinį arba bylą [pagal Niujorko konvenciją], nepaisant ginčo sumos.“ Ten pat, 203 straipsnis.

2 skyriuje taip pat nustatyta, kad „1 skyrius taikomas ieškiniams ir byloms, kurios pagal šį skyrių iškeltos tiek, kiek jis neprieštarauja šiam skyriui arba Jungtinių Amerikos Valstijų ratifikuotai [Niujorko] Konvencijai.“ Ten pat, 208 straipsnis. 1 skyriuje nustatyta, kad „rašytinės <...> sutarties nuostata, kuria patvirtinamas sandoris, susijęs su komercine praktika, kuria siekiama arbitražo tvarka išspręsti ginčą, kilusį dėl tokios sutarties arba sandorio, arba atsisakius atlikti dalį ar visą tokią sutartį ar sandorį, arba susitarimą raštu perduoti arbitražui galiojantį ginčą, kylantį iš tokios sutarties, sandorio arba atsisakymo, galioja, yra nepanaikinama, ir vykdytina, išskyrus atvejus, kai tokiai nuostatai taikomas įstatyme nustatytas arba lygiavertis bet kurios sutarties negaliojimo pagrindas.“ Ten pat, 2 straipsnis. 1 skyriuje taip pat nustatyta, kad „bet kuri arbitražo šalis gali kreiptis į teismą prašydama priimti arbitražo sprendimą patvirtinančią nutartį, o tokį prašymą gavęs teismas privalo patvirtinti tokį sprendimą, išskyrus atvejus, kai sprendimas panaikinamas, pakeičiamas arba ištaisomas, kaip nustatyta [FAA] 10 ir 11 straipsniuose.“ Ten pat, 9 straipsnis.

2. Siekiant užtikrinti, kad tas pats asmens tariamas pažeidimas nebūtų ginamas dvejopomis teisių gynimo priemonėmis arba procedūromis, bus nustatytos procedūros.
3. FPK byla gali vykti lygiagrečiai su arbitražo procedūra.
4. Šiose arbitražo procedūrose negali dalyvauti jokie JAV, ES ar bet kurios ES valstybės narės arba bet kurios kitos Vyriausybės institucijos, valdžios institucijos arba teisėsaugos institucijos atstovai, jeigu ES asmens prašymu ES DAI gali teikti paramą tik rengiant pranešimą, bet ES DAI negali gauti prieigos prie pateiktų faktų arba bet kurios kitos medžiagos, susijusios su šiomis arbitražo procedūromis.
5. Arbitražas vyks Jungtinėse Amerikos Valstijose, o asmuo gali nuspręsti dalyvauti pasitelkdamas vaizdo ar telefonijos paslaugas, kurios jam suteikiamos nemokamai. Asmeninis dalyvavimas nebūtinai.
6. Arbitražo procedūra vyks anglų kalba, nebent šalys susitaria kitaip. Gavus pagrįstą prašymą ir atsižvelgiant į tai, ar asmeniui atstovauja advokatas, asmeniui bus suteiktos nemokamos vertimo žodžiu arbitražo procedūroje paslaugos ir arbitražo medžiagos vertimo raštu paslaugos, išskyrus atvejus, kai komisija nustato, kad konkrečiomis arbitražo procedūromis dėl to arbitražo procedūra taptų nepagrįstai arba neproporcingai brangi.
7. Arbitrai dėl gautos medžiagos laikosi konfidencialumo pareigos ir gali ją naudoti tik tiek, kiek tai susiję su arbitražu.
8. Prireikus gali būti leidžiama susipažinti su faktais apie konkretų asmenį, o dėl tokių faktų šalys laikysis konfidencialumo pareigos ir juos naudos tik tiek, kiek tai susiję su arbitražu.
9. Arbitražo procedūros turėtų būti baigiamos per 90 dienų nuo pranešimo įteikimo atitinkamai organizacijai, išskyrus atvejus, kai šalys susitarė kitaip.

H. Išlaidos

Arbitrai turėtų imtis pagrįstų priemonių, kad kuo labiau sumažintų arbitražo proceso išlaidas arba mokesčius.

Atsižvelgdamas į taikytiną teisę, Komercijos departamentas palengvins fondo įsteigimą o „privatumo skydo“ organizacijos turės mokėti į jį metines įmokas, kurių suma priklausys nuo organizacijos dydžio, ir iš šio fondo bus atlyginamos arbitražo išlaidos, įskaitant mokesčius arbitrams, kurių maksimalus dydis („lubos“) bus nustatytas pasikonsultavus su Europos Komisija. Fondą valdys trečioji šalis, kuri reguliariai teiks fondo veiklos ataskaitas. Atlikdami metinę peržiūrą, Komercijos departamentas ir Europos Komisija peržiūrės fondo veikimą, įskaitant poreikį patikslinti įmokų arba „lubų“ dydį, ir, be kita ko, svarstys arbitražo procedūrų skaičių, išlaidas ir arbitražo procedūrų trukmę, įskaitant abipusį sutarimą, kad „privatumo skydo“ organizacijos nepatirtų pernelyg didelių išlaidų. Ši nuostata netaikoma advokato mokesčiams ar bet kuriam pagal šią nuostatą įsteigtam fondui.

II PRIEDAS

JAV KOMERCIJOS DEPARTAMENTO PASKELBTI ES IR JAV „PRIVATUMO SKYDO“ SISTEMOS PRINCIPAI

I. APŽVALGA

1. Nors Jungtinių Amerikos Valstijų ir Europos Sąjungos bendras tikslas – pagerinti privatumo apsaugą, Jungtinės Amerikos Valstijos privatumą traktuoja kitaip nei Europos Sąjunga. Jungtinėse Amerikos Valstijose taikomas sektorinis metodas, paremtas teisės aktu, reguliavimo ir savireguliacinio deriniu. Atsižvelgdamas į šiuos skirtumus ir siekdamas sudaryti galimybę Jungtinių Amerikos Valstijų organizacijoms pasinaudoti asmens duomenų perdavimo iš Europos Sąjungos į Jungtines Amerikos Valstijas mechanizmais kartu užtikrinant, kad ES duomenų subjektai toliau naudotųsi veiksmingomis saugumo priemonėmis ir apsauga, kurią pagal Europos teisės aktus reikalaujama užtikrinti tvarkant ir ne ES šalis perduotus jų asmens duomenis, Komercijos departamentas, vadovaudamasis jam įstatymu suteiktais įgaliojimais, skelbia šiuos „privatumo skydo“ principus, įskaitant papildomus principus (toliau kartu – privatumo principai), kad skatintų, remtų ir plėtotų tarptautinę prekybą (JAV kodekso 15 antraštinės dalies 1512 straipsnis). Privatumo principai sukurti pasikonsultavus su Europos Komisija, pramonės atstovais ir kitais suinteresuotaisiais subjektais ir skirti prekybai bei komercijai tarp Jungtinių Amerikos Valstijų ir Europos Sąjungos palengvinti. Šių privatumo principų laikosi tik tos Jungtinių Amerikos Valstijų organizacijos, kurios iš Europos Sąjungos gauna asmens duomenis ir atitinka „privatumo skydo“ organizacijos statusą, taigi naudojasi Europos Komisijos sprendimo dėl tinkamumo teikiamais privalumais ⁽¹⁾. Privatumo principai nepakeičia Direktyvą 95/46/EB (toliau – Direktyva) įgyvendinančių nacionalinių nuostatų, kurios taikomos asmens duomenis tvarkant valstybės narėse. Privatumo principais taip pat neribojami privatumo srityje galiojantys išipareigojimai, kurie kitais atvejais taikomi pagal JAV teisę.
2. Kad organizacija galėtų pagal „privatumo skydo“ nuostatas perduoti asmens duomenis iš ES, ji privalo taikyti autosertifikavimo procedūrą, kuria Komercijos departamentui (arba jo paskirtai institucijai) (toliau – Departamentas) patvirtina savo išipareigojimą laikytis privatumo principų. Nors organizacijos sprendimus dėl dalyvavimo „privatumo skydo“ sistemoje priima visiškai savanoriškai, faktinis reikalavimų laikymasis yra privalomas: organizacijos, kurios patvirtina Departamentui savo išipareigojimą laikytis privatumo principų ir viešai apie tai paskelbia, privalo visapusiškai laikytis privatumo principų. Norėdama dalyvauti „privatumo skydo“ sistemoje, organizacija privalo: a) patekti į Federalinės prekybos komisijos (FPK), Transporto departamento arba kitos valstybinės įstaigos, kuri veiksmingai užtikrins privatumo principų laikymąsi, tyrimų ir vykdymo įgaliojimų taikymo sritį (kitos ES pripažintos JAV valstybinės įstaigos ateiityje gali būti nurodomos priede); b) viešai paskelbti savo išipareigojimą laikytis privatumo principų; c) atskleisti visuomenei savo privatumo politiką, atitinkančią šiuos privatumo principus, ir d) visapusiškai juos įgyvendinti. Jeigu organizacija nesilaiko privatumo principų, jai taikomos sankcijos pagal Federalinės prekybos komisijos akto 5 straipsnį, kuriuo draudžiami nesąžiningi ir apgaulingi veiksmai prekybos srityje arba veiksmai, darantys poveikį prekybai (JAV kodekso 15 antraštinės dalies 45 straipsnio a dalis), arba kitus įstatymus arba taisykles, kuriais draudžiami tokie veiksmai.
3. Komercijos departamentas toliau tvarkys ir viešai skelbs patikimą JAV organizacijų, kurios pateikė departamentui autosertifikavimo pažymėjimą ir pareiškė išipareigojancios laikytis privatumo principų, sąrašą (toliau – „privatumo skydo“ sąrašas). „Privatumo skydo“ teikiami privalumai užtikrinami nuo dienos, kurią Departamentas įrašo organizaciją į „privatumo skydo“ sąrašą. Departamentas išbrauks organizaciją iš „privatumo skydo“ sąrašo, jeigu ji savanoriškai nustos dalyvauti „privatumo skydo“ sistemoje arba jeigu ji Departamentui nepateiks metinio patvirtinimo. Jeigu organizacija išbraukiama iš „privatumo skydo“ sąrašo, tai reiškia, kad ji nebegali remtis Europos Komisijos sprendimu dėl tinkamumo ir gauti asmens duomenų iš ES. Organizacija privalo toliau taikyti privatumo principus asmens duomenims, kuriuos gavo dalyvaudama „privatumo skydo“ sistemoje, ir kasmet teikti Departamentui savo išipareigojimo taikyti privatumo principus patvirtinimą ir teikti tokį patvirtinimą tol, kol ji saugo tokią informaciją; priešingu atveju organizacija privalo grąžinti arba ištrinti informaciją arba kitomis leistinomis priemonėmis užtikrinti „tinkamą“ apsaugą. Departamentas iš „privatumo skydo“ sąrašo taip pat išbrauks tas organizacijas, kurios nuolat nesilaikė privatumo principų; šios organizacijos netenka „privatumo skydo“ suteikiamų privalumų ir privalo grąžinti arba ištrinti asmens duomenis, kuriuos gavo dalyvaudamos „privatumo skydo“ sistemoje.
4. Departamentas taip pat tvarkys ir viešai skelbs patikimą JAV organizacijų, kurios anksčiau pateikė Departamentui autosertifikavimo pažymėjimą, tačiau buvo pašalintos iš „privatumo skydo“ sąrašo, registrą. Departamentas aiškiai išpės šias organizacijas, kad jos nebedalyvauja „privatumo skydo“ sistemoje; kad išbraukimas iš „privatumo skydo“ sąrašo reiškia, jog tokios organizacijos nebegali teigti, kad laikosi „privatumo skydo“ nuostatų, ir privalo vengti bet kokių pareiškimų arba klaidinančių veiksmų, iš kurių būtų galima numanyti, kad jos dalyvauja „privatumo skydo“ sistemoje; ir kad tokios organizacijos nebeturi teisės naudotis Europos Komisijos sprendimo dėl tinkamumo teikiamais privalumais, kurie leistų šioms organizacijoms gauti asmens duomenis iš ES. FPK, Transporto

⁽¹⁾ Jeigu Komisijos sprendimas dėl ES ir JAV „privatumo skydo“ suteikiamos apsaugos tinkamumo taikomas Islandijai, Lichtenšteinui ir Norvegijai, „privatumo skydo“ dokumentų rinkinys bus taikomas tiek Europos Sąjungai, tiek šioms trimis šalims. Todėl nuorodos į ES ir jos valstybes nares reiškia nuorodas į Islandiją, Lichtenšteiną ir Norvegiją.

departamentas arba kitos teisėsaugos institucijos gali imtis vykdymo veiksmų dėl organizacijos, kuri toliau teigia dalyvaujanti „privatumo skydo“ sistemoje arba nurodo kitus su „privatumo skydu“ susijusius klaidingus pareiškimus po to, kai buvo išbraukta iš „privatumo skydo“ sąrašo.

5. Šių privatumo principų laikymasis gali būti ribojamas: a) tiek, kiek tai būtina nacionalinio saugumo, viešojo intereso arba teisėsaugos reikalavimams įvykdyti; b) pagal įstatymą, Vyriausybės reglamentą arba teismų praktiką, dėl kurių atsiranda prieštaraujančių pareigų ar aiškių leidimų, jei vykdydama bet kurių tokių leidimų organizacija gali įrodyti, kad privatumo principų nesilaikoma tik tiek, kiek tai būtina atsižvelgiant į organizacijos ginamus viršesnius teisėtus interesus; arba c) jei Direktyvoje arba valstybės narės įstatyme nustatytos išimtys ar leidžiančios nukrypti nuostatos ir jei tokios išimtys ar leidžiančios nukrypti nuostatos taikomos dėl panašių priežasčių. Siekdamas privatumo apsaugos stiprinimo, organizacijos turi stengtis visiškai ir skaidriai laikytis šių privatumo principų, o jei pirmesnio 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 privatumo principus ir (arba) JAV teisę galima pasirinkti kelis variantus, organizacijos pasirinktų geriausią apsaugą suteikiantį variantą.
6. Organizacijos yra įpareigosios taikyti privatumo principus visiems asmens duomenims, perduotiems pagal „privatumo skydo“ nuostatas po to, kai jos tapo „privatumo skydo“ narėmis. Organizacija, kuri nusprendžia praplėsti „privatumo skydo“ privalumus žmoniškųjų išteklių asmeninei informacijai, perduodamai iš ES ir skirtai naudoti darbo santykiuose, privalo tai nurodyti, kai ji patvirtina Departamentui savo įsipareigojimą laikytis papildomo principo dėl autosertifikavimo reikalavimų.
7. Su privatumo principų aiškinimu ir laikymusi susiję klausimai ir su atitinkama „privatumo skydo“ organizacijų privatumo politika susiję klausimai bus sprendžiami taikant JAV teisę, išskyrus atvejus, kai tokios organizacijos įsipareigojo bendradarbiauti su Europos duomenų apsaugos priežiūros institucijomis (DAI). Išskyrus atvejus, kai nurodyta kitaip, visos „privatumo skydo“ principų nuostatos taikomos pagal paskirtį.
8. Apibrėžtys:
 - a) „asmens duomenys“ ir „asmeninė informacija“ – Jungtinių Amerikos Valstijų organizacijos iš Europos Sąjungos gauti ir bet kuria forma įrašyti duomenys apie nustatytos arba galimos nustatyti tapatybės asmenį, kuriems taikoma Direktyva;
 - b) asmens duomenų „tvarkymas“ – bet kokia operacija ar operacijų seka, susijusi su asmens duomenimis, nesvarbu, ar tokios operacijos atliekamos automatinėmis priemonėmis ar ne, pvz., rinkimas, įrašymas, tvarkymas, saugojimas, tikslinimas ir keitimas, gavimas, tikrinimas, naudojimas, atskleidimas ar platinimas, taip pat trynimasis ar sunaikinimas;
 - c) duomenų valdytojas – asmuo ar organizacija, kuri savarankiškai arba kartu su kitais asmenimis ar organizacijomis nustato asmens duomenų tvarkymo tikslus ir priemones.
9. Privatumo principai įsigalioja nuo tos dienos, kurią Europos Komisija galutinai patvirtina sprendimą dėl tinkamumo.

II. PRINCIPAI

1. Pastaba

- a. Organizacija privalo informuoti fizinius asmenis apie:
 - i) savo dalyvavimą „privatumo skydo“ sistemoje ir pateikti nuorodą į svetainę arba svetainės adresą, kuriuo skelbiamas „privatumo skydo“ sąrašas,
 - ii) renkamų asmens duomenų rūšį ir, kai tinkama, organizacijos subjektus arba filialus, kurie taip pat laikosi privatumo principų,

- iii) savo įsipareigojimą visus asmens duomenis, gautus iš ES pagal „privatumo skydo“ nuostatas, tvarkyti pagal privatumo principus,
 - iv) tikslus, kuriais renkami ir naudojami jų asmens duomenys,
 - v) kaip organizacijai pateikti bet kokias užklausas ar skundus, įskaitant bet kurią susijusią ES įmonę, kuri gali atsakyti į tokias užklausas arba nagrinėti skundus,
 - vi) trečiųjų šalių, kurioms ji atskleidžia asmens duomenis, rūšį ir tapatybę ir tikslus, kuriais atskleidžiami tokie duomenys,
 - vii) fizinių asmenų teisę susipažinti su savo asmens duomenimis,
 - viii) sprendimus ir priemones, kurias organizacija siūlo fiziniams asmenims, norintiems riboti jų asmens duomenų naudojimą ir atskleidimą,
 - ix) paskirtą nepriklausomą ginčų sprendimo įstaigą, kuri nagrinėja skundus ir teikia fiziniam asmeniui nemokamas ir tinkamas teisių gynimo paslaugas, taip pat informuoja apie tai, ar tai yra: 1) DAI sudaryta komisija, 2) ES įsisteigęs alternatyvus ginčų nagrinėjimo paslaugų teikėjas arba 3) Jungtinėse Amerikos Valstijose įsisteigęs alternatyvus ginčų nagrinėjimo paslaugų teikėjas,
 - x) tai, ar jai taikomi FPK, Transporto departamento ar bet kurios kitos JAV įgalios valstybinės įstaigos tyrimo ir vykdymo įgaliojimai,
 - xi) galimybę tam tikromis sąlygomis fiziniam asmeniui taikyti privalomą arbitražą,
 - xii) reikalavimą atskleisti asmens duomenis tenkinant teisėtus valdžios institucijų prašymus, įskaitant prašymus dėl nacionalinio saugumo arba teisėsaugos reikalavimų įvykdymo, ir
 - xiii) savo atsakomybę toliau perduodant duomenis trečiosioms šalims.
- b) Toks pranešimas turi būti pateiktas aiškia ir suprantama kalba tada, kai asmenų pirmą kartą prašoma suteikti asmeninę informaciją organizacijai arba kuo greičiau po to, tačiau bet kuriuo atveju prieš organizacijai panaudojant tokią informaciją kitais tikslais, nei tie, dėl kurių duomenis perduodančioji organizacija ją iš pradžių surinko ar tvarkė, arba prieš pirmą kartą ją atskleidžiant trečiajai šaliai.

2. Pasirinkimas

- a) Organizacija privalo suteikti asmenims galimybę pasirinkti (galimybė atsisakyti), ar jų asmeninė informacija gali būti: i) atskleista trečiajai šaliai arba ii) naudojama tikslais, kurie iš esmės neatitinka tų tikslų, dėl kurių ji buvo iš pradžių surinkta, ar vėliau buvo gautas fizinio asmens sutikimas ją naudoti. Fiziniams asmenims turi būti suteikti aiškūs, suprantami ir lengvai prieinami pasirinkimo mechanizmai.
- b) Nukrypstant nuo ankstesnės pastraipos, pasirinkimo galimybės nebūtina užtikrinti, jeigu duomenys atskleidžiami trečiajai šaliai, kuri veikia kaip atstovas, kuris organizacijos vardu arba pagal jos nurodymus atlieka užduotį (-is). Tačiau organizacija su tokiu atstovu visada sudaro sutartį.
- c) Dėl neskelbtinos informacijos (t. y. asmeninės informacijos apie sveikatos būklę, rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, narystę profesinėse sąjungose ar informacijos apie asmens lytinį gyvenimą) organizacijos visada privalo gauti aiškų teigiamą fizinių asmenų sutikimą (galimybė pasirinkti), jeigu tokia informacija turi būti i) atskleista trečiajai šaliai arba ii) naudojama kitu, ne iš pradžių numatytu, tikslu arba fiziniai asmenys duoda tokių sutikimą pasinaudodami pasirinkimo galimybe. Be to, organizacija visuomet turi laikyti iš trečiųjų šalių gautus asmens duomenis neskelbtinais, jei ta trečioji šalis tuos duomenis laiko konfidencialiais ir atitinkamai juos tvarko.

3. Atsakomybė už tolesnį perdavimą

- a) Norėdamos perduoti asmens duomenis trečiajai šaliai, organizacijos privalo laikytis pranešimo ir pasirinkimo principų. Organizacijos taip pat privalo sudaryti sutartį su trečiosios šalies duomenų valdytoju, kurioje nustatoma, kad tokie duomenys gali būti tvarkomi tik ribotais ir konkrečiais tikslais, atitinkančiais fizinio asmens duoto sutikimo sąlygas, ir kad duomenų gavėjas užtikrins tokį pat duomenų apsaugos lygį, kuris užtikrinamas pagal privatumo principus, ir informuos organizaciją, jeigu nustatys, kad ji nebesilaiko šios pareigos. Sutartyje nustatoma, kad tais atvejais, kai tokį sprendimą priima trečioji šalis, duomenų valdytojas nustoja tvarkyti duomenis arba imasi kitų pagrindų ir tinkamų priemonių, kad ištaisytų susidariusią padėtį.
- b) Norėdama perduoti asmens duomenis trečiajai šaliai, kuri veikia kaip atstovas, organizacija privalo: i) perduoti tokius duomenis tik ribotais ir konkrečiais tikslais; ii) patvirtinti, kad atstovas yra įpareigotas užtikrinti ne mažesnę privatumo apsaugos lygį nei tas, kuris užtikrinamas pagal privatumo principus; iii) imtis pagrindų ir tinkamų priemonių, kuriomis būtų užtikrinama, kad atstovas veiksmingai tvarkytų asmens duomenis, kurie buvo perduoti laikantis organizacijos įsipareigojimų, susijusių su privatumo principais; iv) reikalauti, kad atstovas, nustatęs, kad nebegali toliau laikytis pareigos užtikrinti tokį patį apsaugos lygį, kurio reikalaujama pagal privatumo principus, informuotų apie tai organizaciją; v) gavusi pranešimą, įskaitant pranešimą pagal iv punktą, imtis pagrindų ir tinkamų priemonių, kad sustabdytų neteisėtą duomenų tvarkymą ir ištaisytų su tuo susijusią padėtį, ir vi) Departamento prašymu pateikti atitinkamą savo sutarties su tuo atstovu privatumo nuostatų santrauką arba patvirtintą kopiją.

4. Saugumas

- a) Organizacijos, kurios kuria, tvarko, naudoja arba skleidžia asmeninę informaciją, privalo, atsižvelgdamos į su tokios informacijos tvarkymu susijusią riziką ir informacijos pobūdį, imtis pagrindų ir tinkamų priemonių informacijai apsaugoti nuo praradimo, netinkamo naudojimo ir neteisėtos prieigos prie jos, neteisėto atskleidimo, keitimo ir sunaikinimo.

5. Duomenų vientisumas ir tikslo ribojimas

- a) Privatumo principų laikomasi, kai asmens duomenys atitinka tikslus, kuriais jie yra tvarkomi⁽¹⁾. Organizacija neturi teisės tvarkyti asmeninės informacijos tokiais būdais, kurie neatitinka tikslų, dėl kurių ji buvo surinkta ar vėliau buvo gautas asmens sutikimas ją naudoti. Tiek, kiek būtina tokiems tikslams, organizacija privalo imtis pagrindų priemonių užtikrinti, kad asmens duomenys atitiktų numatomą jų naudojimo paskirtį, būtų tikslūs, išsamūs ir naujausi. Organizacija privalo laikytis privatumo principų tol, kol saugo tokią informaciją.
- b) Informacija gali būti saugoma forma, iš kurios galima nustatyti asmens tapatybę arba kuri sudarytų sąlygas nustatyti asmens tapatybę⁽²⁾, tik tiek, kiek ji reikalinga duomenų tvarkymo tikslu, kaip apibrėžta 5 dalies a punkte. Ši pareiga neužkerta kelio organizacijoms tvarkyti asmeninės informacijos ilgiau ir tiek, kiek toks tvarkymas yra pagrįstas atsižvelgiant į archyavimo visuomeniniais interesais, žurnalistikos, literatūros ir meno, mokslinių ar istorinių tyrimų ir statistinių duomenų analizės tikslus. Šiais atvejais tokiam duomenų tvarkymui taikomi kiti privatumo principai ir sistemos nuostatos. Organizacijos turėtų imtis pagrindų ir tinkamų priemonių, kad laikytųsi šios nuostatos.

6. Prieiga prie duomenų

- a) Asmenims turi būti suteikta galimybė susipažinti su organizacijos laikoma asmenine informacija apie juos, ją ištaisyti, pakeisti ar sunaikinti, jei ji būtų netiksli arba tvarkoma pažeidžiant privatumo principus, išskyrus atvejus, kai suteikiant informaciją patiriama našta ar išlaidos būtų neproporcingai didelės, palyginti su pavojumi to asmens privatumui arba būtų pažeistos kitų asmenų teisės.

⁽¹⁾ Priklausomai nuo aplinkybių, su tikslus atitinkantis duomenų tvarkymas gali būti susijęs, pvz., su pagrindais klientų ryšiais, reikalavimų laikymusi ir teisinėmis aplinkybėmis, auditu, saugumu ir sukčiavimo prevencija, organizacijos teisėtų teisių išsaugojimu arba gynimu, arba kitais tikslais, atitinkančiais protingai veikiančio asmens lūkesčius atsižvelgiant į duomenų rinkimą.

⁽²⁾ Šiomis aplinkybėmis jeigu, atsižvelgiant į pagrindas tapatybės nustatymo priemones, kurios, tikėtina, bus naudojamos (be kita ko, atsižvelgiant į tapatybės nustatymo išlaidas ir laiką, reikalingą tapatybei nustatyti, ir technologijas, kurios yra prieinamos duomenų tvarkymo metu), ir duomenų saugojimo formą, organizacija galėtų pagrįstai nustatyti asmens tapatybę arba tai galėtų padaryti trečioji šalis, jeigu jai būtų suteikta prieiga prie duomenų, tai reikšia, kad asmens tapatybę galima nustatyti.

7. Teisių gynimas, reikalavimų užtikrinimas ir atsakomybė

- a) Veiksmingai privatumo apsaugai būtini patikimi mechanizmai, kuriais užtikrinamas privatumo principų laikymasis, fizinių asmenų, kuriems turėjo įtakos privatumo principų nesilaikymas, galimybė ginti teises ir privatumo principų nesilaikančios organizacijos atsakomybė. Būtina, kad tokios institucijos atitiktų šiuos minimalius reikalavimus:
 - i) tai turi būti lengvai prieinamos nepriklausomos teisių gynimo institucijos, kurios operatyviai tirtų ir laikydamosi privatumo principų nemokamai išspręstų kiekvieno asmens skundus bei ginčus ir priteistų žalos atlyginimą, jei tai numatyta taikytinuose teisės aktuose ar privačiojo sektoriaus nuostatose;
 - ii) turi būti nustatytos papildomos procedūros, skirtos patikrinti, ar įmonių pareiškimai ir patikinimai apie privatumo taisyklės yra teisingi ir ar tokios privatumo taisyklės yra taikomos taip, kaip skelbiama ir
 - iii) turi būti nustatytos pareigos išspręsti nesklaidumus, kylančius dėl to, kad organizacijos klaidingai nurodo, kad laikosi privatumo principų, ir nustatyta tokių organizacijų atsakomybė. Sankcijos turi būti pakankamai griežtos, kad priverstų organizacijas laikytis įsipareigojimų.
- b) Organizacijos ir jų pasirinktos nepriklausomos teisių gynimo institucijos greitai reaguos į Departamento pateiktas užklaudas ir prašymus pateikti informaciją, susijusią su „privatumo skydu“. Visos organizacijos privalo greitai reaguoti į skundus dėl privatumo principų nesilaikymo, kuriuos ES valstybės narės valdžios institucijos perdavė per Departamentą. Organizacijos, kurios nusprendė bendradarbiauti su DAI, įskaitant žmogiškųjų išteklių duomenis tvarkančias organizacijas, privalo tiesiogiai bendrauti su tokiomis institucijomis skundų tyrimo ir sprendimo klausimais.
- c) Organizacijos įpareigojamos arbitražo tvarka nagrinėti reikalavimus ir vadovautis I priede nustatytais sąlygomis, jeigu asmuo taikė privalomą arbitražo procedūrą įteikdamas organizacijai atitinkamą pranešimą, taikydamas procedūras ir laikydamasis I priede nustatytų sąlygų.
- d) Jeigu duomenys perduodami toliau, „privatumo skydo“ organizacija atsako už asmens duomenų, gautų pagal „privatumo skydo“ nuostatas, tvarkymą ir tolesnį jų perdavimą trečiajai šaliai, kuri jos vardu veikia kaip atstovas. „Privatumo skydo“ organizacija išlieka atsakinga pagal privatumo principus, jeigu jos atstovas tvarko tokius asmens duomenis su privatumo principais nesuderinamu būdu, nebent organizacija įrodo, kad ji neatsako už įvykį, dėl kurio atsirado žala.
- e) Jeigu FPK arba teismas organizacijos atžvilgiu priima sprendimą dėl reikalavimų nesilaikymo, organizacija viešai skelbia visus su „privatumo skydu“ susijusius FPK pateiktų atitikties arba vertinimo ataskaitų skirsnius ir tai darydama atsižvelgia į konfidencialumo reikalavimus. Departamentas įsteigė specialų DAI kontaktinį centrą, kuris sprendžia visus klausimus, susijusius su tuo, kaip „privatumo skydo“ organizacijos laikosi reikalavimų. FPK prioritetine tvarka nagrinės bylas dėl privatumo principų nesilaikymo, kurias perdavė Departamentas ir ES valstybių narių valdžios institucijos, ir laiku bei laikydamosi galiojančių konfidencialumo apribojimų keisis informacija dėl perduotų bylų su perduodančiosios valstybės valdžios institucijomis.

III. PAPILDOMI PRINCIPAI

1. Neskelbtini duomenys

- a) Nereikalaujama, kad organizacija gautų teigiamą aiškų sutikimą (galimybė pasirinkti) dėl neskelbtinų duomenų, kai:
 - i) duomenys tvarkomi duomenų subjektui ar kitam asmeniui gyvybiškai svarbiais tikslais;
 - ii) duomenis tvarkyti būtina pareiškiant teisinius reikalavimus ar nustatant gynybos argumentus;
 - iii) duomenų reikia medicinos priežiūrai atlikti ar diagnozei nustatyti;
 - iv) duomenys tvarkomi vykdant fondo, asociacijos ar kitos pelno nesiekiančios organizacijos, užsiimančios politine, filosofine, religine ar profesinių sąjungų veikla, teisėtą veiklą, jei tai susiję tik su organizacijos nariais ar reguliariai su jos veikla susijusių reikalų turinčiais asmenimis ir tokie duomenys be duomenų subjekto sutikimo nėra atskleidžiami trečiajai šaliai;

v) duomenys būtini darbo teisinius santykius reglamentuojančiuose teisės aktuose numatytiems organizacijos įsipareigojimams vykdyti arba

vi) tai yra duomenys, kuriuos asmuo aiškiai viešai paskelbė.

2. Su žurnalistika susijusios išimtys

- a) Atsižvelgiant į JAV Konstitucijoje nustatytą spaudos laisvės apsaugą ir Direktyvoje nustatytą išimtį žurnalistinei medžiagai, tais atvejais, kai JAV Konstitucijos Pirmojoje pataisoje nustatytos laisvos spaudos teisės prieštarauja privatumo apsaugos interesams, JAV asmenų ir organizacijų veiklos interesai derinami taikant Pirmosios pataisos normas.
- b) „Privatumo skydo“ principai netaikomi asmeninei informacijai, kuri yra surinkta skelbti, transliuoti ar kitoms visuomenės informavimo apie žurnalistinę medžiagą formoms, – nesvarbu, ar ji būtų panaudota, ar ne, taip pat iš žurnalistikos archyvų išplatintai anksčiau skelbtai informacijai.

3. Netiesioginė atsakomybė

- a) Pagal „privatumo skydo“ principus interneto ar telekomunikacijų paslaugų teikėjai ir kitos organizacijos teisiškai neatsako, jei kitos organizacijos vardu jie tik perduoda, nukreipia, pakeičia ar saugo informaciją. Kaip nustatyta ir pačioje Direktyvoje, „privatumo skydas“ nesukuria netiesioginės atsakomybės. Jei organizacija atlieka tik trečiųjų šalių siunčiamos informacijos perdavimo funkciją ir nenustato tų asmens duomenų tvarkymo tikslų ir priemonių, ji nėra teisiškai atsakinga.

4. Išsamus patikrinimas ir audito atlikimas

- a) Vykdydami savo veiklą auditoriai ir investicijų bankininkai gali tvarkyti asmens duomenis be jo sutikimo ar žinios. Tai leidžiama pagal pranešimo, pasirinkimo ir prieigos prie duomenų principus, atsižvelgiant į toliau aprašytas aplinkybes.
- b) Auditas reguliariai atliekamas akcinėse bendrovėse ir uždarosiose akcinėse bendrovėse, įskaitant „privatumo skydo“ organizacijas. Tokie auditai, visų pirma tie, kurių metu nagrinėjami potencialūs pažeidimo atvejai, gali būti neveiksmingi, jeigu apie juos bus paskelbta iš anksto. Panašiai ir „privatumo skydo“ organizacija, dalyvaujanti potencialiame bendrovių susijungimo arba perėmimo procese, turės arba privalės atlikti išsamų patikrinimą. Tokiu atveju dažnai bus renkami ir tvarkomi asmens duomenys, pvz., informacija apie vyresnius pareigūnus arba kitus svarbias pareigas einančius darbuotojus. Iš anksto paskelbus apie auditą, gali būti pakenkta sandoriui arba netgi pažeidžiamos vertybinių popierių taisyklės. Investicijų bankininkai ir advokatai, dalyvaujantys atliekant išsamų patikrinimą, arba auditą atliekantys auditoriai gali tvarkyti asmens duomenis be jo žinios pirmiausia tuo atveju, kai būtina vykdyti įstatymų ar visuomenės interesų reikalavimus ir esant tokioms aplinkybėms, kai šių privatumo principų taikymas gali pakenkti teisėtiems organizacijos interesams. Tokie teisėti interesai yra organizacijos teisinių įsipareigojimų vykdymo ir teisėtos apskaitos tvarkymo veiklos stebėseną ir poreikis užtikrinti konfidencialumą, susiję su galimais įmonių įsigijimais, susijungimais, bendromis įmonėmis ar kitais panašiais auditorių ir investicijų bankininkų vykdomais sandoriais.

5. Duomenų apsaugos institucijų vaidmuo

- a) Organizacijos įgyvendins savo įsipareigojimą bendradarbiauti su Europos Sąjungos duomenų apsaugos institucijomis (DAI), kaip aprašyta toliau. Pagal „privatumo skydo“ sistemą JAV organizacijos, gaunančios asmens duomenis iš ES, privalo įsipareigoti naudoti veiksmingus mechanizmus, užtikrinančius „privatumo skydo“ principų laikymąsi. Tiksliau tariant, atsižvelgiant į teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principą, dalyvaujančios organizacijos privalo: (a)(i) suteikti fiziniams asmenims, su kuriais yra susiję duomenys, teisių gynimo priemones; (a)(ii) taikyti procedūras, kuriomis patikrinama, ar jų pareiškimai ir patikinimai dėl privatumo praktikos yra tikri, ir (a)(iii) įsipareigoti spręsti problemas, kylančias dėl privatumo principų nesilaikymo ir nustatyti tokioms organizacijoms taikomas sankcijas. Organizacija gali įvykdyti teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principo (a)(i) ir (a)(iii) punktuose nustatytus reikalavimus, jeigu ji laikosi šiame skirsnyje aprašyto bendradarbiavimo su DAI reikalavimo.

- b) Organizacija įsipareigoja bendradarbiauti su DAI, savo pareiškime dėl „privatumo skydo“ autosertifikavimo, kuris teikiamas Komercijos departamentui, nurodydama (žr. papildomą autosertifikavimo principą), kad organizacija:
- i) įsipareigodama bendradarbiauti su DAI, apsisprendė laikytis „privatumo skydo“ teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principo (a)(i) ir (a)(iii) punktų;
 - ii) bendradarbiaus su DAI tiriant ir sprendžiant su „privatumo skydu“ susijusius skundus ir
 - iii) laikysis visų DAI teikiamų rekomendacijų, kai, DAI manymu, organizacijai reikia imtis tam tikrų veiksmų norint laikytis „privatumo skydo“ principų, įskaitant teisės gynimo ir kompensacines priemones asmenims, nukentėjusiems dėl bet kokio privatumo principų pažeidimo, ir raštu patvirtins DAI, kad tokių veiksmų buvo imtasi.
- c) DAI komisijų veikla
- i) DAI bendradarbiaus suteikdamos informaciją ir teikdamos konsultacijas tokiais būdais:
 - 1. DAI konsultacijos bus teikiamos per Europos Sąjungos lygiu įkurtą DAI komisiją, kuri, be kita ko, padės užtikrinti darnų ir nuoseklų požiūrį.
 - 2. Ši komisija konsultuos JAV organizacijas neišspręstų skundų, kuriuos fiziniai asmenys pateikia dėl asmens duomenų, perduotų iš ES pagal „privatumo skydo“ nuostatas, tvarkymo klausimais. Tokiomis konsultacijomis bus siekiama užtikrinti, kad „privatumo skydo“ principai būtų taikomi teisingai ir būtų suteiktos fizinio (-ų) asmens (-ų) teisių gynimo priemonės, kurias DAI laikys tinkamomis.
 - 3. Komisija teiks tokias konsultacijas atsakydama į organizacijų pranešimus ir (arba) tiesiogiai iš fizinių asmenų gautus skundus dėl organizacijų, kurios įsipareigojo bendradarbiauti su DAI, siekdamas laikytis „privatumo skydo“ principų, paskatindama ir, jei reikia, padėdama tokiems fiziniams asmenims iš pradžių pasinaudoti vidinėmis skundų nagrinėjimo procedūromis, kurias gali pasiūlyti organizacija.
 - 4. Konsultacijos bus suteikiamos tik abiem šalims suteikus pagrįstą galimybę pateikti pastabas ir visus pageidaujamus įrodymus. Komisija sieks kuo greičiau suteikti konsultaciją, laikydamosi nustatytos tvarkos reikalavimų. Pagal bendrą taisyklę komisija konsultaciją stengsis suteikti per 60 dienų nuo skundo ar perduotos bylos gavimo, o jei įmanoma – greičiau.
 - 5. Komisija viešai skelbs jai pateiktų skundų svarstymo rezultatus, jei manys, kad tai reikalinga.
 - 6. Komisijoje suteiktos konsultacijos neužtraukia jokios atsakomybės pačiai komisijai ar kuriai nors atskirai DAI.
 - ii) Kaip pažymėta anksčiau, šį ginčų sprendimo būdą pasirinkusios organizacijos privalo įsipareigoti laikytis DAI konsultacijų. Jei organizacija per 25 dienas po konsultacijos suteikimo neįvykdo jos reikalavimų ir nepateikia tinkamo paaiškinimo, komisija praneša apie savo ketinimus perduoti klausimą Federalinei prekybos komisijai, Transporto departamentui ar kitai JAV federalinei ar valstijos institucijai, kad ši imtųsi vykdymo veiksmų apgaulės arba klaidinimo atvejais, arba nusprendžia, kad bendradarbiavimo susitarimas yra rimtai pažeistas ir dėl to turi būti pripažintas niekiniu ir negaliojančiu. Pastaruoju atveju komisija informuos Komercijos departamentą, kad būtų atitinkamai pakoreguotas „privatumo skydo“ sąrašas. Bet koks įsipareigojimo bendradarbiauti su DAI nevykdymas ir „privatumo skydo“ principų nevykdymas pagal FPK akto 5 straipsnį ar panašų normatyvinį aktą bus laikomas apgaulingais veiksmais.
- d) Organizacija, kuri nori, kad „privatumo skydo“ sistemos teikiami privalumai būtų taikomi iš ES įdarbinimo tikslais perduotiems žmoniškųjų išteklių duomenims, privalo įsipareigoti bendradarbiauti su DAI tokių duomenų perdavimo ir tvarkymo srityje (žr. papildomą žmoniškųjų išteklių duomenų principą).

- e) Šią galimybę pasirinkusios organizacijos privalės mokėti metinį mokestį, skirtą grupės veiklos išlaidoms padengti, ir dar papildomai gali būti paprašyta padengti būtinas vertimo išlaidas, susijusias su pranešimų ar skundų prieš organizacijas svarstymu. Metinis mokestis bus ne didesnis kaip 500 JAV dolerių, o mažesnėms bendrovėms jis bus mažesnis.

6. Autosertifikavimas

- a) „Privatumo skydo“ teikiamais privalumais galima naudotis nuo tos dienos, kurią Departamentas įrašo organizacijos pareiškimą dėl autosertifikavimo į „privatumo skydo“ sąrašą po to, kai nustatė, kad pareiškimas yra išsamus.
- b) Norėdama patvirtinti savo dalyvavimą „privatumo skydo“ sistemoje, organizacija gali pateikti Departamentui bendrovės pareigūno organizacijos vardu pasirašytą patvirtinimo pažymėjimą, kad prisijungiama prie „privatumo skydo“, ir jame turėtų būti pateikta bent jau tokia informacija:
- i) organizacijos pavadinimas, pašto adresas, elektroninio pašto adresas, telefono ir fakso numeriai;
 - ii) organizacijos veiklos, susijusios su asmenine informacija, gaunama iš ES, aprašymas ir
 - iii) organizacijos privatumo taisyklių, susijusių su asmenine informacija, aprašymas, įskaitant:
 - 1. jeigu organizacija turi viešą svetainę, – atitinkamą svetainės adresą, kuriuo skelbiama privatumo politika, arba, jeigu organizacija neturi viešos svetainės, kurioje vietoje su privatumo politika gali susipažinti visuomenė;
 - 2. jų faktinio taikymo pradžios datą;
 - 3. kontaktinį biurą, kuris nagrinėja skundus, prašymus leisti susipažinti su duomenimis ir visus kitus klausimus, susijusius su „privatumo skydu“;
 - 4. konkrečią valstybinę įstaigą, turinčią jurisdikciją nagrinėti bet kokius skundus prieš organizaciją dėl galimų nesąžiningų ar apgaulingų veiksmų ir privatumo teisės aktų ar taisyklių pažeidimų (kuri yra įtraukta į privatumo principų sąrašą arba būsimą privatumo principų priedą);
 - 5. bet kokių privatumo programų, kuriose dalyvauja organizacija, pavadinimus;
 - 6. tikrinimo metodą (pvz., vidaus, trečiosios šalies) (žr. papildomą tikrinimo principą) ir
 - 7. nepriklausomą teisių gynimo instituciją, į kurią galima kreiptis tiriant neišspręstus skundus.
- c) Jeigu organizacija nori, kad jos „privatumo skydo“ teikiami privalumai būtų taikomi žmogiškųjų išteklių informacijai, perduotai iš ES ir skirtai naudoti darbo santykiuose, ji tai gali daryti tais atvejais, kai privatumo principų sąrašė arba būsimame privatumo principų priede nurodyta valstybinė įstaiga turi jurisdikciją nagrinėti organizacijoms pareikštus reikalavimus, kylančius dėl žmogiškųjų išteklių informacijos tvarkymo. Be to, organizacija privalo tai nurodyti savo autosertifikavimo pažymėjime ir paskelbti savo išpareigojimą bendradarbiauti su atitinkama ES valdžios institucija ar institucijomis pagal taikomą papildomą žmogiškųjų išteklių duomenų ir duomenų apsaugos institucijų vaidmens principą ir patvirtinti, kad ji toliau paisys tokių valstybinių įstaigų pateiktų konsultacijų. Organizacija taip pat privalo pateikti Departamentui savo žmogiškųjų išteklių privatumo politikos kopiją ir informaciją, kurioje vietoje su privatumo politika gali susipažinti nukentėję darbuotojai.
- d) Departamentas tvarkys „privatumo skydo“ organizacijų, kurios pateikia užpildytus autosertifikavimo pažymėjimus, sąrašą ir taip užtikrins „privatumo skydo“ teikiamų privalumų prieinamumą, taip pat atnaujins tokių sąrašą pagal metinius pakartotinius autosertifikavimo pažymėjimus ir pranešimus, gautus pagal papildomą ginčų nagrinėjimo ir vykdymo principą. Tokie autosertifikavimo pažymėjimai turi būti teikiami ne rečiau kaip

kartą per metus; priešingu atveju organizacija bus išbraukta iš „privatumo skydo“ sąrašo ir nebegalės naudotis „privatumo skydo“ teikiamais privalumais. Tiek „privatumo skydo“ sąrašas, tiek organizacijų pateikti pažymėjimai bus skelbiami viešai. Visos organizacijos, kurias Departamentas įrašė į „privatumo skydo“ sąrašą, taip pat privalo savo atitinkamos paskelbtos privatumo politikos pareiškimuose nurodyti, kad laikosi „privatumo skydo“ principų. Jeigu organizacijos privatumo politika skelbiama internete, joje būtina pateikti saitą į „privatumo skydo“ svetainę, taip pat saitą į nepriklausomos teisių gynimo institucijos, į kurią galima kreiptis tiriant neišspręstus skundus, svetainę arba skundo pateikimo formą.

- e) „Privatumo skydo“ principai taikomi iš karto nuo jų patvirtinimo momento. Pripažindamos, kad privatumo principai darys poveikį komerciniams santykiams su trečiosiomis šalimis, organizacijos, kurios patvirtina dalyvavimą „privatumo skydo“ sistemoje per pirmuosius du mėnesius nuo sistemos įsigaliojimo datos, esamus komercinius santykius su trečiosiomis šalimis kuomet greičiau suderina su atskaitomybės už tolesnį perdavimą principu ir bet kuriuo atveju ne vėliau kaip per devynis mėnesius nuo dienos, kurią jos patvirtino dalyvaujančios „privatumo skydo“ sistemoje. Organizacijos, kurios per šį laikiną terminą perdavė duomenis trečiajai šaliai, i) taiko pranešimo ir pasirinkimo principus ir, ii) jeigu asmens duomenys perduodami trečiajai šaliai, kuri veikia kaip atstovas, patvirtina, kad atstovas yra įpareigotas užtikrinti bent jau tokį pat apsaugos lygį, kurio reikalaujama pagal privatumo principus.
- f) Organizacija „privatumo skydo“ principus privalo taikyti visiems asmens duomenims, kuriuos ji, dalyvaudama „privatumo skydo“ sistemoje, gavo iš ES. Įsipareigojimas laikytis „privatumo skydo“ principų dėl asmens duomenų, gautų per laikotarpį, kurį organizacija naudoja „privatumo skydo“ privalumais, galioja neterminuotai. Toks įsipareigojimas reiškia, kad organizacija ir toliau taikys privatumo principus tokiems duomenims, kol juos laiko, naudoja ar atskleidžia, net jei dėl kokios nors priežasties nustoja dalyvauti „privatumo skydo“ sistemoje. Organizacija, kuri nustoja dalyvauti „privatumo skydo“ sistemoje, tačiau nori išlaikyti tokius duomenis, privalo kasmet patvirtinti Departamentui savo įsipareigojimą toliau taikyti privatumo principus arba kitomis leistinomis priemonėmis (pvz., sudarydamos sutartį, kurioje visapusiškai atsispindi atitinkamų Europos Komisijos nustatytų standartinių sutarčių sąlygų reikalavimai) užtikrinti „pakankamą“ apsaugą; priešingu atveju organizacija privalo grąžinti arba ištrinti informaciją. Organizacija, kuri nustoja dalyvauti „privatumo skydo“ sistemoje, privalo iš visos susijusios privatumo politikos pašalinti bet kokias nuorodas į „privatumo skydą“, iš kurių būtų galima numanyti, kad organizacija toliau aktyviai dalyvauja „privatumo skydo“ sistemoje ir turi teisę naudotis jos teikiamais privalumais.
- g) Organizacija, kuri dėl bendrovių susijungimo ar teisių perėmimo nustoja egzistuoti kaip atskiras juridinis asmuo, apie tai privalo iš anksto informuoti Departamentą. Pranešime taip pat reikėtų nurodyti, ar ją įsigijęs juridinis asmuo ar po susijungimo susikūręs juridinis asmuo i) toliau laikysis „privatumo skydo“ principų pagal bendrovių susijungimą ar teisių perėmimą reglamentuojantį teisės aktą arba ii) nuspręs patvirtinti savo įsipareigojimą laikytis „privatumo skydo“ principų ar imtis kitų apsaugos priemonių, pvz., raštu sudaryti sutartį, kuri užtikrintų, kad bus laikomasi „privatumo skydo“ principų. Jei i ir ii punktai netaikomi, visi „privatumo skydo“ sistemoje gauti asmens duomenys turi būti nedelsiant ištrinti.
- h) Jeigu organizacija dėl kokios nors priežasties nustoja dalyvauti „privatumo skydo“ sistemoje, ji privalo pašalinti visus pareiškimus, iš kurių būtų galima numanyti, kad ji toliau dalyvauja „privatumo skydo“ sistemoje arba turi teisę naudotis „privatumo skydo“ teikiamais privalumais. Naudojamas ES ir JAV „privatumo skydo“ sertifikavimo ženklas taip pat turi būti pašalintas. Už bet koki visuomenės klaidinimą dėl organizacijos įsipareigojimo laikytis „privatumo skydo“ principų ją gali bausti FPK ar kita atitinkama Vyriausybinių įstaigų. Už klaidingos informacijos pateikimą Departamentui gali būti baudžiama pagal Melagingų parodymų aktą (JAV kodekso 18 antraštinės dalies 1001 straipsnis).

7. Tikrinimas

- a) Organizacijos privalo patvirtinti papildomas procedūras, kurias taikys tikrindamos, ar jų pareiškimai ir patikinimai apie jų „privatumo skydo“ privatumo praktiką yra teisingi ir ar ta privatumo praktika įgyvendinta, kaip nurodyta „privatumo skydo“ principuose ir jų nepažeidžiant.
- b) Siekdama laikytis teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principo reikalavimų dėl tikrinimo, organizacija privalo tikrinti tokius pareiškimus ir patikinimus atlikdama vidaus vertinimą arba išorės atitikties peržiūrą.
- c) Taikant vidaus vertinimo būdą, tokiu tikrinimu turi būti nustatyta, ar organizacijos paskelbta privatumo politika dėl asmeninės informacijos, gautos iš ES, yra teisinga, išsami, aiškiai išdėstyta, visiškai vykdoma ir prieinama. Ji taip pat privalo nurodyti, kad jos privatumo politika atitinka „privatumo skydo“ principus; kad asmenys informuojami apie visas vidaus skundų nagrinėjimo procedūras ir apie nepriklausomą mechanizmą, kuriais gali pasinaudoti teikdami skundus; kad ji yra nustačiusi darbuotojų mokymo apie privatumo politikos

įgyvendinimą procedūras ir numachiui drausminę atsakomybę už privatumo politikos nesilaikymą ir kad ji yra nustačiusi vidaus procedūras dėl periodinių objektyvių pirmiau išdėstytų reikalavimų laikymosi peržiūrų. Bent kartą per metus turi būti surašytas kompanijos pareigūno ar kito įgalioto organizacijos atstovo pasirašytas autosertifikavimo pareiškimas, jis turi būti pateikiamas asmenų prašymu atliekant tyrimą arba esant nusiskundimų dėl reikalavimų nesilaikymo.

- d) Jei organizacija pasirenka išorinius reikalavimų laikymosi patikrinimus, jais turi būti nustatyta, ar organizacijos privatumo taisyklės dėl asmeninės informacijos, gautos iš ES, atitinka „privatumo skydo“ principus, ar jų laikomasi ir ar asmenys yra informuoti apie mechanizmus, kuriais naudodamiesi jie gali reikšti nusiskundimus. Patikrinimai gali būti atliekami tokiais (tačiau nebūtinai vien tokiais) būdais: auditu, atsitiktiniais patikrinimais, panaudojant „spąstų“ metodą arba pasitelkiant technologijos priemones. Bent kartą per metus turi būti surašyta tikrintojų, kompanijos pareigūno ar kito įgalioto organizacijos atstovo pasirašyta išorinių reikalavimų laikymosi patikrinimą patvirtinanti ataskaita ir ji turi būti pateikiama asmenų prašymu atliekant tyrimą arba esant nusiskundimų dėl reikalavimų nesilaikymo.
- e) Organizacijos turi tvarkyti savo „privatumo skydo“ privatumo politikos praktinio vykdymo registrus ir pateikti juos už nusiskundimų nagrinėjimą atsakingai nepriklausomai institucijai ar agentūrai, kurios jurisdikcija aprėpia nesąžiningų ir apgaulingų veiksmų tyrimą, kai to pareikalaujama atliekant tyrimą ar esant nusiskundimų dėl reikalavimų nesilaikymo. Organizacijos taip pat privalo greitai reaguoti į Departamento užklausas ir kitus prašymus pateikti informaciją, susijusius su tuo, kaip organizacija laikosi privatumo principų.

8. Galimybė susipažinti su duomenimis

a) Galimybės susipažinti su duomenimis principo praktiniai aspektai

- i) Pagal „privatumo skydo“ principus galimybė susipažinti su duomenimis yra esminis privatumo apsaugos principas. Taip leidžiama asmenims patikrinti saugomos informacijos apie juos tikslumą. Galimybės susipažinti su duomenimis principas reiškia, kad fiziniai asmenys turi teisę:
 - 1. gauti organizacijos patvirtinimą, ar ji tvarko jo asmens duomenis ⁽¹⁾;
 - 2. gauti tokius duomenis, kad galėtų patikrinti jų tikslumą ir tvarkymo teisėtumą, ir
 - 3. ištaisyti, pakeisti arba ištrinti duomenis, kai jie yra netikslūs arba tvarkomi pažeidžiant privatumo principus.
- ii) Fiziniai asmenys neprivalo nurodyti prašymų leisti susipažinti su savo asmens duomenimis motyvų. Atsakydamos į fizinio asmens prašymą leisti susipažinti su duomenimis, organizacijos pirmiausia turėtų įvertinti, dėl kokios (-ių) priežasties (-ių) toks prašymas buvo pateiktas. Pavyzdžiui, jei prašymas leisti susipažinti su duomenimis yra neaiškus ar didelės apimties, organizacija galėtų pabendrauti su asmeniu, kad geriau suprastų prašymo motyvus, ir nustatyti tinkamiausią informaciją. Organizacija gali pasiteirauti, su kuriais organizacijos padaliniais asmuo bendravo, ir (arba) apie informacijos, su kuria prašoma leisti susipažinti, pobūdį (ar panaudojimą).
- iii) Kadangi galimybė susipažinti su duomenimis yra esminio pobūdžio principas, organizacijos turėtų visuomet tinkamai pasistengti suteikti galimybę susipažinti su duomenimis. Pavyzdžiui, kai tam tikrą informaciją reikia apsaugoti ir ją galima lengvai atskirti nuo kitos informacijos, su kuria prašoma leisti susipažinti, organizacija turėtų atskirti apsaugotą informaciją ir pateikti tik tą, kurios prašoma. Jei kuriuo nors konkrečiu atveju organizacija nusprendžia, kad galimybė susipažinti su duomenimis turėtų būti ribojama, ji turi prašančiam asmeniui nurodyti priežastį, dėl kurios taip nusprendė ir pasiūlyti papildomą būdą, kuriuo naudodamasis jis gali prašyti leisti susipažinti su duomenimis.

b) Pareiga teikti informaciją arba su tuo susijusios išlaidos

- i) Prieiga prie duomenų gali būti ribojama išimtinėmis aplinkybėmis, kai būtų pažeistos teisėtos kitų asmenų, išskyrus prašymą pateikusį fizinį asmenį, teisėtos teisės arba kai pareiga pateikti informaciją arba su tuo susijusios išlaidos būtų neproporcingos, atsižvelgiant į atitinkamo fizinio asmens privatumui kylančią riziką. Informacijos pateikimo išlaidos ir pareiga pateikti informaciją yra svarbūs veiksniai ir į juos reikėtų atsižvelgti, tačiau jie nėra lemiami nustatant, ar informacijos suteikimas yra pagrįstas.

⁽¹⁾ Organizacija turėtų atsakyti į fizinių asmenų prašymus nurodyti duomenų tvarkymo tikslus, tvarkomų asmens duomenų kategorijas ir gavėjus, kuriems atskleidžiami asmens duomenys, arba tokių gavėjų kategorijas.

- ii) Pavyzdžiui, jei fizinio asmens duomenys naudojami sprendimams, kurių įtaka tam asmeniui didžiulė (pvz., atimtų ar suteiktų svarbią naudą, kaip antai draudimo, hipotekos ar darbo suteikimo reikalais), tuomet, laikymasi kitų šių papildomų principų, organizacija turėtų atskleisti informaciją net jei ją gana sunku ar brangu suteikti. Jeigu prašomi asmens duomenys nėra konfidencialūs arba nėra naudojami priimančiam sprendimui, kurie turės didelį poveikį fiziniam asmeniui, tačiau jau yra prieinami ir juos galima pateikti nepatiriant didelių išlaidų, organizacija turėtų leisti susipažinti su tokia informacija.

c) Konfidenciali komercinė informacija

- i) Konfidenciali komercinė informacija yra tokia informacija, kurią organizacija stengiasi apsaugoti nuo atskleidimo, jei jos atskleidimas padėtų rinkos konkurentams. Organizacijos gali atsisakyti suteikti visišką prieigą arba riboti pateikiamą informaciją, jei ją suteikus būtų atskleista jos pačios konfidenciali komercinė informacija, pvz., organizacijos padarytos rinkodaros išvados ar sudarytos klasifikacijos, arba kitų organizacijų konfidenciali komercinė informacija, kuriai taikomi sutartiniai konfidencialumo įsipareigojimai.
- ii) Jei konfidencialią komercinę informaciją galima lengvai atskirti nuo kitų asmens duomenų, su kuriais prašoma leisti susipažinti, organizacija turėtų atskirti apsaugotą informaciją ir pateikti nekonfidencialią informaciją.

d) Duomenų bazių organizavimas

- i) Organizacija asmeniui informaciją apie atitinkamus asmens duomenis gali suteikti juos atskleisdama ir asmeniui nebūtina naudotis prieiga prie organizacijos duomenų bazės.
- ii) Prieiga turi būti suteikiama atsižvelgiant į tai, kiek asmens duomenų saugo organizacija. Pats galimybės susipažinti su duomenimis principas neįpareigoja išlaikyti, turėti, pertvarkyti ar restruktūrizuoti asmeninės informacijos kompiuterinių bylų.

e) Kokiais atvejais prieiga gali būti ribojama?

- i) Kadangi organizacijos visada privalo sąžiningai stengtis leisti asmenims susipažinti su savo asmens duomenimis, aplinkybės, kuriomis organizacija gali riboti tokią prieigą, yra ribotos, o visos ribotos prieigos priežastys turi būti konkrečios. Kaip nustatyta Direktyvoje, organizacija gali riboti prieigą prie informacijos, jei ją atskleidus galėtų būti pažeista svarbių kitų visuomenės interesų apsauga, pvz., nacionalinio saugumo, gynybos ar visuomenės saugumo. Be to, tais atvejais, kai asmens duomenys tvarkomi vien tyrimo ar statistinių duomenų rinkimo tikslais, galima atsisakyti suteikti prieigą prie informacijos. Kitos prieigos prie informacijos atsisakymo ar ribojimo priežastys yra tokios:
 - 1. trukdymas vykdyti teisės aktus ar prižiūrėti jų vykdymą arba trukdymas nagrinėti privačias bylas, įskaitant teisės pažeidimų prevenciją, tyrimą ar atskleidimą arba sąžiningo teismo proceso teisę;
 - 2. informacijos atskleidimas, kai būtų pažeistos kitų asmenų teisėtos teisės arba svarbūs interesai;
 - 3. teisinių ar kitų profesinių lengvatų ar įsipareigojimų pažeidimas;
 - 4. kenkimas darbuotojo saugos tyrimui arba skundų procedūrai, arba dėl darbuotojų pareigų perėmimo ir įmonių reorganizavimo;
 - 5. pakenkimas konfidencialumui, kuris gali būti būtinas stebėsenos, inspektavimo ar kontrolės funkcijoms, susijusioms su patikimu valdymu, arba ateityje, arba vykstančioms deryboms, kuriose dalyvauja organizacija.
- ii) Organizacija, kuri taiko išimtį, turi pareigą įrodyti jos būtinybę ir prieigos ribojimo priežastis, taip pat kontaktinį centrą, į kurį asmenys galėtų kreiptis.

f) Teisė gauti patvirtinimą ir mokėti informacijos pateikimo išlaidoms kompensuoti

- i) Asmuo turi teisę gauti patvirtinimą, ar ši organizacija turi jo asmens duomenų. Asmuo taip pat turi teisę gauti su jo asmeniu susijusius asmens duomenis. Organizacija už tai gali imti mokestį, kuris nėra pernelyg didelis.
- ii) Mokesčio ėmimas gali būti pagrįstas, pvz., kai prašymai pateikti informaciją akivaizdžiai yra per didelės apimties, visų pirma dėl jų pasikartojančio pobūdžio.
- iii) Negalima atsakyti suteikti prieigą dėl su išlaidomis susijusių priežasčių, jei asmuo pasisiūlo apmokėti išlaidas.

g) Pasikartojantys arba nepagrįsti prašymai leisti susipažinti su duomenimis

Organizacija gali imti pagrįstą mokestį ir apriboti tenkinamų vieno asmens reikalavimų skaičių per tam tikrą laikotarpį. Nustatydama tokius apribojimus, organizacija turi įvertinti tokius veiksnius: informacijos atnaujinimo dažnumą, informacijos naudojimo paskirtį ir pobūdį.

h) Apgaulingi prašymai leisti susipažinti su duomenimis

Organizacija neprivalo leisti susipažinti su duomenimis, jei jai pateikiama nepakankamai informacijos, kad ji galėtų patvirtinti reikalavimą pateikuso asmens tapatybę.

i) Atsakymų pateikimo terminas

Organizacijos į prašymus leisti susipažinti su informacija turėtų atsakyti per protingą terminą, tinkamu būdu ir asmeniui suprantama forma. Organizacija, kuri duomenų subjektams informaciją teikia reguliariai, gali patenkinti asmens prašymą leisti susipažinti su duomenimis reguliariai juos atskleisdama, jeigu toks atskleidimas nebūtų pernelyg pavėluotas.

9. **Žmogiškųjų išteklių duomenys**

a) „Privatumo skydo“ nuostatų taikymo sritis

- i) Jeigu ES organizacija perduoda savo darbuotojų (buvusių ar esamų) asmens duomenis, kurie buvo surinkti juos įdarbinant, „privatumo skydo“ sistemoje dalyvaujančiai patronuojančiai bendrovei, susijusiai įmonei ar nesusijusiai paslaugų teikėjui Jungtinėse Amerikos Valstijose, tokiems duomenims taikomi „privatumo skydo“ suteikiami privalumai. Tokiais atvejais informacija prieš ją perduodant yra renkama ir tvarkoma laikantis tos ES šalies, kurioje ji buvo surinkta, teisės aktų, ir būtina laikytis visų tuose teisės aktuose numatytų jos perdavimo sąlygų ar apribojimų.
- ii) „Privatumo skydo“ principai galioja tik tuomet, kai yra perduodami ar prieinami asmenį identifikuojantys įrašai arba įrašai, iš kurių galima nustatyti asmens tapatybę. Statistiniai pranešimai, sudaryti remiantis apibendrintais įdarbinimo duomenimis, kuriuose nėra asmens duomenų arba naudojami nuasmeninti duomenys, nėra susiję su privatumo klausimais.

b) Pranešimo ir pasirinkimo principų taikymas

- i) JAV organizacija, gavusi informaciją apie darbuotojus iš ES „privatumo skydo“ sistemos, gali atskleisti ją trečiosioms šalims arba naudoti ją įvairiems tikslams tik laikydamosi pranešimo ir pasirinkimo principų. Pavyzdžiui, jei organizacija ketina panaudoti darbo santykių metu surinktą asmeninę informaciją su įdarbinimu nesusijusiais tikslais, pvz., rinkodaros pranešimuose, JAV organizacija prieš tai privalo suteikti susijusiems asmenims būtiną pasirinkimo galimybę, nebent jie jau būtų leidę naudoti informaciją tokiems tikslams. Toks naudojimas negali būti nesusiderinamas su tikslais, kuriais asmeninę informaciją buvo surinkta arba vėliau ją leido rinkti pats asmuo. Be to, draudžiama atsižvelgiant į pasirinkimą apriboti įdarbinimo galimybes arba imtis kokių nors sankcijų prieš tokius darbuotojus.

- ii) Atkreiptinas dėmesys, kad tam tikromis plačiai taikomomis perdavimo iš kai kurių ES valstybių narių sąlygomis neleidžiama naudoti tokios informacijos kitais tikslais net perdavus ją už ES ribų ir tokias sąlygas būtina vykdyti.
- iii) Be to, darbdaviai turi pagrįstai stengtis vykdyti darbuotojų privatumo pageidavimus. Tai, pavyzdžiui, gali būti daroma apribojant prieigą prie asmens duomenų – kai kuriuos duomenis nuasmeninant, priskiriant jiems kodus ar pseudonimus, kai tikrieji vardai valdymo tikslais nebūtini.
- iv) Laikotarpiui, būtinam, kad nebūtų pakenkta organizacijos gebėjimams, kai paaugštinamos pareigos, skiriama į pareigas ar priimami kiti panašūs darbo santykių sprendimai, organizacija neprivalo pranešti ir suteikti pasirinkimo.

c) Prieigos prie duomenų principo taikymas

Papildomą prieigos prie duomenų principą sudaro nuostatos, kuriomis pateisinamas atsisakymas suteikti reikalaujamą prieigą prie žmogiškųjų išteklių informacijos arba jos apribojimas. Žinoma, darbdaviai Europos Sąjungoje privalo laikytis vietinių teisės aktų ir užtikrinti, kad Europos Sąjungos darbuotojai turėtų prieigą prie tokios informacijos, kaip reikalaujama jų šalių teisės aktuose, neatsižvelgiant į duomenų tvarkymo ir saugojimo vietą. Pagal „privatumo skydo“ principus reikalaujama, kad tokius duomenis tvarkanti organizacija Jungtinėse Amerikos Valstijose bendradarbiautų suteikiant tokią prieigą tiesiogiai arba per ES darbdavį.

d) Reikalavimų užtikrinimas

- i) Jei asmens duomenys naudojami tik darbo santykiams, darbuotojo atžvilgiu už duomenis atsakinga lieka visų pirma ES organizacija. Tai reiškia, kad Europos darbuotojams pasiskundus dėl jų duomenų apsaugos teisių pažeidimų ir jiems nesant patenkintiems vidinio patikrinimo rezultatais, skundo nagrinėjimo ir apeliacijos procedūromis (arba bet kokiomis taikomomis skundų darbovietės administracijai procedūromis pagal sutartį su profesine sąjunga), tie skundai turi būti adresuoti valstybinei ar nacionalinei duomenų apsaugos ar darbo institucijai, kurios jurisdikcijai priklauso darbuotojų darbovietė. Tai apima atvejus, kai JAV organizacija, gavusi informaciją iš darbdavio, atsako už tariamą netinkamą asmens duomenų tvarkymą, todėl tai reiškia „privatumo skydo“ principų pažeidimą. Tai yra veiksmingiausias būdas spręsti klausimus dėl dažnai vienu kitiems prieštaraujančių teisių ir įsipareigojimų, nustatytų vietiniais darbo teisės aktais, darbo sutartimis ir duomenų apsaugos įstatymu.
- ii) „Privatumo skydo“ sistemai priklausanti JAV organizacija, naudojanti darbo santykiams iš Europos Sąjungos perduodamus ES žmogiškųjų išteklių duomenis, kuri nori, kad perduodant tokius duomenis būtų taikomi „privatumo skydo“ principai, privalo įsipareigoti bendradarbiauti su kompetentingomis ES institucijomis joms vykdant tyrimus ir laikytis jų konsultacijų.

e) Atsakomybės už tolesnį perdavimą principo taikymas

Tenkindama nereguliarus su įdarbinimu susijusius veiklos poreikius, kurie apima pagal „privatumo skydą“ perduotų asmens duomenų tvarkymą, pvz., skrydžio ar viešbučio kambario užsakymas arba draudimas, „privatumo skydo“ organizacija nedidelio skaičiaus darbuotojų asmens duomenis duomenų valdytojams gali perduoti netaikydama prieigos prie duomenų principo arba nesudarydama sutarties su duomenų valdytoju, kuris veikia kaip trečioji šalis, kaip kitais atvejais to reikalaujama pagal atsakomybės už tolesnį perdavimą principą, jeigu ta „privatumo skydo“ organizacija laikėsi pranešimo ir pasirinkimo principų.

10. Privalomos sutartys dėl tolesnio perdavimo

a) Duomenų tvarkymo sutartys

- i) Kai duomenys iš ES į Jungtines Amerikos Valstijas perduodami vien tvarkymo tikslais, sutartį reikės sudaryti, nepaisant to, ar duomenų tvarkytojas dalyvauja „privatumo skydo“ sistemoje.

- ii) Europos Sąjungoje duomenų valdytojai visuomet privalo sudaryti sutartį, jei duomenys perduodami vien tvarkyti, nesvarbu, ar duomenys būtų tvarkomi ES, ar už jos ribų ir ar duomenų tvarkytojas dalyvauja „privatumo skydo“ sistemoje. Sutarties tikslas – užtikrinti, kad duomenų tvarkytojas:

1. veiktų tik pagal duomenų valdytojo nurodymus;
2. pasirinktų tinkamomis techninėmis ir organizacinėmis priemonėmis asmens duomenims apsaugoti nuo atsitiktinio arba neteisėto sunaikinimo, arba atsitiktinio praradimo, pakeitimo, neteisėto atskleidimo arba tikrinimo ir aiškiai žinotų, ar duomenis leidžiama perduoti toliau, ir,
3. atsižvelgiant į duomenų tvarkymo pobūdį, padėtų duomenų valdytojui pateikti atsakymus asmenims, kurie pasinaudoja savo teisėmis pagal privatumo principus.

- iii) Kadangi „privatumo skydo“ dalyviai suteikia pakankamą apsaugą, sutarčių su „privatumo skydo“ dalyviais vien duomenų tvarkymo tikslais nereikia iš anksto patvirtinti (arba tokių patvirtinimą ES valstybės narės suteikia automatiškai), tačiau sutartis, sudaromas su „privatumo skydo“ sistemai nepriklausančiais ar nesuteikiančiais pakankamos apsaugos duomenų gavėjais, reikėtų iš anksto patvirtinti.

b) Duomenų perdavimas korporacijų arba įmonių kontroliuojamoje grupėje

Kai asmeninė informacija perduodama tarp dviejų duomenų valdytojų korporacijų arba įmonių kontroliuojamoje grupėje, pagal atsakomybės už tolesnį perdavimą principą sutartį sudaryti ne visada būtina. Korporacijų arba įmonių kontroliuojamoje grupėje veikiantys duomenų valdytojai tokius duomenų perdavimus gali grįsti kitais dokumentais, pvz., ES privalomomis įmonių taisyklėmis arba kitomis grupėje taikomomis priemonėmis (pvz., atitikties ir kontrolės programomis), kuriomis užtikrinama nuolatinė asmeninės informacijos apsauga pagal „privatumo skydo“ principus. Tokiais atvejais „privatumo skydo“ organizacija išlieka atsakinga už „privatumo skydo“ principų laikymąsi.

c) Duomenų perdavimas tarp duomenų valdytojų

Jei vienas duomenų valdytojas perduoda duomenis kitam, duomenų gavėjas nebūtinai turi būti „privatumo skydo“ organizacija arba turėti nepriklausomą teisių gynimo instituciją. „Privatumo skydo“ organizacija privalo sudaryti sutartį su duomenų valdytojo statusą turinčia trečiaja šalimi duomenų gavėja, kuria užtikrinamas toks pat apsaugos lygis kaip ir „privatumo skyde“, ir nereikalauti, kad ta trečioji šalis duomenų valdytoja būtų „privatumo skydo“ organizacija arba turėtų nepriklausomą teisių gynimo instituciją, jeigu ji naudoja lygiavertį mechanizmą.

11. Ginčų sprendimas ir reikalavimų užtikrinimas

- a) Teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principo nuostatose nustatyti „privatumo skydo“ užtikrinimui taikomi reikalavimai. Principo (a)(ii) punkte nustatytų reikalavimų įvykdymo tvarka nustatyta papildomo tikrinimo principo nuostatose. Šio papildomo principo nuostatose aptariami (a)(i) ir (a)(iii) punktai, kuriuose reikalaujama užtikrinti nepriklausomų teisių gynimo institucijų veikimą. Tokie mechanizmai gali būti įvairūs, tačiau jie privalo atitikti teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principo reikalavimus. Organizacijos reikalavimus įvykdo taip: i) laikydamosi privačiojo sektoriaus sukurtų privatumo programų, kurių taisyklėse įtvirtinti „privatumo skydo“ principai ir kuriose nustatyti veiksmingi teisių gynimo mechanizmai, atitinkantys teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principų reikalavimus; ii) laikydamosi teisinių arba reguliavimo priežiūros institucijų reikalavimų, susijusių su individualių skundų nagrinėjimu ir ginčų sprendimu; arba iii) įsipareigodamos bendradarbiauti su Europos Sąjungos duomenų apsaugos institucijomis arba jų įgaliotais atstovais.

- b) Šis sąrašas yra aiškinamojo pobūdžio ir neišsamus. Privačiajame sektoriuje gali būti nustatyti papildomi mechanizmai, kuriais užtikrinamas reikalavimų laikymasis, jeigu jie atitinka teisių gynimo, reikalavimų

užtikrinimo ir atsakomybės principą ir papildomus principus. Atkreipkite dėmesį, kad teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principo reikalavimai papildo reikalavimą, pagal kurį savireguliaciniai veiksmai turi būti užtikrinami pagal Federalinės prekybos komisijos akto 5 straipsnį, kuriuo draudžiami nesąžiningi ir apgaulingi veiksmai, arba kitą teisės aktą, kuriuo draudžiami tokie veiksmai.

- c) Siekdamas palengvinti su „privatumo skydu“ susijusių išipareigojimų vykdymą ir padėti administruoti programą, organizacijos, taip pat jų nepriklausomos teisių gynimo institucijos, Departamento prašymu privalo teikti su „privatumo skydu“ susijusią informaciją. Be to, organizacijos privalo greitai reaguoti į skundus dėl jų padarytų principų pažeidimų, kuriuos per Departamentą perdavė DAL. Atsakyme reikėtų nurodyti, ar skundas turi pagrindą, ir, jei taip, kaip organizacija išspręs problemą. Departamentas gautos informacijos konfidencialumą užtikrins pagal JAV teisę.

d) Teisių gynimo institucijos

- i) Pirmiausia vartotojai turėtų būti raginami teikti bet kokius galimus skundus pačioms organizacijoms, o tik vėliau pasinaudoti nepriklausomomis teisių gynimo institucijomis. Organizacijos vartotojui atsakymą privalo pateikti per 45 dienas nuo skundo gavimo. Tai, ar teisių gynimo institucija yra nepriklausoma, yra faktinis klausimas, į kurį galima atsakyti visų pirma užtikrinant nešališkumą, skaidrią sudėtį ir finansavimą, taip pat reikalaujant įrodyti profesinę patirtį. Kaip reikalaujama pagal teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principą, asmenims prieinamos teisių gynimo priemonės turi būti iš anksto nustatytos ir nemokamos. Ginčų sprendimo institucijos turi nagrinėti visus iš asmenų gautus skundus, nebent jie būtų akivaizdžiai nepagrįsti ar nerimti. Tai nedraudžia teisių gynimo institucija besinaudojančiai organizacijai nustatyti tinkamumo reikalavimų, tačiau tokie reikalavimai turi būti skaidrūs ir pagrįsti (pvz., atmetant skundus, kuriems programa netaikoma arba jie skirti svarstyti kitur) ir negali sumažinti išipareigojimo nagrinėti teisėtus skundus. Be to, asmenims, pateikiantiems skundą teisių gynimo institucijai, turi būti suteikta visa ir lengvai pasiekiama informacija apie ginčų sprendimo tvarką. Ši informacija turi apimti institucijos privatumo praktiką, atitinkančią „privatumo skydo“ principus. Jos taip pat turėtų bendradarbiauti kurdamos tokias priemones kaip standartinės skundų formos, kad palengvintų skundų nagrinėjimo procesą.
- ii) Nepriklausomos teisių gynimo institucijos savo viešose svetainėse privalo pateikti informaciją apie „privatumo skydo“ principus ir paslaugas, kurias jos teikia dalyvaujamos „privatumo skydo“ sistemoje. Ši informacija turi apimti: 1) informaciją apie „privatumo skydo“ principų reikalavimus, susijusius su nepriklausomomis teisių gynimo institucijomis, arba nuorodą į tokią informaciją; 2) nuorodą į Departamento „privatumo skydo“ svetainę; 3) paaiškinimą, kad jų ginčų sprendimo paslaugos pagal „privatumo skydą“ asmenims teikiamos nemokamai; 4) aprašymą, kaip galima pateikti su „privatumo skydu“ susijusį skundą; 5) terminą, per kurį išnagrinėjami su „privatumo skydu“ susiję skundai, ir 6) įvairių galimų teisių gynimo priemonių aprašymą.
- iii) Nepriklausoma teisių gynimo institucija privalo skelbti metinę ataskaitą, kurioje pateikiami apibendrinti statistiniai duomenys apie jų teikiamas ginčų sprendimo paslaugas. Metinėje ataskaitoje būtina nurodyti: 1) bendrą su „privatumo skydu“ susijusių skundų, gautų per ataskaitinius metus, skaičių; 2) gautų skundų rūšis; 3) kokybinius ginčų sprendimo rodiklius, pvz., skundų nagrinėjimo trukmę, ir 4) sprendimus, kurie buvo priimti išnagrinėjus skundus, visų pirma nustatytų teisių gynimo priemonių arba sankcijų skaičių ir rūšis.
- iv) Kaip nustatyta I priede, arbitražu asmenys gali pasinaudoti, kad, atsižvelgdami į neįvykdytus reikalavimus, nustatytų, ar „privatumo skydo“ organizacija pažeidė savo išipareigojimus pagal privatumo principus dėl to asmens ir ar bet kuris toks pažeidimas išlieka visiškai arba iš dalies neištaisytas. Arbitražu galima pasinaudoti tik minėtais tikslais. Ši alternatyva nėra prieinama, pvz., dėl privatumo principo išimčių⁽¹⁾ arba dėl teiginių, susijusių su „privatumo skydo“ tinkamumu. Pagal šią arbitražo alternatyvą „privatumo skydo“ komisija (kuriai sudaro vienas arba trys arbitrai, tai priklauso nuo šalių sutarimo) turi įgaliojimus nustatyti su konkrečiu asmeniu susijusias nepinigines lygiavertes teisių gynimo priemones (pvz., prieiga prie atitinkamų asmens duomenų, šių duomenų taisymas, trynimas arba grąžinimas), kurios yra būtinos siekiant ištaisyti privatumo principų pažeidimą tik to asmens atžvilgiu. Asmenys ir „privatumo skydo“ organizacijos galės siekti, kad arbitražiniai sprendimai būtų peržiūrimi teisme ir vykdomi pagal JAV teisę, t. y. Federalinį arbitražo aktą.

⁽¹⁾ Privatumo principų I.5 skirsnis.

e) Teisių gynimo priemonės ir sankcijos

Ginčų sprendimo institucijos suteiktomis bet kokiomis teisės gynimo priemonėmis turėtų būti užtikrinama, kad organizacija kiek įmanoma panaikintų ar ištaisytų reikalavimų nesilaikymo sukeltus padarinius, toliau tvarkytų informaciją laikydamosi privatumo principų ir nebetvarkytų skundą parašiusio asmens duomenų. Sankcijos turi būti pakankamai griežtos, kad priverstų organizacijas laikytis privatumo principų. Įvairaus sunkumo nusižengimus ginčų sprendimo institucijos reikiama įvertins taikydamos skirtingas griežtumo sankcijas. Pagal sankcijas turi būti numatyta viešai paskelbti išvadas dėl reikalavimų nesilaikymo ir kai kuriais atvejais pareikalauti sunaikinti duomenis⁽¹⁾. Kitos sankcijos gali būti veiklos sustabdymas ir licencijos atėmimas, dėl reikalavimų nesilaikymo asmenims padarytos žalos atlyginimas ir draudimo priemonės. Privačiojo sektoriaus ginčų sprendimo institucijos ir savireguliacijos institucijos privalo pranešti apie „privatumo skydo“ sistemos organizacijų nuostatų nesilaikymą atitinkamai valdžios institucijai arba teismams ir informuoti Departamentą.

f) FPK veikla

FPK įsipareigojo prioritetine tvarka peržiūrėti perduotas bylas, kuriose teigiama, kad nebuvo laikomasi privatumo principų, gautas iš: i) privatumo savireguliacinių organizacijų ir kitų nepriklausomų ginčų sprendimo įstaigų; ii) ES valstybių narių; ir iii) Departamento, kad nustatytų, ar buvo pažeistas FPK akto 5 straipsnis, kuriuos draudžiami nesąžiningi arba apgaulingi veiksmai ar komercinė praktika. Jei FPK nusprendžia, kad yra priežasčių manyti, jog 5 straipsnis buvo pažeistas, ji gali reikalauti sustabdyti administracinę veiklą, paklusti nutraukimo įsakymui, draudžiančiam vykdomą veiklą, pateikti skundą federaliniam apygardos teismui, o šiam priėmus palankų sprendimą, gali išleisti tokio paties pobūdžio federalinio teismo įsakymą. Tai apima neteisingus pareiškimus dėl „privatumo skydo“ principų laikymosi arba dalyvavimo „privatumo skyde“, kuriuos padarė iš „privatumo skydo“ sąrašo išbrauktos arba Departamentui niekada autosertifikavimo pažymėjimo neteikusios organizacijos. FPK gali taikyti administracines nuobaudas už administracinio veiklos sustabdymo ir nutraukimo įsakymo nesilaikymą ir persekioti administracine arba baudžiamąja tvarka už federalinio teismo įsakymo nevykdymą. FPK informuos Departamentą apie visus tokius veiksmus, kurių imasi. Departamentas skatina kitas valdžios institucijas informuoti apie galutinį tokių pranešimų sutvarkymą ir kitus nurodymus, nustatančius „privatumo skydo“ principų laikymąsi.

g) Nuolatinis reikalavimų nesilaikymas

- i) Jei organizacija nuolatos pažeidinėja privatumo principus, iš jos atimama teisė naudotis „privatumo skydo“ privalumais. Sistemingai privatumo principų nesilaikančios organizacijos bus išbraukiamos iš „privatumo skydo“ sąrašo ir privalo grąžinti arba ištrinti pagal ES ir JAV „privatumo skydo“ nuostatas gautus asmens duomenis.
- ii) Nuolatiniai pažeidinėjimai apibūdinami kaip Departamentui įsipareigojusios organizacijos atsisakymas paklusti bet kurios savireguliacijos ar Vyriausybės įstaigos galutiniam sprendimui arba tokia institucija nustato, kad organizacija taip dažnai pažeidinėja privatumo principus, kad jos pasižadėjimas jų laikytis yra nepatikimas. Tokiais atvejais organizacija privalo nedelsdama informuoti Departamentą (arba jo įgaliotą asmenį) apie tokius faktus. Jei organizacija nesilaiko šio reikalavimo, ji gali būti baudžiama pagal Melagingų parodymų aktą (JAV kodekso 18 antraštinės dalies 1001 straipsnis). Organizacijos pašalinimas iš privačiojo sektoriaus savireguliacijos programos arba nepriklausomo ginčų sprendimo mechanizmo neatleidžia nuo pareigos laikytis privatumo principų ir reikštų nuolatinį reikalavimų nesilaikymą.
- iii) Departamentas išbrauks organizaciją iš „privatumo skydo“ sąrašo reaguodamas į bet kokią gautą pranešimą apie nuolatinį reikalavimų nesilaikymą, nepaisant to, ar jis gautas iš pačios organizacijos, privačios savireguliacijos įstaigos ar kitos nepriklausomos ginčų sprendimo įstaigos, ar iš Vyriausybės įstaigos, tačiau tik po to, kai iš pradžių buvo įteiktas 30 dienų pranešimas ir suteikta galimybė reikalavimų nesilaikiusiai

⁽¹⁾ Ginčų sprendimo institucijos gali pasirinkti, kokiomis aplinkybėmis taikys tokias sankcijas. Atitinkamų duomenų konfidencialumas yra vienas iš veiksnių, į kuriuos reikia atsižvelgti nusprendžiant, ar reikėtų reikalauti ištrinti duomenis, į jį taip pat reikėtų atsižvelgti nustatant, ar organizacija informaciją rinko, naudojo arba ją atskleidė akivaizdžiai pažeisdama „privatumo skydo“ principus.

organizacijai pateikti pastabas. Atitinkamai Departamento tvarkomame „privatumo skydo“ sąrašė aiškiai nurodoma, kurios organizacijos gali naudotis „privatumo skydo“ privalumais, o kurios – ne.

- iv) Jei organizacija teikia prašymą dalyvauti savireguliacijos institucijoje, kad galėtų vėl būti priimta į „privatumo skydo“ sistemą, ji privalo pateikti tai institucijai visą informaciją apie savo ankstesnį dalyvavimą „privatumo skydo“ sistemoje.

12. Pasirinkimas – atsakymo laikas

- a) Plačiąja prasme pasirinkimo principo paskirtis — užtikrinti, kad asmeninė informacija būtų naudojama ir atskleidžiama taip, kaip to tikisi ir pasirenka pats asmuo. Todėl asmuo turi turėti galimybę bet kuriuo metu atsisakyti savo asmens duomenų tvarkymo tiesioginės rinkodaros tikslais per organizacijos nustatytus pagrįstus terminus, kurių, pvz., pakaktų atsisakymui įgyvendinti. Organizacija taip pat gali reikalauti pateikti pakankamai informacijos, kad būtų nustatyta atsisakymo reikalaujančio asmens tapatybė. Jungtinėse Amerikos Valstijose asmenys šią pasirinkimo galimybę gali įgyvendinti pasinaudodami centrine atsisakymo programa, pvz., „Direct Marketing Association's Mail Preference Service“. Šią programą naudojančios organizacijos klientus, kurie nepageidauja gauti komercinės informacijos, turėtų aiškiai informuoti apie galimybę ją pasinaudoti. Bet kuriuo atveju asmeniui turi būti suteiktas lengvai prieinamas ir suprantamas pasirinkimo mechanizmas.
- b) Panašiai organizacija gali naudoti informaciją tam tikrais tiesioginės rinkodaros tikslais, kai suteikti asmeniui atsisakymo galimybę iki panaudojant informaciją neįmanoma, jei organizacija suteikia asmeniui galimybę iškart (o pareikalavus – bet kuriuo metu) atsisakyti (nemokamai) gauti kitus tiesioginės rinkodaros pranešimus ir įvykdo asmens pageidavimą.

13. Kelionės informacija

- a) Oro vežėjo keleivio rezervacijos duomenys ir kita kelionės informacija, pvz., lojalaus keleivio arba viešbučio rezervacijos informacija ir specialūs keleivio poreikiai, pvz., religiją atitinkantis valgis arba fizinė pagalba, gali būti perduodami organizacijoms, esančioms už ES, keliomis skirtingomis aplinkybėmis. Pagal Direktyvos 26 straipsnį asmens duomenys „trečiajai šaliai, kuri neužtikrina pakankamo apsaugos lygio, nurodyto 25 straipsnio 2 dalyje“ gali būti perduodami tik tuo atveju, kai i) būtina suteikti kliento reikalaujamas paslaugas arba vykdyti sutarties, pvz., lojalaus keleivio sutarties, sąlygas, arba ii) vartotojas davė aiškų sutikimą. „Privatumo skydo“ sistemoje dalyvaujančios JAV organizacijos suteikia tinkamą apsaugą asmens duomenims ir todėl gali gauti iš ES perduodamus duomenis nesilaikydamos tų sąlygų arba kitų Direktyvos 26 straipsnyje nurodytų sąlygų. Kadangi „privatumo skyde“ galioja specialios taisyklės neskelbtinai informacijai apsaugoti, tokią informaciją (kurią gali prireikti surinkti todėl, kad klientui reikia fizinės pagalbos) galima siųsti „privatumo skydo“ dalyviams kartu su kita informacija. Informaciją perduodanti organizacija visuomet privalo laikytis ES valstybės narės, kurioje veikia, teisės aktų, kuriuose, be kita ko, gali būti nustatytos specialios ypatingos informacijos tvarkymo sąlygos.

14. Farmaciniai ir medicinos produktai

- a) ES valstybių narių įstatymų arba „privatumo skydo“ principų taikymas

ES valstybės narės teisės aktai galioja renkant asmens duomenis ir juos tvarkant iki perduodant į Jungtines Amerikos Valstijas. Perdavus duomenis į Jungtines Amerikos Valstijas, galioja „privatumo skydo“ principai. Farmaciniams tyrimams ir kitais tikslais naudojami duomenys gali būti pakeisti taip, kad nebūtų galima nustatyti duomenų subjekto tapatybės.

b) Būsimi moksliniai tyrimai

- i) Specialiųjų medicinos ar farmacinių tyrimų studijų metu gauti asmens duomenys dažnai yra labai svarbūs būsimiems moksliniams tyrimams. Jeigu atliekant vieną mokslinį tyrimą asmens duomenys perduodami „privatumo skydo“ sistemoje dalyvaujančiai JAV organizacijai, organizacija gali panaudoti duomenis naujai mokslinio tyrimo veiklai, jei iš pradžių tinkamai informavo duomenų subjektą ir suteikė jam pasirinkimo galimybę. Tokiame pranešime turi būti pateikta informacija apie bet kokią konkretų būsimą duomenų panaudojimą, pvz., periodinius atsiliepimus, susijusias studijas ar rinkodarą.
- ii) Suprantama, kad neįmanoma nurodyti visko, kam ateityje gali būti panaudota informacija, nes naujų galimybių ją panaudoti tyrimams gali atsirasti dėl naujo pirminių duomenų supratimo, naujų medicinos atradimų ir pažangos, taip pat visuomenės sveikatos ir kontrolės plėtros. Todėl pranešime turi būti paaiškinta, kad asmens duomenys gali būti panaudoti būsimiems medicinos ir farmacijos tyrimams, kurių neįmanoma numatyti. Jeigu asmens duomenis ketinama panaudoti tikslams, neatitinkantiems pirminių bendrųjų tyrimo tikslų ar tų, kuriems asmuo vėliau davė sutikimą, būtina gauti naują sutikimą.

c) Atsisakymas dalyvauti klinikiniame tyrime

Bet kuriuo metu dalyviai gali nuspręsti arba jų gali būti paprašyta nebedalyvauti klinikiniuose tyrimuose. Visi iki to laiko surinkti asmens duomenys ir kiti klinikinio tyrimo metu gauti duomenys gali būti tvarkomi, jei dalyviui apie tai buvo pranešta tuomet, kai jis sutiko juose dalyvauti.

d) Duomenų perdavimas reguliavimo ir priežiūros tikslais

Farmacinius ir medicinos įrenginius gaminančios kompanijos ES vykdytų klinikinių tyrimų metu gautus asmens duomenis gali suteikti tvarkytojams Jungtinėse Amerikos Valstijose priežiūros ir kontrolės tikslais. Panašiai duomenis galima perduoti kitoms nei reguliavimo institucijos šalims, pvz., įmonės padaliniais ir kitiems tyrėjams, jeigu toks perdavimas atitinka pranešimo ir pasirinkimo principus.

e) „Aklieji“ tyrimai

- i) Kad būtų užtikrintas daugelio klinikinių tyrimų objektyvumas, dalyviams, o dažnai ir tyrėjams, negalima suteikti prieigos prie informacijos apie kiekvieno dalyvio gydymą. Ją suteikus, kiltų pavojus, kad tyrimų studijos ir jų rezultatai taptų nebepatikimi. Tokiuose klinikiniuose tyrimuose (toliau – „aklieji“ tyrimai) dalyvaujantiems asmenims neturi būti suteikiama prieiga prie duomenų apie jų gydymą bandymo metu, jeigu šis apribojimas buvo paaiškintas dalyviui sutinkant dalyvauti bandyme, o tokios informacijos atskleidimas pakenktų mokslinio tyrimo vientisumui.
- ii) Sutikimas dalyvauti tyrime tokiomis sąlygomis yra pagrįstas prieigos teisės atsisakymu. Jei dalyviai pageidauja prieiti prie savo duomenų, tai galima padaryti tik pabaigus tyrimą ir išanalizavus rezultatus. Iš pradžių jie turi to prašyti tyrimo metu juos gydžiusio gydytojo ar kito sveikatos priežiūros teikėjo arba po to – rėmusiosios organizacijos.

f) Produkto saugumo ir veiksmingumo stebėseną

Farmacinius ar medicinos prietaisus gaminanti bendrovė, vykdydama su jos produkto saugumo ir veiksmingumo stebėseną susijusią veiklą, privalo taikyti „privatumo skydo“ pranešimo, pasirinkimo, atsakomybės už tolesnį duomenų perdavimą ir prieigos prie duomenų principus, įskaitant šių principų laikymąsi rengiant ataskaitas apie neigiamas pasekmes ir tam tikrus vaistus arba medicinos prietaisus naudojančių pacientų (subjektų) sekimą, jeigu laikantis privatumo principų daroma įtaka reguliavimo reikalavimų laikymuisi. Tai

pasakytina apie sveikatos priežiūros teikėjų farmacijos ir medicinos prietaisų gamybos bendrovėms teikiamus pranešimus ir šių bendrovių pranešimus valdžios institucijoms, kaip antai Maisto ir vaistų valdybai.

g) Raktu užkoduoti duomenys

Dažniausiai pagrindinis tyrėjas, vos tik gavęs tyrimų duomenis, iš karto juos užkoduoja unikaliu kodu, kad nebūtų atskleista atskirų duomenų subjektų tapatybė. Tokį tyrimą remiančios farmacijos kompanijos kodo rakto negauna. Unikalo kodo raktą turi tik tyrėjas, kad tam tikromis aplinkybėmis galėtų nustatyti tyrimų subjekto tapatybę (pvz., jei reikia tęstinės medicinos priežiūros). Tokiu būdu užkoduotų duomenų perdavimas iš ES į Jungtines Amerikos Valstijas nereikštų asmens duomenų perdavimo, kuriam būtų taikomi „privatumo skydo“ principai.

15. Viešasis archyvas ir viešai prieinama informacija

- a) Organizacija privalo „privatumo skydo“ saugumo, duomenų vientisumo, tikslo ribojimo ir teisių gynimo reikalavimų užtikrinimo ir atsakomybės principus taikyti iš viešai prieinamų šaltinių gautiems asmens duomenims. Šie privatumo principai taip pat taikomi iš viešųjų archyvų surinktiems asmens duomenims, t. y. iš bet kokio lygio Vyriausybės agentūrų ar įstaigų saugomų archyvų, kurie apskritai prieinami visuomenei.
- b) Pranešimo, pasirinkimo ar atsakomybės už tolesnį duomenų perdavimą principų viešųjų archyvų informacijai taikyti nebūtina, jei ji nėra sujungta su neviešųjų archyvų informacija ir turi būti paisoma bet kurioje atitinkamoje jurisdikcijoje galiojančių duomenų tikrinimo sąlygų. Taip pat nebūtina taikyti pranešimo, pasirinkimo ar atsakomybės už tolesnį duomenų perdavimą principų viešai prieinamai informacijai, nebent siuntėjas iš Europos nurodo, kad tokiai informacijai taikomi apribojimai, dėl kurių organizacija privalo taikyti privatumo principus. Organizacijos neatsako už tai, kaip tokią informaciją panaudos gaunantieji ją iš paskelbtos medžiagos.
- c) Jei nustatoma, kad organizacija, pažeisdama privatumo principus, sąmoningai viešai paskelbė asmeninę informaciją ir kad ji arba kiti gali turėti iš to naudos, ji netenka teisės naudotis „privatumo skydo“ privalumais.
- d) Prieigos prie duomenų principo nebūtina taikyti iš viešųjų archyvų gautai informacijai, jeigu ji nenaudojama su kita asmenine informacija (išskyrus nedidelius kiekius, kurie naudojami viešuosiuose archyvuose pateikiamai informacijai indeksuoti arba tvarkyti); tačiau turi būti paisoma bet kurioje atitinkamoje jurisdikcijoje galiojančių duomenų tikrinimo sąlygų. Priešingai, kai viešųjų archyvų informacija yra sujungta su kita neviešųjų archyvų informacija (kitokia, nei nurodyta pirmiau), organizacija privalo suteikti prieigą prie visos tokios informacijos, jei ji neribojama dėl kitų leistinų išimtinių priežasčių.
- e) Kalbant apie viešųjų archyvų informaciją, nebūtina suteikti prieigos prie plačiai visuomenei prieinamos informacijos, jei ji nesujungta su viešai neprieinama informacija. Viešai prieinama informacija prekiaujančios organizacijos gali imti iš klientų mokestį už prieigos reikalavimus. Tačiau asmenys gali bandyti susipažinti su informacija apie save per organizaciją, kuri iš pradžių tą informaciją sukaupė.

16. Valdžios institucijų pateikti prašymai suteikti prieigą prie duomenų

- a) Siekiant užtikrinti valdžios institucijų teisėtą prašymų suteikti prieigą prie asmeninės informacijos skaidrumą, „privatumo skydo“ organizacijos gali savanoriškai teikti periodines skaidrumo ataskaitas, kuriose būtų pateikiama informacija apie prašymų leisti susipažinti su asmenine informacija skaičių, kuriuos valdžios institucijos gauna teisėsaugos arba nacionalinio saugumo sumetimais, tiek, kiek atskleisti tokią informaciją pagal taikytiną teisę yra leidžiama.

- b) Šiose ataskaitose „privatumo skydo“ organizacijų pateikta informacija kartu su žvalgybos bendruomenės paskelbta informacija ir kita informacija gali būti naudojama atliekant „privatumo skydo“ veikimo pagal privatumo principus bendrą metinę peržiūrą.
 - c) Tai, kad nėra pranešimo pagal pranešimo principo (a)(xii) dalį, neužkerta organizacijai kelio arba nepažeidžia jos galimybių pateikti atsakymą į bet kurį teisėtą prašymą.
-

*I priedas***Arbitražinis modelis**

Šiame I priede pateikiamos sąlygos, kuriomis „privatumo skydo“ organizacijos įpareigojamos pagal teisių gynimo, reikalavimų užtikrinimo ir atsakomybės principą arbitražo tvarka nagrinėti reikalavimus. Toliau aprašyta arbitražo sąlyga taikoma tam tikriems neįvykdytiems reikalavimams, susijusiems su duomenimis, kuriems galioja ES ir JAV „privatumo skydo“ apsauga. Šios arbitražo sąlygos paskirtis – sukurti operatyvų, nepriklausomą ir sąžiningą mechanizmą, kurį pasirinkę fiziniai asmenys galėtų pašalinti tariamus privatumo principų pažeidimus, kurie nebuvo išspręsti naudojant kurį nors kitą „privatumo skydo“ mechanizmą.

A. Taikymo sritis

Šia arbitražo alternatyva asmenys gali pasinaudoti, kad, atsižvelgdami į neįvykdytus reikalavimus, nustatytų, ar „privatumo skydo“ organizacija pažeidė savo įsipareigojimus pagal privatumo principus dėl to asmens ir ar bet kuris toks pažeidimas lieka visiškai arba iš dalies neišaišytas. Arbitražu galima pasinaudoti tik minėtais tikslais. Ši alternatyva nėra prieinama, pvz., dėl privatumo principo išimčių ⁽¹⁾ arba dėl teiginių, susijusių su „privatumo skydo“ tinkamumu.

B. Prieinamos teisių gynimo priemonės

Pagal šią arbitražo alternatyvą „privatumo skydo“ komisija (kurią sudaro vienas arba trys arbitrai, tai priklauso nuo šalių sutarimo) turi įgaliojimus nustatyti su konkrečiu asmeniu susijusias nepinigines lygiavertes teisių gynimo priemones (pvz., prieiga prie atitinkamų asmens duomenų, šių duomenų taisymas, trynimasis arba grąžinimas), kurios yra būtinos siekiant ištaisyti privatumo principų pažeidimą tik to asmens atžvilgiu. Šiais įgaliojimais arbitražo komisija gali naudotis tik dėl teisių gynimo priemonių. Nagrinėdama teisių gynimo priemones, arbitražo komisija turi apsvarstyti kitas teisių gynimo priemones, kurios jau privalomai taikomos pagal kitus „privatumo skydo“ mechanizmus. Netaikomas žalos, išlaidų ar mokesčių atlyginimas ar kitos teisių gynimo priemonės. Kiekviena šalis sumoka savo advokato mokesčius.

C. Reikalavimai, kuriuos reikia įvykdyti iki arbitražo

Asmuo, kuris nusprendžia naudotis šia arbitražo alternatyva, prieš perduodamas reikalavimą arbitražui privalo atlikti šiuos veiksmus: 1) pareikšti reikalavimą dėl tariamo pažeidimo tiesiogiai organizacijai ir suteikti jai galimybę išspręsti klausimą per privatumo principų III.11 skirsnio d dalies i punkte nustatytą terminą; 2) pasinaudoti nepriklausoma ir nemokama teisių gynimo institucija pagal privatumo principus; ir 3) klausimą per duomenų apsaugos instituciją perduoti Komercijos departamentui ir suteikti jam galimybę visomis pastangomis išspręsti klausimą nemokamai per Komercijos departamento Tarptautinės prekybos administracijos rašte nustatytus terminus.

Šia arbitražo alternatyva negalima remtis, jeigu tas pats asmens reikalavimas dėl tariamo privatumo principų pažeidimų 1) buvo anksčiau nagrinėtas arbitražo tvarka ir dėl jo buvo priimtas įpareigojantis sprendimas, 2) buvo priimtas galutinis teismo sprendimas teismo byloje, kurioje asmuo dalyvavo kaip šalis, arba 3) šalis išsprendė jį anksčiau. Be to, šia alternatyva negalima naudotis, jeigu ES duomenų apsaugos institucija 1) turi įgaliojimus pagal privatumo principų III.5 arba III.9 skirsnį; arba 2) turi įgaliojimus pašalinti tariamą pažeidimą tiesiogiai organizacijoje. DAI įgaliojimai nagrinėti tą patį reikalavimą dėl ES duomenų valdytojo patys savaime nepanaikina galimybės remtis šia arbitražo alternatyva kitame juridiniame asmenyje, kuris nėra pavaldus DAI įgaliojimams.

D. Privalomas sprendimų pobūdis

Asmens sprendimas remtis šia privaloma arbitražo alternatyva yra visiškai savanoriškas. Arbitražo sprendimai bus privalomi visoms arbitražo šalims. Pradėjus arbitražo procedūrą, asmuo netenka galimybės kitame teisme ginti savo teisių dėl to paties tariamo pažeidimo, išskyrus tai, kad jeigu lygiavertė nepiniginė teisių gynimo priemonė nepadėjo visiškai ištaisyti tariamo pažeidimo, asmens pradėta arbitražo procedūra nepanaikins galimybės reikalauti atlyginti nuostolius, kuriuos kitu atveju būtų galima prisieisti teisme.

⁽¹⁾ Privatumo principų I.5 skirsnis.

E. Peržiūra ir reikalavimų užtikrinimas

Asmenys ir „privatumo skydo“ organizacijos galės siekti, kad arbitražiniai sprendimai būtų peržiūrimi teisme ir vykdomi pagal JAV teisę, t. y. Federalinį arbitražo aktą⁽¹⁾. Visos tokios bylos turi būti iškeltos federaliniame apygardos teisme, kurio teritorinė veiklos sritis apima pagrindinę „privatumo skydo“ organizacijos verslo vietą.

Ši arbitražo alternatyva ketinama išspręsti individualius ginčus, o arbitražiniais sprendimais neketinama sukurti atgrasančio arba privalomo precedento bylose, susijusiose su kitomis šalimis, įskaitant būsimą arbitražą arba ES ir JAV teismuose, arba FPK bylose.

F. Arbitražo komisija

Šalys arbitrus pasirenka iš toliau aptarto arbitrų sąrašo.

Laikydami taikytinos teisės, JAV komercijos departamentas ir Europos Komisija sudaro ne mažiau kaip 20 arbitrų, atrinktų atsižvelgiant į jų nepriklausomumą, sąžiningumą ir patirtį, sąrašą. Šiam procesui taikomos toliau nurodytos nuostatos:

Arbitrai:

- 1) bus įtraukti į sąrašą 3 metų terminui, kuris, išskyrus išimtines aplinkybes arba pagrįstą priežastį, atnaujinamas papildomam 3 metų terminui;
- 2) nesivadovauja jokiais kurios nors šalies instrukcijomis arba nėra susiję su kuria nors iš šalių arba bet kuria „privatumo skydo“ organizacija, arba JAV, ES ar bet kuria ES valstybe nare ar bet kuria kita Vyriausybine institucija, valdžios institucija arba teisės saugos institucija arba
- 3) turi turėti teisę verstis advokato praktika JAV ir būti JAV privatumo teisės ekspertais ir turėti žinių apie ES duomenų apsaugos teisę.

G. Arbitražo procedūros

Laikydami taikytinos teisės per 6 mėnesius nuo sprendimo dėl tinkamumo priėmimo Komercijos departamentas ir Europos Komisija sutars priimti galiojančių išsamių JAV arbitražo procedūrų rinkinį (pvz., AAA arba JAMS), kad užtikrintų arbitražo procedūrų reglamentavimą „privatumo skydo“ komisijoje, ir atsižvelgs į toliau nurodytas aplinkybes.

1. Asmuo gali inicijuoti privalomą arbitražą, jeigu įvykdyti pirmiau nurodyti prieš arbitražo procedūrą taikomi reikalavimai, įteikdamas pranešimą organizacijai. Pranešime pateikiama priemonių, kurių pagal C punktą buvo imtasi siekiant įvykdyti reikalavimą, santrauka, tariamo pažeidimo aprašymas ir asmens pasirinkimu – bet kurie patvirtinamieji dokumentai, medžiaga ir (arba) teisės aiškinimas, susijęs su tariamu reikalavimu.

⁽¹⁾ Federalinio arbitražo akto (FAA) 2 skyriuje nustatyta, kad „susitarimas dėl arbitražo arba arbitražo sprendimas atitinkamai sudarytas arba priimtas dėl teisinių santykių, nepaisant to, ar tai sutartiniai, ar nesutartiniai santykiai, kurie laikomi komerciniais, įskaitant sandorį, sutartį arba susitarimą, aprašytą [FAA 2 straipsnyje], patenka į [1958 m. birželio 10 d.] Konvencijos [dėl užsienio arbitražo sprendimų pripažinimo ir vykdymo taikymo sritį, 21 U.S.T. 2519, T.I.A.S. Nr. 6997 („Niujorko konvencija“)].“ JAV kodekso 9 antraštinės dalies 202 straipsnis. FAA taip pat nustatyta, kad „iš tokių santykių, kurie išimtinai yra susiję su Jungtinių Amerikos Valstijų piliečiais, kylantis susitarimas arba arbitražo sprendimas nepatenka į [Niujorko] Konvencijos taikymo sritį, išskyrus atvejus, kai tie santykiai yra susiję su užsienyje esančiu turtu, pagal juos užsienyje turi būti atliekami veiksmai ar vykdomos pareigos, arba jis kitais atžvilgiais yra iš esmės susijęs su viena arba daugiau užsienio valstybių“. Ten pat. Pagal 2 skyrių „bet kuri arbitražo šalis gali kreiptis į bet kurį pagal šį skyrių jurisdikciją turintį teismą, kad šis priimtų patvirtinamąją nutartį dėl arbitražo sprendimo bet kurios kitos arbitražo šalies atžvilgiu. Teismas patvirtina arbitražo sprendimą, nebent nustato vieną iš [Niujorko] Konvencijoje nurodytų arbitražo sprendimo atsisakymo, pripažinimo atidėjimo arba vykdymo pagrindų.“ Ten pat, 207 straipsnis. 2 skyriuje taip pat nustatyta, kad „Jungtinių Amerikos Valstijų apygardos teismai <...> turi dalykinę jurisdikciją nagrinėti <...> ieškinį arba bylą [pagal Niujorko konvenciją], nepaisant ginčo sumos.“ Ten pat, 203 straipsnis.

2 skyriuje taip pat nustatyta, kad „1 skyrius taikomas ieškiniams ir byloms, kurios pagal šį skyrių iškeltos tiek, kiek jis neprieštarauja šiam skyriui arba Jungtinių Amerikos Valstijų ratifikuotai [Niujorko] Konvencijai.“ Ten pat, 208 straipsnis. 1 skyriuje nustatyta, kad „rašytinės <...> sutarties nuostata, kuria patvirtinamas sandoris, susijęs su komercine praktika, kuria siekiama arbitražo tvarka išspręsti ginčą, kilusį dėl tokios sutarties arba sandorio, arba atsisakius atlikti dalį ar visą tokią sutartį ar sandorį, arba susitarimą raštu perduoti arbitražui galiojantį ginčą, kylantį iš tokios sutarties, sandorio arba atsisakymo, galioja, yra nepanaikinama, ir vykdytina, išskyrus atvejus, kai tokiai nuostatai taikomas įstatyme nustatytas arba lygiavertis bet kurios sutarties negaliojimo pagrindas.“ Ten pat, 2 straipsnis. 1 skyriuje taip pat nustatyta, kad „bet kuri arbitražo šalis gali kreiptis į teismą prašydama priimti arbitražo sprendimą patvirtinančią nutartį, o tokį prašymą gavęs teismas privalo patvirtinti tokį sprendimą, išskyrus atvejus, kai sprendimas panaikinamas, pakeičiamas arba ištaisomas, kaip nustatyta [FAA] 10 ir 11 straipsniuose.“ Ten pat, 9 straipsnis.

2. Siekiant užtikrinti, kad tas pats asmens tariamas pažeidimas nebūtų ginamas dvejopomis teisių gynimo priemonėmis arba procedūromis, bus nustatytos procedūros.
3. FPK byla gali vykti lygiagrečiai su arbitražo procedūra.
4. Šiose arbitražo procedūrose negali dalyvauti jokie JAV, ES ar bet kurios ES valstybės narės arba bet kurios kitos Vyriausybės institucijos, valdžios institucijos arba teisėsaugos institucijos atstovai, jeigu ES asmens prašymu ES DAI gali teikti paramą tik rengiant pranešimą, bet ES DAI negali gauti prieigos prie pateiktų faktų arba bet kurios kitos medžiagos, susijusios su šiomis arbitražo procedūromis.
5. Arbitražas vyks Jungtinėse Amerikos Valstijose, o asmuo gali nuspręsti dalyvauti pasitelkdamas vaizdo ar telefonijos paslaugas, kurios jam suteikiamos nemokamai. Asmeninis dalyvavimas nebūtinai.
6. Arbitražo procedūra vyks anglų kalba, nebent šalys susitaria kitaip. Gavus pagrįstą prašymą ir atsižvelgiant į tai, ar asmeniui atstovauja advokatas, asmeniui bus suteiktos nemokamos vertimo žodžiu arbitražo procedūroje paslaugos ir arbitražo medžiagos vertimo raštu paslaugos, išskyrus atvejus, kai komisija nustato, kad konkrečiomis arbitražo procedūromis dėl to arbitražo procedūra taptų nepagrįstai arba neproporcingai brangi.
7. Arbitrai dėl gautos medžiagos laikosi konfidencialumo pareigos ir gali ją naudoti tik tiek, kiek tai susiję su arbitražu.
8. Prireikus gali būti leidžiama susipažinti su faktais apie konkretų asmenį, o dėl tokių faktų šalys laikysis konfidencialumo pareigos ir juos naudos tik tiek, kiek tai susiję su arbitražu.
9. Arbitražo procedūros turėtų būti baigiamos per 90 dienų nuo pranešimo įteikimo atitinkamai organizacijai, išskyrus atvejus, kai šalys susitarė kitaip.

H. Išlaidos

Arbitrai turėtų imtis pagrįstų priemonių, kad kuo labiau sumažintų arbitražo proceso išlaidas arba mokesčius.

Atsižvelgdamas į taikytiną teisę, Komercijos departamentas palengvins fondo įsteigimą o „privatumo skydo“ organizacijos turės mokėti į jį metines įmokas, kurių suma priklausys nuo organizacijos dydžio, ir iš šio fondo bus atlyginamos arbitražo išlaidos, įskaitant mokesčius arbitrams, kurių maksimalus dydis („lubos“) bus nustatytas pasikonsultavus su Europos Komisija. Fondą valdys trečioji šalis, kuri reguliariai teiks fondo veiklos ataskaitas. Atlikdami metinę peržiūrą, Komercijos departamentas ir Europos Komisija peržiūrės fondo veikimą, įskaitant poreikį patikslinti įmokų arba „lubų“ dydį, ir, be kita ko, svarstys arbitražo procedūrų skaičių, išlaidas ir arbitražo procedūrų trukmę, įskaitant abipusį sutarimą, kad „privatumo skydo“ organizacijos nepatirtų pernelyg didelių išlaidų. Ši nuostata netaikoma advokato mokesčiams ar bet kuriam pagal šią nuostatą įsteigtam fondui.

III PRIEDAS

JAV sekretoriaus Johno Kerry raštas

2016 m. liepos 7 d.

Gerbiama Komisijos nare V. Jourová,

džiaugiuosi galėdamas pranešti, kad pasiekėme bendrą sutarimą dėl Europos Sąjungos ir Jungtinių Amerikos Valstijų „privatumo skydo“ sistemos, kuriai taip pat priklauso ombudsmeno mechanizmas, kuriuo naudodamasi ES institucijos galės ES asmenų vardu teikti prašymus dėl JAV signalų žvalgybos veiksmų.

2014 m. sausio 17 d. Prezidentas Barackas Obama paskelbė apie svarbias žvalgybos reformas, numatytas Prezidento politinėje direktyvoje Nr. 28 (PPD-28). Vadovaudamasis PPD-28, valstybės sekretorę Catheriną A. Novelli, kuri taip pat veikia kaip Tarptautinės informacinių technologijų diplomatijos vyresnioji koordinatorė, paskyriau kontaktiniu asmeniu, kuris nagrinės užsienio Vyriausybių užklausas dėl JAV signalų žvalgybos veiklos. Remdamasis šiomis funkcijomis, įsteigiau „privatumo skydo“ ombudsmeno mechanizmą, veikiantį A priede nustatytais sąlygomis, kurios po mano 2016 m. vasario 22 d. rašto buvo dar atnaujintos. Eiti šias pareigas pavedžiau Sekretorei C. A. Novelli. Sekretorė C. A. Novelli yra nepriklausoma nuo JAV žvalgybos bendruomenės ir tiesiogiai man atskaitinga.

Savo darbuotojams pavedžiau skirti reikalingus išteklius šiam naujam ombudsmeno mechanizmui įgyvendinti ir esu įsitikinęs, kad tai bus veiksminga priemonė, padedanti spręsti ES asmenims rūpimus klausimus.

Pagarbiai
Johnas F. Kerry

A priedas

ES ir JAV „privatumo skydo“ ombudsmeno mechanizmas dėl signalų žvalgybos

Pripažįstant ES ir JAV „privatumo skydo“ sistemos svarbą, šiame memorandume nustatomas naujo mechanizmo, atitinkančio Prezidento politinę direktyvą Nr. 28 (PPD-28) ir susijusio su signalų žvalgyba, įgyvendinimo procesas ⁽¹⁾.

2014 m. sausio 17 d. Prezidentas B. Obama savo kalboje paskelbė apie svarbias žvalgybos reformas. Toje kalboje jis nurodė, kad „[i]š visų jėgų stengiamės apsaugoti ne tik savo tautą, bet ir savo draugus bei sąjungininkus. Mūsų pastangos duos vaisių tik jeigu paprasti kitų šalių piliečiai bus įsitikinę, kad Jungtinės Amerikos Valstijos gerbia ir jų privatumą.“ Prezidentas B. Obama paskelbė apie naujai priimtą politinę direktyvą – PPD-28, – kurioje aiškiai nurodoma, kokių veiksmų imamės užsienio žvalgybos srityje ir ko nedarome.

PPD-28 4 skirsnio d dalyje valstybės sekretoriui pavedama paskirti „Tarptautinės informacinių technologijų diplomatijos vyresnįjį koordinatorių“ (vyresnysis koordinatorius), „kuris <...> veiktų kaip kontaktinis centras, į kurį užsienio Vyriausybės galėtų kreiptis kilus klausimams dėl Jungtinių Amerikos Valstijų vykdomos signalų žvalgybos veiklos“. Nuo 2015 m. sausio mėn. vyresniojo koordinatoriaus pareigas eina sekretorė C. Novelli.

Šiame memorandume aprašomas naujas mechanizmas, kurį vyresnysis koordinatorius naudos, kad palengvintų prašymų dėl prieigos prie duomenų, perduotų pagal ES ir JAV „privatumo skydą“, standartines sutarčių sąlygas, privalomas įmonių taisyklės, išimtis ⁽²⁾ arba galimas būsimas išimtis ⁽³⁾ nacionalinio saugumo tikslais, nagrinėjimą pasinaudojant Jungtinių Amerikos Valstijų taikomuose įstatymuose ir politikoje nustatytais būdais ir šių prašymų patenkinimą.

1. **„Privatumo skydo“ ombudsmenas.** Vyresnioji koordinatorė veiks kaip „privatumo skydo“ ombudsmenė ir, kai tinkama, paskirs papildomus Valstybės departamento pareigūnus, kad padėtų jai vykdyti šiame memorandume nustatytas pareigas. (toliau koordinatorė ir visi pareigūnai, einantys tokias pareigas, bus vadinami „privatumo skydo“ ombudsmenu). „Privatumo skydo“ ombudsmenas glaudžiai dirbs su atitinkamais kitų departamentų ir agentūrų pareigūnais, kurie atsako už prašymų nagrinėjimą pagal taikytiną Jungtinių Amerikos Valstijų teisę ir politiką. Ombudsmenas yra nepriklausomas nuo žvalgybos bendruomenės. Ombudsmenas atsiskaito tiesiogiai Valstybės sekretoriui, kuris užtikrina, kad ombudsmenas vykdytų savo funkcijas objektyviai ir nepriklausomai nuo jokios netinkamos įtakos, kuri gali būti daroma siekiant gauti atitinkamą sprendimą.
2. **Veiksmingas koordinavimas.** „Privatumo skydo“ ombudsmenas galės veiksmingai naudoti ir koordinuoti toliau aprašytas priežiūros institucijas, siekdamas užtikrinti, kad ombudsmeno atsakymas į prašymus, susijusius su ES asmenų skundu, būtų pagrįstas būtina informacija. Kai prašymas yra susijęs su stebėjimo veiklos atitiktimi JAV teisei,

⁽¹⁾ Jeigu Komisijos sprendimas dėl ES ir JAV „privatumo skydo“ suteikiamos apsaugos tinkamumo taikomas Islandijai, Lichtenšteinui ir Norvegijai, „privatumo skydo“ dokumentų rinkinys bus taikomas tiek Europos Sąjungai, tiek šioms trimis šalims. Todėl nuorodos į ES ir jos valstybes nares reiškia nuorodas į Islandiją, Lichtenšteiną ir Norvegiją.

⁽²⁾ Šiomis aplinkybėmis sąvoka „išimtis“ reiškia komercinę duomenų perdavimo operaciją (-as), kuri (-ios) vyksta jeigu: a) duomenų subjektas davė aiškų sutikimą dėl siūlomo duomenų perdavimo; arba b) duomenis perduoti būtina siekiant įvykdyti duomenų subjekto ir duomenų valdytojo sutartį arba įgyvendinti iki sutarties sudarymo taikomas priemones, kurių buvo imtasi atsižvelgiant į duomenų subjekto prašymą; arba c) duomenis perduoti būtina siekiant sudaryti arba įvykdyti sutartį, kurią duomenų valdytojas ir trečioji šalis sudarė atsižvelgdami į duomenų subjekto interesus; arba d) duomenis perduoti būtina arba teisiškai reikalaujama atsižvelgiant į svarbius viešojo intereso pagrindus arba siekiant nustatyti, įgyvendinti arba apginti teisinius reikalavimus; arba e) duomenis perduoti būtina siekiant apsaugoti gyvybiškai svarbius duomenų subjekto interesus; arba f) duomenys perduodami iš registro, kuris pagal įstatymus arba reglamentus yra skirtas informacijai visuomenei teikti ir kuris apskritai yra prieinamas visuomenei arba bet kuriam asmeniui, galinčiam įrodyti teisėtą interesą tiek, kiek konkrečiu atveju įvykdomos įstatyme nustatytos informacijos tikrinimo sąlygos.

⁽³⁾ Šiomis aplinkybėmis sąvoka „galimos būsimos išimties“ reiškia komercinę duomenų perdavimo operaciją (-as), kuri (-ios) vyksta tiek, kiek sąlyga reiškia teisėtą asmens duomenų perdavimą iš ES į JAV: a) duomenų subjektas aiškiai sutiko su siūlomu duomenų perdavimu, po to, kai buvo informuotas apie tokių duomenų perdavimo riziką, kylančią duomenų subjektui dėl sprendimo dėl tinkamumo ir tinkamų apsaugos priemonių nebuvimo; arba b) duomenis perduoti būtina siekiant apsaugoti duomenų subjekto arba kitų asmenų gyvybiškai svarbius interesus, kai duomenų subjektas fiziškai arba teisiškai negali duoti savo sutikimo; arba c) tuo atveju, kai duomenys perduodami į trečiąją šalį arba tarptautinę organizaciją ir netaikomos jokios išimties ar galimos būsimos išimties, bet tik jei duomenys nėra perduodami pakartotinai, yra susiję tik su ribotu duomenų subjektų skaičiumi, yra būtini siekiant apginti teisėtus duomenų valdytojo interesus, kurie nekenkia duomenų subjekto interesams arba teisėms ir laisvėms, kai duomenų valdytojas įvertino visas duomenų perdavimo aplinkybes ir, remdamasis šiuo įvertinimu, nustatė tinkamas asmens duomenų apsaugos priemones.

„privatumo skydo“ ombudsmenas galės bendradarbiauti su viena iš nepriklausomų priežiūros institucijų, turinčių tyrimo įgaliojimus.

- a) „Privatumo skydo“ ombudsmenas glaudžiai dirbs su kitais Jungtinių Amerikos Valstijų Vyriausybės pareigūnais, įskaitant atitinkamas nepriklausomas priežiūros įstaigas, siekdamas užtikrinti, kad tinkami prašymai būtų nagrinėjami ir sprendžiami pagal taikytinus įstatymus ir politiką. Visų pirma „privatumo skydo“ ombudsmenas galės glaudžiai koordinuoti savo veiksmus su Nacionalinės žvalgybos direktoriaus biuru, Teisingumo departamentu ir kitais departamentais ir agentūromis, kurios atitinkamais atvejais dalyvauja Jungtinių Amerikos Valstijų nacionalinio saugumo veiksmuose, ir generaliniais inspektoriais, Informacijos laisvės akto pareigūnais ir pilietinių laisvių ir privatumo pareigūnais.
- b) Jungtinių Amerikos Valstijų Vyriausybė remsis nacionalinio saugumo klausimų koordinavimo ir priežiūros departamentuose ir agentūrose mechanizmais, kad padėtų užtikrinti, jog „privatumo skydo“ ombudsmenas galės imtis veiksmų pagal 4 skirsnio e dalį ir patenkinti pagal 3 skirsnio b dalį pateiktus prašymus.
- c) „Privatumo skydo“ ombudsmenas gali perduoti klausimus, susijusius su prašymais Privatumo ir pilietinių laisvių priežiūros valdybai, kad ji juos išnagrinėtų.

3. Prašymų pateikimas.

- a) Prašymas pirmiausia bus teikiamas valstybių narių priežiūros įstaigoms, atsakingoms už nacionalinio saugumo tarnybų priežiūrą ir (arba) asmens duomenų tvarkymą valdžios institucijose. Prašymą ombudsmenui pateiks ES centralizuota įstaiga (toliau kartu – ES individualių skundų nagrinėjimo įstaiga).
- b) ES individualių skundų nagrinėjimo įstaiga, imdamasi toliau nurodytų veiksmų, užtikrins, kad prašymas būtų tinkamai užpildytas:
 - i) patikrindama asmens tapatybę ir ar asmuo veikia savo vardu, o ne kaip Vyriausybės ar tarpvyriausybės organizacijos atstovas;
 - ii) užtikrindama, kad prašymas būtų pateiktas raštu ir kad jame būtų nurodyta ši pagrindinė informacija:
 - bet kokia informacija, kuri sudaro prašymo pagrindą,
 - informacijos arba teisių gynimo pobūdis,
 - susiję Jungtinių Amerikos Valstijų subjektai, jeigu tokių yra, ir
 - kitos priemonės, kurias prašoma taikyti siekiant gauti prašomą informaciją arba teisių gynimo priemonę ir šiomis priemonėmis gautas atsakymas;
 - iii) patikrindama, kad prašymas yra susijęs su duomenimis, kurie, kaip pagrįstai manoma, buvo perduoti iš ES į Jungtines Amerikos Valstijas pagal „privatumo skydą“, standartines sutarčių nuostatas, įmonėms privalomas taisyklės, išimtis arba galimas būsimas išimtis.
 - iv) preliminariai nustatydamas, kad prašymas nėra nerimtas, nepagrįstas arba pateiktas nesąžiningai.
- c) Kad prašymą pagal šį memorandumą galėtų toliau nagrinėti „privatumo skydo“ ombudsmenas, jame nebūtina įrodyti, kad pareiškėjo duomenis iš tikrųjų tikrino Jungtinių Amerikos Valstijų Vyriausybė vykdydama signalų žvalgybą.

4. Įsipareigojimai palaikyti ryšį su teikiančiąja ES individualių skundų nagrinėjimo įstaiga.

- a) „Privatumo skydo“ ombudsmenas ES individualių skundų nagrinėjimo įstaigai patvirtins prašymo gavimą.
- b) „Privatumo skydo“ ombudsmenas atliks preliminarį peržiūrą, kad patikrintų, ar prašymas užpildytas laikantis 3 skirsnio b dalyje nustatytų reikalavimų. Jeigu „privatumo skydo“ ombudsmenas pastebi kokių nors trūkumų arba turi kokių nors klausimų dėl prašymo išsamumo, jis atkreips dėmesį į šiuos trūkumus ir stengsis juos išspręsti bendradarbiaudamas su ES individualių skundų nagrinėjimo įstaiga.

- c) Jeigu tam, kad būtų palengvintas tinkamas prašymo nagrinėjimas, „privatumo skydo“ ombudsmenui reikia daugiau informacijos apie prašymą arba jeigu asmuo, kuris pateikė prašymą, turi imtis konkrečių veiksmų, „privatumo skydo“ ombudsmenas apie tai informuos ES individualių skundų nagrinėjimo įstaigą.
- d) „Privatumo skydo“ ombudsmenas seks prašymų nagrinėjimo eigą ir prireikus teiks naujausią informaciją teikiančiai ES individualių skundų nagrinėjimo įstaigai.
- e) Užpildžius prašymą, kaip aprašyta šio memorandumo 3 skirsnyje, „privatumo skydo“ ombudsmenas laiku pateiks tinkamą atsakymą teikiančiai ES individualius skundus nagrinėjančiai įstaigai ir laikysis nuolatinės pareigos saugoti informaciją pagal taikytinus įstatymus ir politiką. „Privatumo skydo“ ombudsmenas teiks atsakymą teikiančiai ES individualius skundus nagrinėjančiai įstaigai, patvirtindamas, i) kad skundas buvo tinkamai ištirtas ir ii) kad buvo laikomasi JAV teisės, įstatymų, vykdomųjų įsakų, prezidento direktyvų ir agentūros politikos, kurioje nustatyti ODNI rašte aprašyti apribojimai ir apsaugos priemonės, arba, jeigu šių teisės aktų nebuvo laikomasi, patvirtins, kad reikalavimų nesilaikymo pasekmės buvo pašalintos. „Privatumo skydo“ ombudsmenas nei patvirtins, nei paneigs, ar asmuo buvo stebimas, „privatumo skydo“ ombudsmenas taip pat nepatvirtins, ar buvo taikoma konkreti teisių gynimo priemonė. Kaip paaiškinta 5 straipsnyje, pagal FOIA pateikti prašymai bus nagrinėjami šiame akte ir taikytinose taisyklėse nustatyta tvarka.
- f) „Privatumo skydo“ ombudsmenas palaikys tiesioginį ryšį su ES individualius skundus nagrinėjančia įstaiga, kuri bus atsakinga už prašymą pateikusio asmens informavimą. Jeigu tiesioginiai ryšiai yra toliau aprašytų pagrindinių procesų sudedamoji dalis, tuomet šie ryšiai vyks pagal galiojančias procedūras.
- g) Šiame memorandume nustatyti išipareigojimai nebus taikomi bendro pobūdžio pareiškimams, kad ES ir JAV „privatumo skydas“ neatitinka Europos Sąjungos privatumo apsaugos reikalavimų. Šiame memorandume nurodyti išipareigojimai pagrįsti bendru Europos Komisijos ir JAV Vyriausybės sutarimu, kad, atsižvelgiant į pagal šį mechanizmą duotų išipareigojimų taikymo sritį, gali būti išteklių apribojimų, įskaitant apribojimus, susijusius su prašymais, kurie teikiami pagal Informacijos laisvės aktą (FOIA). Jeigu „privatumo skydo“ ombudsmeno funkcijų vykdymas viršija pagrįstus išteklių apribojimus ir trukdo įgyvendinti šiuos išipareigojimus, JAV Vyriausybė su Europos Komisija aptars bet kokius pakeitimus, kurie gali būti tinkami sprendžiant dėl šios situacijos.
- 5. Prašymai suteikti informacijos.** Prašymai suteikti prieigą prie Jungtinių Amerikos Valstijų įrašų gali būti teikiami ir nagrinėjami pagal Informacijos laisvės aktą (FOIA).
- a) FOIA nustatytos priemonės, kuriomis gali pasinaudoti bet kuris asmuo, kad gautų prieigą prie esamų federalinių agentūros įrašų, nepaisant pareiškėjo pilietybės. Ši nuostata kodifikuota Jungtinių Amerikos Valstijų kodekso 5 antraštinės dalies 552 straipsnyje. Įstatymą ir kitą papildomą informaciją apie FOIA galima rasti internete (www.foia.gov ir <http://www.justice.gov/oip/foia-resources>). Kiekviena agentūra turi FOIA vyriausiąjį pareigūną, o savo svetainėje pateikia informaciją, kaip agentūrai pateikti prašymą pagal FOIA. Agentūrose taikomos tarpusavio konsultacijų FOIA prašymų klausimais procedūros, kuriose naudojami kitos agentūros turimi įrašai.
- b) Pavyzdžiui,
- i) Nacionalinės žvalgybos direktoriaus biuras (ODNI) sukūrė ODNI FOIA portalą: <http://www.dni.gov/index.php/about-this-site/foia>. Šiame portale pateikiama informacija apie prašymo pateikimą, kaip patikrinti pateikto prašymo statusą ir susipažinti su informacija, kurią pagal FOIA atskleidė ir paskelbė ODNI. ODNI FOIA portale pateikiamos nuorodos į kitas FOIA svetaines, kuriomis gali pasinaudoti žvalgybos bendruomenės subjektai: <http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites>.
- ii) Teisingumo departamento Informacijos politikos biuras teikia išsamią informaciją apie FOIA: <http://www.justice.gov/oip>. Tai apima ne tik informaciją apie FOIA prašymo pateikimą Teisingumo departamentui, bet ir Jungtinių Amerikos Valstijų Vyriausybei skirtas gaires apie FOIA reikalavimų aiškinimą ir taikymą.

- c) Pagal FOIA prieigai prie Vyriausybės įrašų taikomos tam tikros išvardytos išimtys. Šios išimtys apima prieigos prie išlaptintos nacionalinio saugumo informacijos, trečiųjų šalių asmens duomenų ir informacijos, susijusios su teisės saugos tyrimais, apribojimus ir yra panašios į kiekvienos ES valstybės narės nustatytus apribojimus, galiojančius pagal jų prieigos prie informacijos teisę. Šie apribojimai amerikiečiams ir užsieniečiams taikomi vienodai.
- d) Ginčai dėl įrašų atskleidimo, kurio prašoma pagal FOIA, gali būti skundžiami administracine tvarka, o vėliau – ir federaliniame teisme. Reikalaujama, kad teismas iš naujo nustatytų, ar įrašai tinkamai saugomi (JAV kodekso 5 antraštinės dalies 552 straipsnio a dalies 4 punkto B papunktis), ir gali įpareigoti Vyriausybę suteikti prieigą prie įrašų. Kai kuriais atvejais teismai panaikino Vyriausybės pareiškimus, kad informacija turėtų būti saugoma kaip išlaptinta. Nors piniginių kompensacijų negalima gauti, teismai gali priteisti atlyginti advokato mokesčius.

6. Prašymai imtis papildomų veiksmų. Prašymas, kuriame teigiama, kad buvo pažeista teisė, arba nurodomas kitas netinkamas elgesys, bus perduotas atitinkamai Jungtinių Amerikos Valstijų Vyriausybės įstaigai, įskaitant nepriklausomas priežiūros įstaigas, turinčias įgaliojimus tirti atitinkamą prašymą ir spręsti reikalavimų nesilaikymo klausimus, kaip aprašyta toliau.

- a) Generaliniai inspektoriai pagal įstatymą yra nepriklausomi; turi plačius įgaliojimus atlikti tyrimus, auditą ir peržiūrėti programas, įskaitant sukčiavimo ir piktnaudžiavimo arba teisės pažeidimo atvejų peržiūras, ir gali rekomenduoti imtis taisomųjų veiksmų.
- i) Pakeistame 1978 m. Generalinio inspektoriaus akte nustatyta federalinių generalinių inspektorių pareigybė, daugumoje agentūrų jie veikia kaip nepriklausomi ir nešališki pareigūnai, kurių pareiga – kovoti su atitinkamose jų agentūrose pasitaikančiais lėšų švaistymo, sukčiavimo ir piktnaudžiavimo programomis ir operacijomis atvejais. Šiuo tikslu kiekvienas generalinis inspektorius atsako už auditą ir tyrimus, susijusių su jo agentūros programomis ir operacijomis, atlikimą. Be to, generaliniai inspektoriai vadovauja politinei veiklai, kuria siekiama skatinti ekonomiką, veiksmingumą ir efektyvumą ir užkirsti kelią sukčiavimui ir piktnaudžiavimui įgyvendinant agentūros programas ir vykdant operacijas bei atskleisti tokius atvejus, taip pat koordinuoja ir teikia rekomendacijas dėl šios politinės veiklos.
- ii) Kiekvienas žvalgybos bendruomenės subjektas turi savo generalinio inspektoriaus biurą, kuris, be kitų pareigų, turi pareigą prižiūrėti užsienio žvalgybos veiklą. Paskelbta nemažai generalinio inspektoriaus ataskaitų apie žvalgybos programas.
- iii) Pavyzdžiui,

— Žvalgybos bendruomenės generalinio inspektoriaus biuras (IC IG) buvo įsteigtas pagal 2010 m. fiskalinių metų (<http://www.gpo.gov/fdsys/pkg/PLAW-111publ259/pdf/PLAW-111publ259.pdf>) Žvalgybos įgaliojimų akto 405 straipsnį. IC IG turi pareigą atlikti visos žvalgybos bendruomenės auditą, tyrimus, patikrinimus ir peržiūras, per kurias nustatoma ir šalinama sisteminė rizika, pažeidžiamos vietos ir trūkumai, būdingi visoms žvalgybos bendruomenės misijoms, siekiant daryti teigiamą poveikį visai žvalgybos bendruomenės ekonomikai ir efektyvumui. IC IG turi įgaliojimus tirti skundus ar informaciją, susijusią su tariamu teisės, taisyklės ar reglamento pažeidimu, lėšų švaistymu, sukčiavimu, piktnaudžiavimu įgaliojimais arba dideliu ar konkrečiu pavojumi visuomenės sveikatai ir saugumui, kiek tai susiję su ODNI ir (arba) žvalgybos bendruomenės žvalgybos programomis ir veikla. IC IG teikia informaciją, kaip tiesiogiai susisiekti su IC IG ir pateikti pranešimą: <http://www.dni.gov/index.php/about-this-site/contact-the-ig>.

— JAV teisingumo departamento (DOJ, <https://www.justice.gov>) Generalinio inspektoriaus biuras (OIG) yra pagal įstatymą sukurtas nepriklausomas subjektas, kurio misija – atskleisti lėšų švaistymą, sukčiavimą, piktnaudžiavimą ir netinkamą elgesį įgyvendinant DOJ programas ir personalo valdymo srityje bei užkirsti tam kelią, taip pat skatinti šių programų ekonomiškumą ir veiksmingumą. OIG tiria tariamus DOJ darbuotojų baudžiamosios ir civilinės teisės pažeidimus, taip pat atlieka auditą ir tikrina DOJ programas. OIG turi jurisdikciją nagrinėti visus skundus dėl Teisingumo departamento, įskaitant Federalinį tyrimų biurą, Vaistų administraciją, Federalinį kalėjimų biurą, JAV maršalo tarnybą, Alkoholio, tabako, šaunamųjų ginklų ir sprogstamųjų medžiagų biurą, Jungtinių Amerikos Valstijų advokatų kontorų darbuotojų kituose Teisingumo departamento skyriuose ar biuruose dirbančių darbuotojų netinkamo elgesio. (Vienintelė išimtis yra susijusi su kaltinimais dėl Departamento advokato arba teisės saugos darbuotojo netinkamo

elgesio įgyvendinant Departamento advokato įgaliojimus tirti, bylinėtis arba teikti teisinę konsultaciją, kuriuos turi pareigą nagrinėti Profesinės atsakomybės biuro departamentas.) Be to, 2001 m. spalio 26 d. įsigaliojusio JAV patriotinio akto 1001 straipsnyje generaliniam inspektoriui pavedama peržiūrėti informaciją ir priimti skundus dėl tariamo Teisingumo departamento darbuotojų piktnaudžiavimo pilietinėmis teisėmis ir laisvėmis. OIG tvarko viešą svetainę (<https://www.oig.justice.gov>), kurioje yra specialii skiltis skundams pateikti („Skundų karštoji linija“) (<https://www.oig.justice.gov/hotline/index.htm>).

- b) Jungtinių Amerikos Valstijų Vyriausybei pavaldūs privatumo ir pilietinių laisvių biurai ir subjektai taip pat turi atitinkamas pareigas. Pavyzdžiui,
- i) 2007 m. 9/11 komisijos akto įgyvendinimo rekomendacijų 803 straipsnyje, kuris kodifikuotas Jungtinių Amerikos Valstijų kodekso 42 antraštinės dalies 2000-ee1 straipsnyje, tam tikruose departamentuose ir agentūrose (įskaitant Valstybės departamentą, Teisingumo departamentą ir ODNI) nustatytos privatumo ir pilietinių laisvių pareigūnų pareigybės. 803 straipsnyje nustatyta, jog šie privatumo ir pilietinių laisvių pareigūnai veikia kaip pagrindiniai patarėjai, kurie, be kita ko, užtikrina, kad toks departamentas, agentūra arba subjektas taikytų tinkamas procedūras, kuriomis nagrinėtų asmenų, teigiančių, kad toks departamentas, agentūra ar subjektas pažeidė jų privatumą ar pilietines laisves, skundus.
 - ii) ODNI Pilietinių laisvių ir privatumo biurui (ODNI CLPO) vadovauja ODNI pilietinių laisvių apsaugos pareigūnas, kurio pareigybė nustatyta pakeistu 1948 m. Nacionalinio saugumo aktu. ODNI CLPO, be kita ko, užtikrina, kad žvalgybos bendruomenės subjektų politikoje ir procedūrose būtų nustatytos tinkamos privatumo ir pilietinių laisvių apsaugos priemonės ir skundų, kuriuose teigiama, kad ODNI programose ir veikloje buvo piktnaudžiaujama pilietinėmis laisvėmis ir privatumu arba pilietinės laisvės ir privatumas buvo pažeistas, peržiūros ir tyrimo mechanizmai. ODNI CLPO savo svetainėje teikia visuomenei informaciją, įskaitant skundo pateikimo instrukcijas: www.dni.gov/clpo. Jeigu ODNI CLPO gauna skundą dėl privatumo ar pilietinių laisvių, susijusį su žvalgybos bendruomenės programomis ir veikla, ji su kitais žvalgybos bendruomenės subjektais koordinuos, kaip tas skundas turėtų būti toliau nagrinėjamas žvalgybos bendruomenėje. Pažymėtina, kad Nacionalinio saugumo agentūra (NSA) taip pat turi Pilietinių laisvių ir privatumo biurą, kurio svetainėje teikiama informacija apie jo atsakomybės sritis (https://www.nsa.gov/civil_liberties/). Jeigu iš informacijos matyti, kad agentūra nesilaiko privatumo reikalavimų (pvz., PPD-28 4 skirsnio reikalavimo), tuomet agentūros taiko savo atitikties mechanizmus, kad peržiūrėtų ir ištaisytų incidentą. Pagal PPD-28 reikalaujama, kad agentūros apie incidentų ištaisymą praneštų ODNI.
 - iii) Teisingumo departamento Privatumo ir pilietinių laisvių biuras (OPCL) padeda Departamento vyriausiajam privatumo ir pilietinių laisvių pareigūnui (CPCLO) vykdyti savo pareigas. Pagrindinė OPCL misija – saugoti Amerikos žmonių privatumą ir pilietines laisves atliekant Departamento operacijų peržiūrą, priežiūrą ir koordinavimą. OPCL teikia teisinę konsultaciją ir rekomendacijas Departamento padaliniams; užtikrina, kad Departamentas paisytų privatumo reikalavimo, įskaitant 1974 m. Privatumo akto, 2002 m. E. Vyriausybės akto ir Federalinio informacijos saugumo valdymo akto privatumo nuostatų, taip pat administracinių politinių direktyvų, priimtų siekiant papildyti šiuos aktus, laikymąsi; rengia Departamento privatumo mokymo medžiagą ir organizuoja mokymo kursus; padeda CPCLO rengti Departamento privatumo politiką; rengia su privatumu susijusias ataskaitas prezidentui ir Kongresui ir peržiūri informacijos tvarkymo praktiką Departamente, kad užtikrintų tokios praktikos atitiktį privatumo ir pilietinių laisvių apsaugai. OPCL teikia visuomenei informaciją apie savo pareigas svetainėje <http://www.justice.gov/opcl>.
 - iv) Pagal JAV kodekso 42 antraštinės dalies 2000ee ir kitus straipsnius Privatumo ir pilietinių laisvių valdyba nuolat peržiūri: i) departamentų, agentūrų ir vykdomosios valdžios subjektų, kurie veikia siekdami apsaugoti tautą nuo terorizmo ir užtikrinti privatumo ir pilietinių laisvių apsaugą, politiką ir procedūras ir tai, kaip jos įgyvendinamos, ir ii) kitus vykdomosios valdžios veiksmus, susijusius su i punkte nurodyta veikla, kad nustatytų, ar tokia veikla tinkamai apsaugomas privatumas ir pilietinės laisvės ir ar ji dera su pagrindiniais įstatymais, reglamentais ir politika, galiojančia privatumo ir pilietinių laisvių srityje. Ji gauna ir peržiūri ataskaitas ir kitą informaciją iš privatumo pareigūnų ir pilietinių laisvių pareigūnų ir, kai tinkama, teikia jiems rekomendacijas dėl jų veiklos. 2007 m. 9/11 komisijos akto įgyvendinimo rekomendacijų 803 straipsnyje, kuris kodifikuotas JAV kodekso 42 antraštinės dalies 2000ee-1 straipsnyje, nurodoma, kad aštuonių federalinių agentūrų (įskaitant gynybos sekretorių, vidaus saugumo sekretorių, Nacionalinės žvalgybos direktorių ir Centrinės žvalgybos valdybos direktorių) ir bet kurių papildomų Valdybos paskirtų agentūrų

privatumo ir pilietinių laisvių pareigūnai teikia PCLOB periodines ataskaitas, kuriose, be kita ko, nurodo atitinkamos agentūros gautų skundų dėl tariamų pažeidimų skaičių, pobūdį ir esmę. PCLOB steigiamajame įstatyme nurodyta, kad Valdyba priima šias ataskaitas ir, kai tinkama, teikia privatumo ir pilietinių laisvių pareigūnams rekomendacijas dėl jų veiklos.

IV PRIEDAS

Federalinės prekybos komisijos pirmininkės Edith Ramirez raštas

2016 m. liepos 7 d.

GAUTA E. PAŠTU

Vėrai Jourovái
už teisingumą, vartotojų reikalus ir lyčių lygybę atsakingai Komisijos narei
Europos Komisija
Rue de la Loi/Wetstraat 200
1049 Briuselis
Belgija

Gerbiamą Komisijos narę V. Jourová,

Jungtinių Amerikos Valstijų federalinė prekybos komisija (FPK) teigiamai vertina galimybę aprašyti, kaip ji užtikrina naujos ES ir JAV „privatumo skydo“ sistemos (toliau – „privatumo skydo“ sistema arba sistema) veikimą. Manome, kad sistema atliks lemiamą vaidmenį palengvinant komercinių sandorių, kuriuose užtikrinama privatumo apsauga, sudarymą vis glaudesniais tarpusavio ryšiais susijusioje pasaulinėje rinkoje. Ši sistema sudarys sąlygas įmonėms atlikti svarbias operacijas globalios ekonomikos sąlygomis, kartu padės užtikrinti, kad ES vartotojai naudotųsi svarbiomis privatumo apsaugos priemonėmis. FPK jau seniai įsipareigojo užtikrinti privatumo apsaugą tarpvalstybiniu mastu, o naujos sistemos veikimo užtikrinimui skirs ypatingą dėmesį. Toliau paaiškiname bendrąsias FPK užtikrinamos griežtos apsaugos istoriją, įskaitant pradinės „saugaus uosto“ programos įgyvendinimą, taip pat FPK požiūrį į naujos sistemos užtikrinimą.

FPK įgyvendinti „saugaus uosto“ programą pirmą kartą viešai įsipareigojo 2000 metais. Tuo metu pareigas ėjęs FPK pirmininkas Robertas Pitas savo iniciatyva nusiuntė Europos Komisijai raštą, kuriame išdėstė FPK įsipareigojimą dėti visas pastangas, kad užtikrintų „saugaus uosto“ privatumo principų laikymąsi. FPK toliau laikėsi šio įsipareigojimo išskeldama beveik 40 bylų, atlikdama įvairius papildomus tyrimus ir bendradarbiaudama su atskiromis Europos duomenų apsaugos institucijomis (ES DAI), kai sprendė abiem pusėms svarbius klausimus.

2013 m. lapkričio mėn. Europos Komisijai išreiškus nerimą dėl „saugaus uosto“ programos administravimo ir įgyvendinimo, mes kartu su JAV komercijos departamentu pradėjome konsultuotis su Europos Komisijos pareigūnais, kad ištirtume programos stiprinimo būdus. Vykstant šioms konsultacijoms, 2015 m. spalio 6 d. Europos Teisingumo Teismas priėmė sprendimą *Schrems* byloje, kurioje, be kita ko, Europos Komisijos sprendimą dėl „saugaus uosto“ programos tinkamumo pripažino negaliojančiu. Po šio sprendimo toliau glaudžiai bendradarbiauome su Komercijos departamentu ir Europos Komisija stengdamiesi stiprinti ES gyventojams suteikiamas privatumo apsaugos priemones. „Privatumo skydo“ sistema yra šių vykstančių konsultacijų rezultatas. Kaip ir „saugaus uosto“ programos atveju, FPK šiuo raštu įsipareigoja dėti visas pastangas, kad užtikrintų naujosios sistemos veikimą. Šiuo raštu patvirtinamas minėtas įsipareigojimas.

Visų pirma patvirtiname savo įsipareigojimą keturioje pagrindinėse srityse: 1) teikti prioritetą perduotoms byloms ir jas nagrinėti; 2) šalinti klaidingus arba apgaulingus pareiškimus dėl dalyvavimo „privatumo skydo“ sistemoje; 3) nuolat stebėti, kaip laikomasi reikalavimų, ir 4) imtis aktyvesnių veiksmų ir bendradarbiauti su ES DAI reikalavimų užtikrinimo srityje. Toliau pateikiame išsamią informaciją apie kiekvieną iš šių įsipareigojimų ir svarbias aplinkybes, susijusias su FPK vaidmeniu užtikrinant vartotojų apsaugą ir „saugaus uosto“ veikimą, taip pat išsamiau apibūdinsime Jungtinių Amerikos Valstijų privatumo sistemą ⁽¹⁾.

I. APLINKYBĖS

A. FPK užtikrinamas privatumas ir politinis darbas

FPK turi plačius civilinius reikalavimo užtikrinimo įgaliojimus, susijusius su vartotojų apsauga ir konkurencijos skatinimu prekybos srityje. Įgyvendindama įgaliojimus vartotojų apsaugos srityje, FPK vykdo įvairius įstatymus, kad apsaugotų

⁽¹⁾ Papildomos informacijos apie JAV federalinius ir valstijų įstatymus pateikiame A priede, o B priede pateikiame neseniai atliktų privatumo ir saugumo užtikrinimo veiksmų santrauką. Šią santrauką taip pat galima rasti FPK svetainėje adresu <https://www.ftc.gov/reports/privacy-data-security-update-2015>.

vartotojų duomenų privatumą ir saugumą. Pagrindiniame įstatyme, FPK akte, kurį įgyvendina FPK, draudžiami „nesąžiningi“ arba „apgaulingi“ veiksmai ar praktika prekybos srityje arba darantys poveikį prekybai ⁽¹⁾. Pareiškimas, neveikimas arba praktika yra apgaulingi, jeigu jie yra esminiai ir, tikėtina, gali klaidinti šiomis aplinkybėmis veikiančius vartotojus ⁽²⁾. Subjekto praktika yra nesąžininga, jeigu ja sukeliamas arba, tikėtina, gali būti sukelta didelė žala, kurios vartotojas pagrįstai negali išvengti, arba kuri negali būti kompensuojama vartotojui arba ištaisoma konkurencinėje aplinkoje ⁽³⁾. FPK taip pat vykdo konkrečius įstatymus, kad apsaugotų su sveikata, išsiskolinimais ir kitais finansiniais klausimais susijusią informaciją, taip pat vaikų informaciją internete, ir dėl kiekvieno iš šių įstatymų priėmė įgyvendinimo taisykles.

FPK jurisdikcija pagal FPK aktą taikoma „prekybos srityje kylantiems arba jai poveikį darantiems klausimams“. FPK neturi jurisdikcijos nagrinėti baudžiamosios teisės užtikrinimo arba nacionalinio saugumo klausimų. FPK taip pat negali kontroliuoti daugumos kitų Vyriausybės veiksmų. Be to, FPK jurisdikcijai prekybos srityje taikomos išimties, įskaitant su bankais, oro vežėjais, draudimo bendrovėmis ir bendra telekomunikacijų paslaugų teikėjų vežimo veikla susijusios išimties. FPK taip pat neturi jurisdikcijos daugumos ne pelno organizacijų atžvilgiu, tačiau ji turi jurisdikciją apgaulingų labdaros fondų ir kitų ne pelno organizacijų, kurios iš tikrųjų siekia pelno, atžvilgiu. FPK taip pat turi jurisdikciją ne pelno organizacijų, kurios veikia siekdamos pelno savo nariams, atžvilgiu, įskaitant esminės ekonominės naudos šioms nariams teikimą ⁽⁴⁾. Kai kuriais atvejais FPK jurisdikcija sutampa su kitų teisėsaugos institucijų jurisdikcija.

Užmezgėme tvirtus darbo santykius su federalinėmis ir valstijų valdžios institucijomis ir glaudžiai su jomis dirbame koordinuodami tyrimus arba, kai tinkama, perduodami bylas.

Vykdyimo užtikrinimas yra pagrindinis FPK požiūrio į privatumo apsaugą aspektas. Iki šiol FPK iškėlė daugiau nei 500 bylų, susijusių su vartotojų informacijos privatumo ir saugumo apsauga. Ši bylų visuma apima ne internete ir internete pateiktą informaciją ir vykdyimo veiksmus prieš dideles ir mažas bendroves, kuriose teigiama, kad jos nesugebėjo tinkamai tvarkyti neskelbtinų vartotojų duomenų, neužtikrinto vartotojų asmeninės informacijos apsaugos, apgaulingai sekė vartotojus internete, siuntė vartotojams brukalus, įdiegė vartotojų kompiuteriuose šnipinėjimo programas ir kitą kenkimo programinę įrangą, pažeidė „Do Not Call“ bei kitas telemarketingo taisykles ir netinkamai rinko vartotojų informaciją mobiliuosiuose įrenginiuose ir ja dalijosi. FPK vykdyimo veiksmais, kurių ji imasi fizinėje ir skaitmeninėje aplinkoje, bendrovėms siunčiama rimta žinia apie poreikį apsaugoti vartotojų privatumą.

FPK taip pat įgyvendino įvairias politines iniciatyvas, kuriomis siekė didinti vartotojų privatumą, kuris yra FPK vykdyimo veiksmų pagrindas. FPK surengė praktinius seminarus ir parengė ataskaitas, kuriose rekomenduojama vadovautis geriausia patirtimi, susijusia su privatumo mobiliuoje ekosistemoje stiprinimu, skaidrumo duomenų tarpininkų sektoriuje didinimu, kuo didesnės didelių duomenų kiekio naudos užtikrinimu kartu sumažinant riziką, visų pirma kylančią mažas pajamas gaunantiems ir nepakankamai aptarnaujamiems vartotojams, ir kuriose atkreiptas dėmesys į privatumo ir saugumo aspektus, be kita ko, susijusius su veido atpažinimu ir daiktų internetu.

FPK taip pat užsiima vartotojų ir įmonių švietimu, kad didintų savo reikalavimų užtikrinimo ir politikos tobulinimo iniciatyvų poveikį. FPK naudoja įvairias priemones – leidinius, elektroninius išteklius, praktinius seminarus ir socialinę žiniasklaidą, kad suteiktų mokymo medžiagą pačiomis įvairiausiomis temomis, įskaitant mobiliąsias programas, vaikų privatumą ir duomenų saugumą. Visai neseniai Komisija pradėjo įgyvendinti iniciatyvą „Saugumas svarbiausia“, kurioje įmonėms pateikiamos naujos praktinė patirtimi, kurią agentūra įgijo nagrinėdama saugumo bylas, taip pat surengdama įvairius praktinius seminarus visoje šalyje, pagrįstos rekomendacijos. Be to, FPK ilgą laiką yra lyderė šviečiant vartotojus pagrindiniais kompiuterinio saugumo klausimais. Praėjusiais metais mūsų tinklalapis „On Guard Online site“ ir jo analogas ispanų kalba „Alerta en Línea“ buvo peržiūrėtas daugiau nei 5 mln. kartų.

B. ES vartotojams palankios JAV teisinės apsaugos priemonės

Sistema veiks platesniame JAV privatumo kontekste, kuriame ES vartotojų apsauga užtikrinama įvairiais būdais.

⁽¹⁾ JAV kodekso 15 antraštinės dalies 45 straipsnio a dalis.

⁽²⁾ Žr. FPK politinį pareiškimą dėl apgaulės, pridėdamą prie Cliffdale Assocs., Inc., 103F.T.C. 110,174 (1984),

⁽³⁾ skelbiama adresu <https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception>.

⁽⁴⁾ Žr. JAV kodekso 15 antraštinės dalies 45 straipsnio n dalį; FPK politinį pareiškimą dėl nesąžiningumo, pridėdamą prie Int'l Harvester Co., 104, F.T.C. 949, 1070 (1984), skelbiamas adresu <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>.

FPK akte nustatytas nesąžiningų arba apgaulingų veiksmų ar praktikos draudimas taikomas ne tik JAV vartotojams, siekiant juos apsaugoti nuo JAV bendrovių, nes jame aptariama praktika, kuri 1) sukelia arba gali sukelti pagrįstai numatomą žalą Jungtinėse Amerikos Valstijose, arba 2) yra susijusi su esminiu elgesiu Jungtinėse Amerikos Valstijose. Be to, siekdamas apsaugoti užsienio vartotojus, FPK gali naudoti visas teisių gynimo priemones, įskaitant restituciją, kuri yra prieinama vidaus vartotojams.

Tiesą sakant, FPK darbas reikalavimų užtikrinimo srityje yra labai naudingas tiek JAV, tiek užsienio vartotojams. Pavyzdžiui, mūsų bylos, kuriomis užtikrinamas FPK akto 5 straipsnio laikymasis, padėjo užtikrinti vienodą JAV ir užsienio vartotojų privatumo apsaugą. Byloje prieš informacijos tarpininką „Accu search“ FPK teigė, kad bendrovė pardavė slapstus telefoninius įrašus trečiosioms šalims be vartotojų žinios arba sutikimo, ir tai buvo nesąžiningi veiksmai, kuriais pažeistas FPK akto 5 straipsnis. „Accu search“ pardavė informaciją, susijusią su JAV ir užsienio vartotojais ⁽¹⁾. Teismas dėl „Accu search“ priėmė išakymą, kuriuo, be kita ko, uždraudė teikti rinkai ar pardavinėti asmeninę informaciją be rašytinio sutikimo, išskyrus atvejus, kai tokia informacija buvo teisėtai gauta iš viešai prieinamų informacijos šaltinių, ir nurodė sumokėti beveik 200 000 JAV dolerių kompensaciją ⁽²⁾.

FPK susitarimas su bendrove „TRUSTe“ yra kitas pavyzdys. Susitarimu užtikrinama, kad vartotojai, įskaitant Europos Sąjungos vartotojus, galėtų remtis pasaulinės savireguliacijos organizacijos pareiškimais, kuriuos ji pateikia dėl savo viduje ir užsienyje teikiamų internetinių paslaugų peržiūros ir sertifikavimo ⁽³⁾. Dar svarbiau, kad mūsų veiksmai „TRUSTe“ atžvilgiu taip pat padeda stiprinti privatumo savireguliacinę sistemą platesniu mastu užtikrinant subjektų, kurie dalyvauja savireguliacijos schemose, įskaitant tarpvalstybines privatumo sistemas, atskaitomybę.

FPK taip pat vykdo kitus specialius įstatymus, kuriais užtikrinama ne tik JAV vartotojų apsauga, pvz., Vaikų privatumo internete apsaugos aktas (COPPA). COPPA, be kita ko, reikalaujama, kad vaikams skirtų svetainių ir internetinių paslaugų operatoriai arba visai auditorijai skirtose svetainėse, kuriose, kaip žinoma, renkama asmeninė informacija iš 13 metų nesulaukusių vaikų, būtų pateiktas išpėjimas tėvams ir gaunamas tėvų sutikimas. JAV veikiančios svetainės ir paslaugos, kurioms taikomas COPPA ir kuriose renkama asmeninė informacija iš užsienio vaikų, turi atitikti COPPA. Užsienyje veikiančios svetainės ir internetinės paslaugos turi atitikti COPPA, jeigu jos orientuotos į JAV vaikus arba jeigu, kaip žinoma, jose renkama asmeninė informacija iš JAV vaikų. Be JAV federalinių įstatymų, kurių vykdymą užtikrina FPK, tam tikruose kituose federaliniuose ir valstijų lygmeniu galiojančiuose vartotojų privatumo apsaugos įstatymuose gali būti numatyta papildoma ES vartotojų apsauga.

C. „Saugaus uosto“ užtikrinimas

Vykdydama privatumo ir saugumo užtikrinimo programą, FPK taip pat siekė apsaugoti ES vartotojus iškeldama vykdymo bylas dėl „saugaus uosto“ nuostatų pažeidimo. FPK iškėlė 39 bylas dėl „saugaus uosto“ reikalavimų užtikrinimo: 36 bylos buvo susijusios su klaidingais pareiškimais dėl sertifikavimo ir trys bylos iškeltos „Google“, „Facebook“ ir „Myspace“, susijusios su tariamais „saugaus uosto“ privatumo principų pažeidimais ⁽⁴⁾. Šios bylos parodo, kad sertifikavimo reikalavimai yra užtikrinami, be to, jose galima pamatyti už jų nesilaikymą kylančias pasekmes. Pagal dvidešimties metų sutikimo reikalavimą „Google“, „Facebook“ ir „Myspace“ įpareigojamos įgyvendinti išsamias privatumo programas, kurios turi būti sukurtos taip, kad padėtų spręsti privatumo riziką, susijusią su naujų ir esamų produktų ir paslaugų tobulinimu ir valdymu, ir užtikrinti asmeninės informacijos privatumą ir konfidencialumą. Pagal šiuos reikalavimus parengtose išsamiose programose turi būti nurodyta numatoma esminė rizika ir kontrolės priemonės šiai rizikai suvaldyti. Bendrovės taip pat turi pateikti savo privatumo programas nuolatiniam nepriklausomam vertinimui ir tai turi būti daroma FPK. Reikalavimais bendrovėms taip pat draudžiama laikytis klaidingos privatumo praktikos ir dalyvauti bet kurioje privatumo ar saugumo programoje. Šis draudimas taip pat bus taikomas bendrovės veiksams ir praktikai pagal naują „privatumo skydo“ sistemą. FPK gali užtikrinti šių reikalavimų vykdymą skirdama civilines baudas.

⁽¹⁾ Žr. California Dental Ass'n v. FTC, 526 U.S. 756 (1999).

⁽²⁾ Žr. Kanados privatumo komisaro biuro pagal PIPDEA pateiktą skundą dėl „Accu search, Inc.“, kuris veikė kaip „Abika.com“, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. Kanados privatumo komisaro biuras pateikė *amicus curiae* raštą, kuriuo apskundė FPK bylą, ir, atlikęs savo tyrimą, padarė išvadą, kad „Accu search“ praktika taip pat pažeidė Kanados teisę.

⁽³⁾ Žr. FTC v. Accu search, Inc., Nr. 06CV015D (D. Wyo., 2007 m. gruodžio 20 d.), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

⁽⁴⁾ Žr. sprendimą byloje True Ultimate Standards Everywhere, Inc., Nr. C-4512 (FPK. 2015 m. kovo 12 d.) (sprendimas ir išakymas), skelbiama adresu <https://www.ftc.gov/system/files/documents/cases/150318trust-edo.pdf>.

Tiesą sakant, „Google“ 2012 m. sumokėjo rekordinę 22,5 mln. JAV dolerių baudą, kad patenkintų reikalavimus, susijusius su pažeistu reikalavimu. Todėl šie FPK reikalavimai padeda užtikrinti daugiau nei milijardo vartotojų visame pasaulyje, iš kurių šimtai milijonų gyvena Europoje, apsaugą.

FPK bylose taip pat daug dėmesio skirta neteisingsiems, apgaulingiems arba klaidinantiems pareiškimams, susijusiems su dalyvavimu „saugiame uoste“. FPK šiuos pareiškimus vertina rimtai. Pavyzdžiui, byloje FPK prieš *Karnani* FPK pareiškė ieškinį 2011 m. Jungtinių Amerikos Valstijų internetinio marketingo specialistui – ji teigė, kad jis ir jo bendrovė klaidino Britanijos vartotojus, priversdama juos manyti, kad bendrovė buvo įsisteigusi Jungtinėje Karalystėje, įskaitant „uk“ interneto plėtinį naudojimą ir nuorodą į Britanijos valiutą bei JK pašto sistemą⁽¹⁾. Tačiau kai gaudavo produktus, vartotojai sužinodavo turį sumokėti importo mokesčius, kurių nesitikėjo, gavę garantijas, kurios negalioja Jungtinėje Karalystėje, ir sumokėti mokesčius, susijusius su lėšų susigrąžinimu. FPK taip pat pateikė kaltinimus, kad atsakovai apgavo vartotojus dėl savo dalyvavimo „saugaus uosto“ programoje. Visų pirma pažymėtina, kad visi nukentėję vartotojai gyveno Jungtinėje Karalystėje.

Dauguma kitų mūsų „saugaus uosto“ užtikrinimo bylų buvo susijusios su organizacijomis, kurios prisijungė prie „saugaus uosto“ programos, tačiau nesugebėjo atnaujinti savo metinio patvirtinimo ir toliau teigė esančios programos narės. Kaip aptarta toliau, FPK taip pat išipareigoja šalinti klaidingus pareiškimus dėl dalyvavimo „privatumo skydo“ sistemoje. Ši strateginė reikalavimų užtikrinimo veikla papildys intensyvesnius Komercijos departamento veiksmus tikrinant atitiktį programos reikalavimams, susijusiems su sertifikavimu ir pakartotiniu sertifikavimu, veiksminga atitikties stebėseną, įskaitant sistemos dalyviams skirtų klausimynų siuntimą, ir jos didesnes pastangas nustatyti klaidingus pareiškimus dėl narystės sistemoje ir bet kokią netinkamą sistemos sertifikavimo ženklo naudojimą⁽²⁾.

II. PERDUODAMŲ BYLŲ PRIORITETAIR TYRIMAI

Kaip ir „saugaus uosto“ programoje, FPK išipareigoja pirmenybę teikti ES valstybių narių perduotoms byloms, susijusioms su „privatumo skydu“. Pirmenybę taip pat teiksime byloms dėl savireguliacijos rekomendacijų, susijusių su „privatumo skydo“ sistemos reikalavimų nesilaikymu, gautoms iš privatumo savireguliacinių organizacijų ir kitų nepriklausomų ginčų sprendimo įstaigų.

Siekdama palengvinti bylų perdavimą pagal sistemą iš ES valstybių narių, FPK kuria standartizuotą bylų perdavimo procesą ir teikia ES valstybėms narėms rekomendacijas dėl informacijos, kuri geriausiai padėtų FPK tirti perduotą bylą, rūšių. Atlikdama šiuos veiksmus, FPK paskirs kontaktinę agentūrą, kuriai ES valstybės narės galės perduoti bylas. Tai naudingiausia, kai perduodančioji institucija atlieka preliminarų tariamo pažeidimo tyrimą ir gali bendradarbiauti su tyrimą atliekančia FPK.

Gavusi bylą iš ES valstybės narės arba savireguliacinės organizacijos, FPK gali imtis įvairių veiksmų, kad išspręstų iškeltus klausimus. Pavyzdžiui, galime peržiūrėti bendrovės privatumo politiką, tiesiogiai gauti papildomą informaciją iš bendrovės arba trečiųjų šalių, bendradarbiauti su byla perdavusia institucija, įvertinti, ar yra pažeidimų modelis arba ar yra daug nukentėjusių vartotojų, nustatyti, ar perduota byla yra susijusi su Komercijos departamento kompetencijai priklausančiais klausimais, įvertinti, ar būtų naudinga mokyti vartotojus ir įmones, ir, kai tinkama, pradėti vykdymo bylą.

FPK taip pat išipareigoja keistis informacija apie perduotas bylas su perduodančiosiomis teisėsaugos institucijomis, įskaitant informaciją apie perduotos bylos statusą, ir laikytis konfidencialumo įstatymų ir apribojimų. Tiek, kiek pagrįsta atsižvelgiant į perduotų bylų skaičių ir rūšį, teikiama informacija sudarys perduotų klausimų vertinimą, įskaitant svarbiausių iškeltų klausimų ir bet kokių veiksmų, kurių pagal savo kompetenciją ėmėsi FPK, kad ištaisytų teisės pažeidimus, aprašymą. FPK perduodančiajai institucijai taip pat teiks grįžtamąją informaciją apie gautų bylų rūšis, kad padidintų veiksmų, kuriais siekiama spręsti neteisėto elgesio problemą, veiksmingumą. Jeigu perduodančioji teisėsaugos

⁽¹⁾ Žr. sprendimą byloje *Google, Inc.*, Nr. C-4336 (FPK, 2011 m. spalio 13 d.) (sprendimas ir įsakymas), <https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz>; sprendimą byloje *Facebook, Inc.*, Nr. C-4365 (FPK, 2012 m. liepos 27 d.) (sprendimas ir įsakymas), skelbiama adresu <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook>; sprendimą byloje *My space LLC*, Nr. C-4369 (FPK, 2012 m. rugpjūčio 30 d.) (sprendimas ir įsakymas), skelbiama adresu <https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace>.

⁽²⁾ Žr. *FTC v. Karnani*, Nr. 2:09-cv-05276 (C.D. Cal., 2011 m. gegužės 20 d.) (galutinis sprendimas), skelbiamas adresu <https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf>; taip pat žr. *Lesley Fair*, FTC Business Center Blog, *Around the World in Shady Ways*, <https://www.ftc.gov/blog/2011/06/around-world-shady-ways> (2011 m. birželio 9 d.).

institucija siekia gauti informacijos apie konkrečios bylos statusą, kad atliktų savo tyrimą, FPK, atsižvelgdama į nagrinėjamų bylų skaičių ir laikydamasi konfidencialumo ir kitų teisinių reikalavimų, teiks tokiai institucijai prašomą informaciją.

FPK taip pat glaudžiai dirbs su ES DAI, kad suteiktų vykdymo pagalbą. Atitinkamais atvejais tai galėtų reikšti dalijimąsi informacija ir tyrimo pagalba pagal JAV saugaus tinklo aktą, kuriuo FPK leidžiama teikti pagalbą užsienio teisėsaugos institucijoms, kurios vykdo įstatymus, kuriais draudžiama praktika, kuri iš esmės yra panaši į praktiką, kuri draudžiama FPK vykdomais įstatymais ⁽¹⁾. Teikdama šią paramą, FPK gali dalytis informacija, kurią gavo atlikdama FPK tyrimą, ESA DAI, atliekančios savo tyrimą, vardu priimti procesinius dokumentus ir siekti gauti žodinį patvirtinimą iš liudytojų arba atsakovo DAI vykdymo byloje, laikydamasi JAV saugaus tinklo akto. FPK reguliariai naudojami šiais įgaliojimais, kad padėtų kitoms institucijoms nagrinėti privatumo ir vartotojų apsaugos bylas ⁽²⁾.

FPK ne tik prioritetine tvarka nagrinėja ES valstybių narių ir privatumo savireguliacijos organizacijų perduotas „privatumo skydo“ bylas ⁽³⁾, bet ir išipareigoja savo iniciatyva tirti galimus sistemos pažeidimus, kai tinkama, naudodama įvairias priemones.

Jau gerą dešimtmetį FPK įgyvendina griežtą privatumo ir saugumo klausimų tyrimo programą, kurioje taip pat dalyvauja komercinės organizacijos. Atlikdama šiuos tyrimus, FPK paprastai nagrinėjo, ar atitinkamas subjektas teikė pareiškimus dėl „saugaus uosto“. Jeigu subjektas teikė tokius pareiškimus ir tyrimo metu buvo nustatyti aiškūs „saugaus uosto“ privatumo principų pažeidimai, FPK visus kaltinimus pažeidus „saugumo uosto“ nuostatas įtraukė į savo vykdymo bylas. Šio aktyvaus veikimo būdo laikysimės ir pagal naująją sistemą. Svarbu, kad FPK atlieka daug daugiau tyrimų, kuriuos baigus galiausiai pradedamos vykdymo bylos. Dauguma FPK tyrimų baigiami darbuotojams nenustačius akivaizdaus pažeidimo. Kadangi FPK tyrimai yra nevieši ir konfidencialūs, dažnai apie baigtą tyrimą viešai nepranešama.

Beveik 40 FPK pradėtų vykdymo bylų, susijusių su „saugaus uosto“ programa, patvirtina agentūros išipareigojimą aktyviai įgyvendinti tarpvalstybines privatumo programas. FPK toliau tirs galimus sistemos pažeidimus atlikdama privatumo ir saugumo tyrimus, kurių imamės reguliariai.

III. KLAIDINGŲ ARBA APGAULINGŲ PAREIŠKIMŲ DĖL DALYVAVIMO „PRIVATUMO SKYDO“ SISTEMOJE ŠALINIMAS

Kaip nurodyta pirmiau, FPK imsis veiksmų dėl subjektų, kurie klaidingai praneša apie savo dalyvavimą sistemoje. FPK prioritetine tvarka nagrinės Komercijos departamento perduotas bylas dėl organizacijų, kurios, kaip nustatyta, klaidingai nurodo dalyvaujančios sistemoje arba be leidimo naudoja bet kokią sistemos sertifikavimo ženklą.

Be to, atkreipiame dėmesį į tai, kad jeigu organizacijos privatumo politikoje nurodoma, jog ji laikosi „privatumo skydo“ principų, jos nesugebėjimas patvirtinti arba registruotis Komercijos departamente pats savaime nebus tinkama priežastis pateisinti FPK savo išipareigojimą pagal sistemą nesilaikymo.

⁽¹⁾ Tarptautinės prekybos administracijos Tarptautinės prekybos komercijos sekretoriaus Stefano M. Seligo raštas Komisijos narei, atsakingai už teisingumą, vartotojų reikalus ir lyčių lygybę, Vėrai Jourová (2016 m. vasario 23 d.).

⁽²⁾ Nustatydama, ar pasinaudoti JAV saugaus tinklo aktu suteikiamais įgaliojimais, FPK, be kita ko, nagrinėja: a) ar prašančioji agentūra sutiko teikti ar teiks abipusę pagalbą Komisijai; b) ar tenkinant prašymą būtų pažeistas Jungtinių Amerikos Valstijų viešasis interesas, ir c) ar prašančiosios agentūros tyrimas arba vykdymo byla yra susijusi su veiksmais arba praktika, kurie sukelia arba gali sukelti žalą dideliame skaičiu žmonių.“ JAV kodekso 15 antraštinės dalies 46 straipsnio j dalies 3 punktas. Šie įgaliojimai netaikomi konkurencijos įstatymų vykdymui.

⁽³⁾ Pavyzdžiui, 2012–2015 fiskaliniiais metais FPK pasinaudojo jai pagal JAV saugaus tinklo aktą suteiktais įgaliojimais, kad dalytųsi informacija atsakydama beveik į 60 prašymų, kuriuos pateikė užsienio agentūros, ir priėmė beveik 60 pilietinių tyrimo užklausų (lygiavėčių administraciniais tyrimais), kad padėtų atlikti 25 užsienio tyrimus.

IV. NUTARČIŲ VYKDYMO STEBĖSENA

FPK taip pat patvirtina savo išsipareigojimą stebėti, kaip vykdomos nutartys, kad būtų užtikrinta atitiktis „privatumo skydo“ sistemos reikalavimams.

Taikydami įvairias tinkamas draudžiamas priemones, kurias ateityje nustatysime FPK sistemos nutarčių forma, reikalausime, kad būtų laikomasi sistemos reikalavimų. Tai apima draudimą teikti klaidingus pareiškimus dėl sistemos ir kitų privatumo programų, kai tokie pareiškimai yra pagrindinės FPK bylos pagrindas.

FPK bylos dėl pradinės „saugumo uosto“ programos vykdymo yra ribojamojo pobūdžio. 36 bylose dėl klaidingų arba apgaulingų pareiškimų dėl „saugaus uosto“ sertifikavimo kiekviena nutartimi atsakovui buvo draudžiama klaidingai pareikšti apie dalyvavimą „saugiamo uoste“ arba bet kurioje kitoje privatumo arba saugumo programoje ir reikalaujama, kad bendrovė leistų FPK susipažinti su atitikties ataskaita. Bylose, susijusiose su „saugaus uosto“ privatumo principų pažeidimu, iš bendrovių buvo reikalaujama įgyvendinti išsamias privatumo programas, gauti metinį nepriklausomos trečiosios šalies programų vertinimą ir teikti jį FPK dvidešimt metų.

FPK administracinių nutarčių pažeidimas gali užtraukti piniginę baudą iki 16 000 JAV dolerių už vieną pažeidimą, arba 16 000 JAV dolerių už vieną dieną, jeigu pažeidimas tęsiasi ⁽¹⁾, o ši suma, jeigu pažeidimas susijęs su veiksmu, nuo kurių nukenčia daugybė vartotojų, gali siekti milijonus dolerių. Kiekvienoje nutartyje dėl draudimo yra nustatytos atsiskaitymo ir atitikties nuostatos. Subjektai, kuriems adresuota nutartis, konkretų skaičių metų turi saugoti dokumentus, kuriais įrodoma, kad jie laikėsi reikalavimų. Nutartys taip pat turi būti įteikiamos darbuotojams, atsakingiems už reikalavimų užtikrinimą.

Kaip ir visais kitais atvejais, FPK sistemiškai stebi, kaip laikomasi „saugaus uosto“ nutarčių. FPK rimtai žiūri į savo privatumo ir saugumo nutarčių vykdymą ir prireikus imasi jų vykdymo veiksmų. Pavyzdžiui, kaip nurodyta pirmiau, „Google“ sumokėjo 22,5 mln. JAV dolerių civilinę baudą, kad pašalintų visus pažeidimus, kuriuos padarė nesilaikydama FPK nutarties. Svarbu, kad FPK nutartimis toliau bus saugomi visi pasaulio vartotojai, kurie bendrauja su įmonėmis, o ne tik skundus pateikę vartotojai.

Galiausiai FPK toliau tvarkys internetinį bendrovių, dėl kurių buvo priimtos nutartys, susijusių su „saugaus uosto“ programa ir „privatumo skydo“ sistema, sąrašą ⁽²⁾. Be to, pagal „privatumo skydo“ principus dabar reikalaujama, kad bendrovės, dėl kurių FPK arba teismas priėmė nutartį dėl privatumo principų nesilaikymo, viešai paskelbtų visų FPK pateiktų atitikties arba vertinimo ataskaitų skirsnius, susijusius su sistema, ir tai padarytų laikydamosi konfidencialumo įstatymų ir taisyklių.

V. DARBAS SU ES DAI IR BENDRADARBIAVIMAS VYKDYMO SRITYJE

FPK pripažįsta svarbų ES DAI vaidmenį, kurį jos atlieka užtikrinamos atitiktį sistemos reikalavimams, ir skatina intensyvesnes konsultacijas ir bendradarbiavimą vykdymo srityje. Be įvairių konsultacijų, susijusių su DAI perduotų bylų klausimais, FPK išsipareigoja dalyvauti periodiniuose susitikimuose su paskirtais 29 straipsnio darbo grupės atstovais ir bendrais bruožais aptarti, kaip pagerinti bendradarbiavimą vykdymo srityje pagal sistemą. FPK kartu su Komercijos departamentu, Europos Komisija ir 29 straipsnio darbo grupės atstovais taip pat dalyvaus metinėje sistemos peržiūroje, kad aptartų jos įgyvendinimo klausimus.

FPK taip pat ragina sukurti priemonę, kuri paskatins bendradarbiavimą vykdymo srityje su ES DAI, taip pat kitomis privatumo užtikrinimo institucijomis visame pasaulyje. Visų pirma FPK kartu su vykdymo partneriais Europos Sąjungoje ir visame pasaulyje, praėjusiais metais Pasauliniame privatumo užtikrinimo tinkle (angl. *Global Privacy Enforcement Network*, GPEN) pradėjo naudoti perspėjimo sistemą, kad dalytųsi informacija apie tyrimus ir skatintų bendradarbiavimą vykdymo srityje. Ši GPEN perspėjimo priemonė galėtų būti ypač naudinga įgyvendinant „privatumo skydo“ sistemą. FPK ir ES DAI galėtų šią sistemą naudoti su „privatumo skydu“ susijusiems ir kitiems privatumo tyrimams koordinuoti, įskaitant jos naudojimą dalijantis informacija siekiant užtikrinti koordinuotą ir veiksmingesnę vartotojų apsaugą. Toliau

⁽¹⁾ Nors FPK nesprendžia individualių vartotojų skundų ir netarpininkauja juos nagrinėjant, ji patvirtina, kad pirmenybę teiks „privatumo skydo“ byloms, kurias perdavė ES DAI. Be to, FPK naudoja skundus savo vartotojų apsaugos duomenų bazėje, kuri yra prieinama daugumai kitų teisėsaugos institucijų, kad nustatytų tendencijas, vykdymo prioritetus ir galimus tyrimo tikslus. ES piliečiai gali naudotis ta pačia skundų sistema, kuri yra prieinama JAV piliečiams, kad pateiktų skundą FPK (www.ftc.gov/complaint). Tačiau individualius su „privatumo skydu“ susijusius skundus ES piliečiams gali būti naudingiausia pateikti savo valstybės narės DAI arba alternatyvaus ginčo sprendimo paslaugų teikėjui.

⁽²⁾ JAV kodekso 15 antraštinės dalies 45 straipsnio m dalis; 16 C.F.R. § 1.98.

stengsimės dirbti su dalyvaujančiomis ES institucijomis, kad diegtume GPEN perspėjimo sistemą platesniu mastu ir kurtume kitas priemones, kad gerintume bendradarbiavimą vykdymo srityje, kiek jis susijęs su privatumo bylomis, įskaitant su sistema susijusias bylas.

FPK su malonumu patvirtina savo išipareigojimą įgyvendinti naują „privatumo skydo“ sistemą. Taip pat ketiname toliau bendradarbiauti su savo ES kolegomis, kad užtikrintume vartotojų privatumą abiejose Atlanto pusėse.

Pagarbiai

Edith Ramirez,

pirmininkė

A priedas

ES ir JAV „privatumo skydas“: JAV privatumo ir saugumo sistemos apžvalga

ES ir JAV „privatumo skydo“ sistemoje (toliau – sistema) nustatytos apsaugos priemonės galioja kartu su kitomis pagal JAV teisės sistemą taikomomis privatumo apsaugos priemonėmis. Visų pirma Federalinė prekybos komisija (toliau – FPK) yra nustačiusi išsamią privatumo ir duomenų saugumo programą, taikomą JAV prekybos veiklai, kuria užtikrinama viso pasaulio vartotojų apsauga. Antra, vartotojų privatumo ir saugumo užtikrinimas Jungtinėse Amerikos Valstijose gerokai patobulėjo nuo 2000 m., kai buvo patvirtinta ES ir JAV „saugaus uosto“ programa. Nuo to laiko federaliniu ir valstybių lygmenimis priimta nemažai privatumą ir saugumą reglamentuojančių įstatymų ir iš esmės padidėjo valstybinių ir privačių bylų, susijusių su teisių į privatumą užtikrinimu. Įvairios JAV teisinės vartotojų privatumo ir saugumo užtikrinimo priemonės, kurios taikomos duomenų tvarkymo komerciniais tikslais veiklai, papildė naujoje sistemoje nustatytas ES gyventojų apsaugos priemones.

I. FPK BENDROJI PRIVATUMO IR SAUGUMO UŽTIKRINIMO PROGRAMA

FPK yra pagrindinė JAV vartotojų apsaugos agentūra, kurios veikla orientuota į privatumą prekybos sektoriuje. FPK turi įgaliojimus vykdyti nesąžiningų ir apgaulingų veiksmų ar praktikos, kuria pažeidžiamas vartotojų privatumas, baudžiamąjį persekiojimą, taip pat įgyvendinti konkretesnius įstatymus, kuriais užtikrinama tam tikra finansinė informacija ir informacija apie sveikatą ir vaikus, ir informacija, kuri naudojama priimant tam tikrus sprendimus dėl vartotojų atitikties nustatytoms sąlygoms.

FPK patirtis vartotojų apsaugos užtikrinimo srityje yra beprecedentė. FPK vykdymo ieškiniai padėjo panaikinti neteisėtą praktiką fiziniame pasaulyje ir elektroninėje erdvėje. Pavyzdžiui, FPK pareiškė vykdymo ieškinius gerai žinomoms bendrovėms, pvz., „Google“, „Facebook“, „Twitter“, „Microsoft“, „Wyndham“, „Oracle“, „HTC“ ir „Snapchat“, taip pat mažiau žinomoms bendrovėms. FPK iškėlė bylas įmonėms, kurios tariamai siuntinėjo vartotojams brukalus, diegė vartotojų programose šnipinėjimo programas, nesugebėjo apsaugoti vartotojų asmeninės informacijos, apgaulingai sekė vartotojus internete, pažeidė vaikų privatumą, neteisėtai rinko informaciją apie vartotojų mobiliuosius prietaisus ir nesugebėjo užtikrinti prie interneto prijungtų prietaisų, kuriuose saugojama asmeninė informacija, saugumo. Priimtose nutartyse paprastai buvo nustatoma, kad FPK turi vykdyti nuolatinę priežiūrą dvidešimt metų, draudimas toliau pažeidinėti įstatymus ir didelės finansinės baudos, kurios įmonėms gali būti skiriamos už nutarties nesilaikymą⁽¹⁾. Svarbu tai, kad FPK nutartimis ne tik apsaugomi asmenys, kurie galėjo pranešti apie problemą, jais, tiesą sakant, apsaugomi visi vartotojai, kurie ateityje gali turėti reikalų su tokiais įmonėmis. Tarpvalstybiniu lygmeniu FPK jurisdikcija apima viso pasaulio vartotojų apsaugą nuo Jungtinėse Amerikos Valstijose taikomos praktikos⁽²⁾.

Iki šiol FPK iškėlė daugiau nei 130 brukalų ir šnipinėjimo bylų, daugiau nei 120 „Do Not Call“ telemarketingo bylų, daugiau nei 100 su Sąžiningo kreditinių ataskaitų sudarymo aktu susijusių bylų, beveik 60 duomenų saugumo bylų, daugiau nei 50 bendro pobūdžio privatumo bylų, beveik 30 bylų dėl *Gramm-Leach-Bliley* akto pažeidimų ir daugiau nei 20 bylų, kuriomis užtikrinamas Vaikų privatumo internete akto (COPPA) vykdymas⁽³⁾. Be šių bylų FPK taip pat parengė ir paskelbė įspėjamuosius raštus⁽⁴⁾.

⁽¹⁾ Kiekvienam FPK nutarties nesilaikančiam subjektui gali būti skiriama iki 16 000 JAV dolerių civilinė bauda už kiekvieną pažeidimą arba 16 000 JAV dolerių už dieną, jeigu pažeidimas yra tęstinio pobūdžio. Žr. JAV kodekso 15 antraštinės dalies 45 straipsnio l dalį; 16 CFR 1.98 dalies c punktą).

⁽²⁾ Kongresas aiškiai patvirtino FPK įgaliojimus siekti apginti teises, įskaitant restituciją, dėl kiekvieno su užsienio prekyba susijusio veiksmo ar praktikos, kai toks veiksmas ar praktika 1) pagrįstai yra arba gali būti Jungtinėse Amerikos Valstijose patiriamos žalos priežastimi, arba 2) yra susijęs su esminiu elgesiu Jungtinėse Amerikos Valstijose. Žr. JAV kodekso 15 antraštinės dalies 45 straipsnio a dalies 4 punktą.

⁽³⁾ Kai kuriais atvejais Komisijos nagrinėjamos privatumo ir duomenų saugumo bylose teigiama, kad bendrovė vykdė apgaulingą ir nesąžiningą veiklą; kartais šios bylos taip pat yra susijusios su tariamu įvairių įstatymų pažeidimu, pvz., Sąžiningo kreditinių ataskaitų sudarymo aktu, *Gramm-Leach-Bliley* aktu ir COPPA.

⁽⁴⁾ Žr., pvz., FPK pranešimą spaudai, FPK išpėja vaikų programėlės kūrėją „Baby Bus“ dėl galimų COPPA pažeidimų (2014 m. gruodžio 22 d.), <https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa>; FPK pranešimą spaudai, FPK išpėja duomenų tarpininkus apie operacijas, susijusias su galimais privatumo pažeidimais (2013 m. gegužės 7 d.), <https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations>; FPK pranešimą spaudai, FPK išpėja duomenų tarpininkus, kurie teikia informaciją apie nuomininkų nuomos istoriją, kad jiems gali būti taikomas Sąžiningo kreditinių ataskaitų sudarymo aktas (2013 m. balandžio 3 d.), <https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may>.

Atsižvelgdama į ilgalaikę patirtį privatumo užtikrinimo srityje, FPK taip pat atliko reguliarią galimų „saugaus uosto“ programos pažeidimų stebėseną. Nuo to laiko, kai buvo patvirtinta „saugaus uosto“ programa, FPK savo iniciatyva ėmėsi įvairių tyrimų dėl „saugaus uosto“ atitikties reikalavimams ir JAV bendrovėms išskėlė 39 bylas dėl „saugaus uosto“ pažeidimų. Užtikrindama naujos sistemos įgyvendinimą, FPK toliau vadovausis į aktyvią veiklą orientuotu požiūriu.

II. FEDERALINĖS IR VALSTIJŲ VARTOTOJŲ PRIVATUMO APSAUGOS PRIEMONĖS

„Saugaus uosto“ užtikrinimo apžvalgoje, pridedamoje prie Europos Komisijos sprendimo dėl „saugaus uosto“ tinkamumo, pateikiama įvairių federalinių ir valstijų įstatymų, kurie galiojo 2000 m. priėmus „saugaus uosto“ programą, santrauka⁽¹⁾. Tuo metu įvairiais federaliniais įstatymais buvo reglamentuojamas komercinis asmeninės informacijos, nurodytos ne tik FPK akto 5 straipsnyje, rinkimas ir naudojimas, įskaitant: Kabeliais perduodamų ryšių aktą, Vairuotojų privatumo apsaugos aktą, Elektroninių ryšių privatumo aktą, Elektroninio lėšų pervedimo aktą, Sąžiningo kreditinių ataskaitų sudarymo aktą, *Gramm-Leach-Bliley* aktą, Teisės į finansinį privatumą aktą, Telefono vartotojų apsaugos aktą ir Vaizdo privatumo aktą. Daugumoje valstybių šiose srityse taip pat galioja analogiški įstatymai.

Nuo 2000 m. federaliniu ir valstijų lygmeniu įvyko nemažai pokyčių, dėl kurių atsirado papildomų vartotojų privatumo apsaugos priemonių⁽²⁾. Pavyzdžiui, federaliniu lygmeniu FPK 2013 m. iš dalies pakeitė COPPA nuostatas ir numatė įvairias papildomas vaikų asmeninės informacijos apsaugos priemones. FPK taip pat priėmė dvi taisykles, kuriomis įgyvendinamas *Gramm-Leach-Bliley* aktas – taisyklę dėl privatumo ir taisyklę dėl apsaugos priemonių, – pagal kurias reikalaujama, kad finansų įstaigos⁽³⁾ atskleistų savo dalijimosi informacija praktiką ir įgyvendintų visapusišką informacijos saugumo programą, kad apsaugotų informaciją apie vartotojus⁽⁴⁾. Be to, 2003 m. priimtas Sąžiningo kreditinių ataskaitų sudarymo aktu (FACTA) papildomi daug anksčiau priimti JAV kredito įstatymai ir nustatomi reikalavimai, susiję su tam tikrų konfidencialių duomenų nuasmeninimu, dalijimusi ir tvarkymu. FPK paskelbė nemažai pagal FACTA priimtų taisyklių, be kita ko, susijusių su vartotojų teise nemokamai gauti metinę kredito ataskaitą; vartotojų ataskaitose pateikiamos informacijos saugiu tvarkymu; vartotojų teise atsisakyti gauti tam tikrus kredito ir draudimo pasiūlymus; vartotojų teise nesutikti, kad susijusios įmonės pateikta informacija nebūtų naudojama prekiaujant šios įmonės prekėmis ir paslaugomis, ir finansų įstaigoms ir kreditoriams taikomais reikalavimais įgyvendinti tapatybės vagystės nustatymo ir prevencijos programas⁽⁵⁾. Be to, 2013 m. peržiūrėjus kartu su Sveikatos draudimo ir atskaitomybės aktu paskelbtas taisykles, buvo nustatytos papildomos apsaugos priemonės, kurių paskirtis – apsaugoti informacijos apie asmens sveikatą privatumą ir saugumą⁽⁶⁾. Tai pat pradėtos taikyti vartotojų apsaugos nuo nepageidaujamų telemarketingo skambučių, automatizuotų skambučių ir brukalų priemonės. Kongresas taip pat priėmė įstatymus, kuriuose reikalaujama, kad tam tikros informaciją apie sveikatą renkančios bendrovės informuotų vartotojus apie pažeidimą⁽⁷⁾.

Valstijos taip pat labai aktyviai priiminėjo su privatumu ir saugumu susijusius įstatymus. Nuo 2000 m. keturiasdešimt septynios valstijos, Kolumbijos apygarda, Guamas, Puerto Rikas ir Mergelių salos priėmė įstatymus, kuriuose

⁽¹⁾ Žr. JAV komercijos departamento parengtą „Saugaus uosto“ vykdymo užtikrinimo apžvalgą (https://build.export.gov/main/safeharbor/eu/eg_main_018476).

⁽²⁾ Dėl išsamesnės Jungtinėse Amerikos Valstijose galiojančių teisinių apsaugos priemonių apžvalgos žr. Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (5-asis leidimas, 2015).

⁽³⁾ Pagal *Gramm-Leach-Bliley* aktą finansų įstaigos apibrėžiamos labai plačiai, kad apimtų visas įmones, kurios „vykdo aktyvią veiklą“ siūlydamos finansinius produktus ar paslaugas. Tai, pvz., apima čekių išgryninančias įmones, dienos trukmės paskolų teikėjus, hipotekos tarpininkus, nebankinius paskolų teikėjus, asmeninio turto arba nekilnojamojo turto vertintojus ir profesionalius mokesčių konsultantus.

⁽⁴⁾ Pagal 2010 m. Vartotojų finansinės apsaugos aktą (CFPA) (oficialiojo leidinio Nr. 111–203, 124 Stat. 1955, X antraštinė dalis (2010 m. liepos 21 d.) (taip pat vadinamas Dodd-Frank Wall Street reformų ir vartotojų apsaugos aktu) dauguma FPK *Gramm-Leach-Bliley* akte nustatytų įgaliojimų priimti taisykles buvo perduota Vartotojų finansinės apsaugos biurui (CFPB). FPK išlaiko vykdymo užtikrinimo įgaliojimus pagal *Gramm-Leach-Bliley* aktą, taip pat įgaliojimus priimti nuostatas dėl apsaugos priemonių taisyklės ir ribotus įgaliojimus priimti taisykles pagal privatumo taisyklės, dėl prekiautojų automobiliams.

⁽⁵⁾ Pagal CFPA Komisija savo FCRA vykdymo užtikrinimo įgaliojimais dalijasi su CFPB, tačiau įgaliojimai priimti taisykles iš esmės perduoti CFPB (išskyrus „raudonas vėliavėles“ ir duomenų tvarkymo taisykles).

⁽⁶⁾ Žr. 45 C.F.R. 160, 162 ir 164 punktus.

⁽⁷⁾ Žr., pvz., 2009 m. Amerikos ekonomikos atgaivinimo ir naujų investicijų aktą, oficialusis leidinys Nr. 111–5, 123 Stat. 115 (2009) ir susijusias taisykles, 45 C.F.R. 164.404–164.414 straipsniai; 16 C.F.R. 318 punktus.

reikalaujama, kad įmonės informuotų asmenis apie su asmenine informacija susijusius saugumo pažeidimus ⁽¹⁾. Ne mažiau kaip trisdešimt trys valstijos ir Puerto Rikas yra priėmusios duomenų tvarkymo įstatymus, kuriuose nustatyti asmeninės informacijos sunaikinimo ar tvarkymo reikalavimai ⁽²⁾. Dauguma valstijų taip pat priėmė bendruosius duomenų saugumo įstatymus. Be to, Kalifornijoje priimti įvairūs privatumo įstatymai, įskaitant įstatymą, kuriuo reikalaujama, kad bendrovės turėtų parengtą privatumo politiką ir atskleistų savo nesekimo (angl. *Do Not Track*) praktiką ⁽³⁾, *Shine the Light* įstatymas, kuriame reikalaujama užtikrinti skaidresnę duomenų tarpininkų veiklą ⁽⁴⁾, ir įstatymas, kuriuo sukuriamas „informacijos trynimo mygtukas“, leidžiantis nepilnamečiams prašyti, kad būtų ištrinta tam tikra su jais susijusi socialiniuose portaluose esanti informacija ⁽⁵⁾. Taikydamos šiuos įstatymus ir naudodamosi kitais įgaliojimais, federalinės ir valstijų Vyriausybės skyrė dideles baudas bendrovėms, kurios nesugebėjo užtikrinti vartotojų asmeninės informacijos privatumo ir saugumo ⁽⁶⁾.

Išnagrinėjus privatinės teisės bylas, taip pat priimta teigiamų rezultatų davusių teismo sprendimų ir sudaryta taikos sutarčių, kuriose nustatytos papildomos vartotojų privatumo ir duomenų saugumo apsaugos priemonės. Pavyzdžiui, 2015 m. bendrovė „Target“ sutiko sumokėti 10 mln. JAV dolerių kaip kompensaciją vartotojams, kurie teigė, kad jų asmeninei finansinei informacijai kilo pavojus dėl visuotinai paplitusių duomenų pažeidimo. 2013 m. bendrovė „AOL“ sutiko sumokėti 5 mln. JAV dolerių kompensacijos, kad patenkintų kolektyvinį ieškinį dėl tariamo netinkamo identifikavimo, susijusio su šimtų tūkstančių AOL narių paieškų užklausų atskleidimu. Be to, federalinis teismas patvirtino 9 mln. JAV dolerių išmoką, kurią bendrovė „Netflix“ sumokėjo už tariamą nuomos istorijos įrašų saugojimą, kuriuo buvo pažeistas 1988 m. Vaizdo privatumo apsaugos aktas. Kalifornijos federaliniai teismai patvirtino dvi atskiras taikos sutartis su „Facebook“ – vieną dėl 20 mln. JAV dolerių, o kitą dėl 9,5 mln. JAV dolerių, – susijusias su tuo, kad bendrovė rinko, naudojo ir dalijosi savo naudotojų asmenine informacija. Be to, 2008 m. Kalifornijos valstijos teismas patvirtino 20 mln. JAV dolerių vertės taikos sutartį su bendrove „Lens Crafters“ dėl neteisėto vartotojų sveikatos informacijos atskleidimo.

Apibendrinant galima teigti, kad, kaip matyti iš šios santraukos, Jungtinėse Amerikos Valstijose užtikrinama patikima teisinė vartotojų privatumo ir saugumo apsauga. Nauja „privatumo skydo“ sistema, kuria užtikrinamos svarbios ES gyventojų apsaugos priemonės, veiks atsižvelgiant į šį platesnį teisinės apsaugos kontekstą, kuriame vartotojų privatumo ir saugumo užtikrinimas yra svarbus prioritetas.

⁽¹⁾ Žr., pvz., Nacionalinę valstijų teisėkūros institucijų konferenciją (NCSL), *Valstijos saugumo pažeidimų pranešimo įstatymai* (2016 m. sausio 4 d.), skelbiama adresu <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

⁽²⁾ NCSL, *Data Disposal Laws* (2016 sausio 12 d.), skelbiama adresu <http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx>.

⁽³⁾ Cal. Verslo ir profesinio kodekso 22575–22579 straipsniai.

⁽⁴⁾ Cal. Civilinio kodekso 1798.80–1798.84 straipsniai.

⁽⁵⁾ Cal. Verslo ir profesinio kodekso 22580–22582 straipsniai.

⁽⁶⁾ Žr. Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, *Computer world* (2014 m. vasario 17 d.), skelbiama adresu <http://www.computerworld.com/s/article/9246393/jay-cline-u.s.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1>.

V PRIEDAS

JAV transporto sekretoriaus Anthony Foxxo raštas

2016 m. vasario 19 d.

Komisijos narei Verai Jourovái
Europos Komisija
Rue de la Loi/Wetstraat 200
1049 Briuselis
Belgija

Dėl ES ir JAV „privatumo skydo“ sistemos

Gerbiamą Komisijos narę V. Jourová,

Jungtinių Amerikos Valstijų transporto departamentas (toliau – Departamentas arba DOT) teigiamai vertina galimybę aprašyti savo vaidmenį užtikrinant ES ir JAV „privatumo skydo“ sistemos įgyvendinimą. Ši sistema atlieka esminį vaidmenį apsaugant asmens duomenis, kurie teikiami sudarant komercinius sandorius vis labiau globalėjančiame pasaulyje. Jis sudaro sąlygas įmonėms atlikti svarbias operacijas pasaulinėje ekonomikoje, kartu suteikiant ES vartotojams svarbias privatumo apsaugos priemones.

DOT pirmą kartą viešai išsipareigojo užtikrinti „saugaus uosto“ sistemą daugiau nei prieš 15 metų Europos Komisijai adresuotame rašte. Tame rašte DOT pažadėjo energingai užtikrinti „saugaus uosto“ privatumo principų laikymąsi. DOT toliau laikosi šio išsipareigojimo, o šiuo raštu dar kartą patvirtinamas anksčiau priimtas išsipareigojimas.

Be to, DOT atnauja savo išsipareigojimą šiose keturiose pagrindinėse srityse: 1) prioritetiniai tyrimai dėl tariamų „privatumo skydo“ pažeidimų; 2) tinkamos vykdymo bylos, iškeltos subjektams, kurie pateikia klaidingus arba apgaulingus pareiškimus dėl dalyvavimo „privatumo skydo“ sistemoje, ir 3) vykdymo nutarčių stebėseną ir „privatumo skydo“ principų pažeidimų viešinimas. Teikiame informaciją visose keturiose išsipareigojimų srityse ir pririnkus informuojame apie DOT vaidmenį saugant vartotojų privatumą ir užtikrinant „privatumo skydo“ sistemos veikimą.

I. APLINKYBĖS**A. DOT įgaliojimai privatumo srityje**

Departamentas tvirtai išsipareigojo užtikrinti informacijos, kurią vartotojai teikia oro vežėjams ir bilietų pardavėjams, apsaugą. DOT įgaliojimai imtis veiksmų šioje srityje yra nustatyti JAV kodekso 49 antraštinės dalies 41712 straipsnyje, kuriame vežėjui arba bilietų pardavėjui draudžiama užsiimti „nesąžininga arba apgaulinga veikla arba taikyti nesąžiningus konkurencijos metodus“ parduodant oro vežimo paslaugą, dėl kurios vartotojas, tikėtina, patirs žalą. 41712 straipsnis suformuluotas pagal Federalinės prekybos komisijos (FPK) akto 5 straipsnį (JAV kodekso 15 antraštinės dalies 45 straipsnis). Savo įstatymus, kuriais reglamentuojama nesąžininga ar apgaulinga veikla, aiškiname kaip draudžiančius oro vežėjui ar bilietų pardavėjui: 1) pažeisti savo privatumo politikos sąlygas arba 2) rinkti arba atskleisti informaciją tokiu būdu, kuriuo pažeidžiama viešoji politika, kuris prieštarauja moralei arba sukelia vartotojui didelę žalą, kurios negalima kompensuoti jokiomis kompensacinėmis priemonėmis. 41712 straipsnį taip pat aiškiname kaip draudžiantį vežėjams ir bilietų pardavėjams: i) pažeisti bet kokias Departamento priimtas taisykles, kuriose konkrečiai privatumo praktika įvardijama kaip nesąžininga arba apgaulinga, arba 2) pažeisti Vaikų privatumo apsaugos internete aktą (COPPA) arba FPK taisykles, kuriomis įgyvendinamas COPPA. Pagal federalinę teisę DOT turi išimtinis įgaliojimus reguliuoti oro vežėjų privatumo praktiką, be to, ji dalijasi jurisdikcija su FPK, kiek ji susijusi su bilietų pardavėjo privatumo praktika parduodant oro vežėjų teikiamas paslaugas.

Iš esmės, vežėjui arba oro vežėjo paslaugų pardavėjui viešai išsipareigojus taikyti „privatumo skydo“ sistemos principus, Departamentas gali naudotis 41712 straipsnyje nustatytais įgaliojimais, kad užtikrintų šių principų laikymąsi. Todėl, jeigu keleivis pateikia informaciją vežėjui arba bilietų pardavėjui, kuris išsipareigojo laikytis „privatumo skydo“ sistemos privatumo principų, kiekvienas atvejis, kai vežėjas arba bilietų pardavėjas nesilaikys šių principų, bus laikomas 41712 straipsnio pažeidimu.

B. Vykdyto praktika

Departamento Aviacijos užtikrinimo ir procedūrų biuras (Aviacijos reikalavimų užtikrinimo biuras) vykdo tyrimus ir baudžiamąjį persekiojimą pagal JAV kodekso 49 antraštinės dalies 41712 straipsnį. Jis užtikrina įstatymo 41712 straipsnyje nustatytą draudimą, susijusį su nesąžininga ir apgaulinga praktika, visų pirma derėdamasis, rengdamas veiksmų nutraukimo ir sustabdymo nutartis ir rengdamas nutartis dėl civilinių baudų skyrimo. Biuras apie galimus pažeidimus iš esmės sužino iš asmenų, kelionių agentų, oro vežėjų ir JAV bei užsienio Vyriausybių agentūrų gautų skundų. Vartotojai gali pasinaudoti DOT svetaine, kad pateiktų privatumo skundą dėl oro vežėjų ir bilietų pardavėjų ⁽¹⁾.

Jeigu byloje nepasiekiamas pagrįstas ir tinkamas susitarimas, Aviacijos reikalavimų užtikrinimo biuras turi įgaliojimus pradėti DOT administracinės teisės teisėjo (ALJ) nagrinėjamą vykdymo bylą, kurioje rengiamas įrodymų nagrinėjimo posėdis. ALJ turi įgaliojimus priimti sustabdymo ir nutraukimo nutartis ir skirti civilines baudas. Dėl 41712 straipsnio pažeidimų gali būti priimamos sustabdymo ir nutraukimo nutartys, o už kiekvieną 41712 straipsnio pažeidimą gali būti skiriamos iki 27 500 JAV dolerių civilinės baudos.

Departamentas neturi įgaliojimų priteisti nuostolių atlyginimą arba priimti sprendimą dėl piniginių kompensacijų išmokėjimo pavieniams pareiškėjams. Tačiau Departamentas turi įgaliojimus patvirtinti susitarimus, kurie sudaromi Aviacijos reikalavimų užtikrinimo biurui atlikus tyrimą, duoda tiesioginę naudą vartotojams (pvz., gryniesiems pinigais, kvitais) ir kuriais atlyginamos paprastai JAV Vyriausybei mokėtinos piniginės baudos. Tokios praktikos laikytasi praeityje ir jos taip pat gali būti laikomasi įgyvendinant „privatumo skydo“ sistemos principus, jei tai yra pateisinama atsižvelgiant į aplinkybes. Jeigu oro vežėjas nuolat pažeidinėja 41712 straipsnį, gali kilti klausimų dėl oro vežėjo pajėgumo laikytis reikalavimų, o tokiu atveju išimtinėmis aplinkybėmis gali būti pripažįstama, kad oro vežėjas nėra tinkamas toliau vykdyti veiklą, ir jis gali prarasti veiklos licenciją.

Iki šiol DOT gavo gana mažai skundų, kuriuose bilietų pardavėjai arba vežėjai kaltinami privatumo pažeidimais. Pateikti skundai tiriami pagal pirmiau nurodytus principus.

C. DOT užtikrinama ES vartotojų teisinė apsauga

Pagal 41712 straipsnį nesąžiningos arba apgaulingos veiklos draudimas oro vežimo arba oro vežimo paslaugų pardavimo srityje taikomas JAV ir užsienio vežėjams ir bilietų pardavėjams. DOT dažnai imasi veiksmų JAV ir užsienio oro vežėjų atžvilgiu, kai jų veikla daro poveikį užsienio ir JAV vartotojams, remdamiesi oro vežėjų praktika, kurios jie laikėsi teikdami vežimo į JAV ir iš JAV paslaugas. DOT naudoja ir toliau naudos visas prieinamas teisių gynimo priemones, kad apsaugotų užsienio ir JAV vartotojus nuo nesąžiningos arba apgaulingos praktikos oro vežimo srityje, kurią taiko reguliuojami subjektai.

Oro vežėjų atžvilgiu DOT taip pat vykdo kitus konkrečius įstatymus, kurių apsaugos priemonės taikomos ir ne JAV vartotojams, pvz., COPPA. Be to, COPPA reikalaujama, kad į vaikus orientuotų svetainių ir internetinių paslaugų arba visai auditorijai skirtų svetainių operatoriai, kaip žinoma, renka asmeninę informaciją iš 13 metų nesulaukusių vaikų, teiktų tėvams išpėjimą ir gautų patikrinamą tėvų sutikimą. JAV veikiančios svetainės ir paslaugos, kurioms taikoma COPPA ir kuriose renkama asmeninė informacija iš užsienio vaikų, privalo atitikti COPPA. Užsienyje veikiančios svetainės ir internetinės paslaugos taip pat privalo atitikti COPPA, jeigu jos yra orientuotos į Jungtinių Amerikos Valstijų vaikus arba jeigu jose, kaip žinoma, renkama asmeninė informacija iš Jungtinių Amerikos Valstijų vaikų. Tiek, kiek JAV arba užsienio oro vežėjai, kurie veikia Jungtinėse Amerikos Valstijose, pažeidžia COPPA, DOT turi jurisdikciją imtis vykdymo veiksmų.

II. „PRIVATUMO SKYDO“ UŽTIKRINIMAS

Jeigu oro vežėjas arba bilietų pardavėjas nusprendžia dalyvauti „privatumo skydo“ sistemoje, o Departamentas gauna skundą, kad toks oro vežėjas arba bilietų pardavėjas tariamai pažeidė sistemą, Departamentas imsis toliau nurodytų veiksmų, kad užtikrintų tinkamą sistemos veikimą.

⁽¹⁾ <http://www.transportation.gov/airconsumer/privacy-complaints>.

A. Tariamų pažeidimų tyrimas prioritetine tvarka

Departamento Aviacijos reikalavimų užtikrinimo biuras tirs kiekvieną skundą dėl tariamo „privatumo skydo“ pažeidimo (įskaitant iš ES duomenų apsaugos institucijų gautus skundus) ir, pasitvirtinus įrodymams dėl pažeidimo, imsis vykdymo veiksmų. Be to, Aviacijos reikalavimų užtikrinimo biuras bendradarbiaus su FPK ir Komercijos departamentu ir prioritetine tvarka nagrinės kaltinimus, kad reguliuojami subjektai nesilaiko privatumo įsipareigojimų, susijusių su dalyvavimu „privatumo skydo“ sistemoje.

Gavęs skundą dėl tariamo „privatumo skydo“ sistemos pažeidimo, Departamento Aviacijos reikalavimų užtikrinimo biuras gali imtis įvairių su atliekamu tyrimu susijusių veiksmų. Pavyzdžiui, jis gali peržiūrėti bilietų pardavėjo arba oro vežėjo privatumo politiką, gauti papildomą informaciją iš bilietų pardavėjo, oro vežėjo arba trečiųjų šalių, kreiptis į bylą perdavusią instituciją ir įvertinti, ar yra pažeidimo modelis arba daug nukentėjusių vartotojų. Be to, jis nustatys, ar nagrinėjamas klausimas patenka į Komercijos departamento ar FPK kompetencijos sritį, įvertins, ar būtų naudinga surengti vartotojų ir įmonių mokymo kursus, ir, kai tinkama, pradės vykdymo bylą.

Sužinojęs apie galimą „privatumo skydo“ pažeidimą, kurį padarė bilietų pardavėjai, Departamentas šiuo klausimu savo veiksmus koordinuos su FPK. Taip pat teiksime informaciją FPK ir Komercijos departamentui apie kiekvienos „privatumo skydo“ vykdymo bylos rezultatus.

B. Klaidingų arba apgaulingų pareiškimų dėl dalyvavimo „privatumo skydo“ sistemoje šalinimas

Departamentas toliau laikosi įsipareigojimo tirti „privatumo skydo“ pažeidimus, įskaitant klaidingus arba apgaulingus pareiškimus dėl dalyvavimo „privatumo skydo“ programoje. Prioritetine tvarka nagrinėsime Komercijos departamento perduotas bylas dėl organizacijų, kurios, Departamento manymu, netinkamai save laiko „privatumo skydo“ narėmis arba be leidimo naudoja „privatumo skydo“ sistemos sertifikavimo ženklą.

Be to, atkreipiame dėmesį į tai, kad, jeigu organizacijos privatumo politikoje įsipareigojama laikytis esminių „privatumo skydo“ principų, organizacijos nesiregistravimas arba pakartotinis nesiregistravimas Komercijos departamente pats savaime, tikėtina, nebus tinkama priežastis, dėl kurios DOT negalės užtikrinti jos įsipareigojimų vykdymo.

C. Vykdyto nutarčių dėl „privatumo skydo“ pažeidimų stebėsena ir viešas skelbimas

Departamento Aviacijos reikalavimų užtikrinimo biuras taip pat toliau įsipareigoja stebėti, kaip vykdomos nutartys, ir prireikus užtikrina atitiktį „privatumo skydo“ programai. Konkrečiau kalbant, jeigu Biuras priima nutartį, kurioje oro vežėjui arba bilietų pardavėjui liepiama sustabdyti ir nutraukti „privatumo skydo“ ir 41712 straipsnio pažeidimus, jis stebės, kaip subjektas laikosi šių nutartyje nustatytų sustabdymo ir nutraukimo nuostatų. Be to, Biuras užtikrins, kad „privatumo skydo“ bylose priimtos nutartys būtų skelbiamos internete.

Spręsdami „privatumo skydo“ klausimus, toliau stengsimės dirbti su savo federaliniais partneriais ir ES suinteresuotaisiais subjektais.

Tikiuosi, kad ši pateikta informacija bus naudinga. Jeigu turite kokių nors papildomų klausimų, prašom susisiekti su manimi.

Pagarbiai

Anthony R. Foxx

transporto sekretorius

VI PRIEDAS

**Generalinio advokato Roberto Litto raštas
Nacionalinės žvalgybos direktoriaus biuras**

2016 m. vasario 22 d.

Justinui S. Antonipillai,
JAV komercijos departamento
advokatui
1401 Constitution Ave., NW
Vašingtonas, DC 20230

Tedui Deanui,
Tarptautinės prekybos administracijos
sekretoriaus pavaduotojui
1401 Constitution Ave., NW
Vašingtonas, DC 20230

Gerbiami J. Antonipillai ir T. Deanai,

per pastaruosius pusantrų metų derėdamosi dėl ES ir JAV „privatumo skydo“ Jungtinės Amerikos Valstijos teikė esminę informaciją apie JAV žvalgybos bendruomenės signalų žvalgybos duomenų rinkimo veiklą. Per šias derybas buvo pateikta informacija apie reglamentuojančią teisinę sistemą, daugialypę šios veiklos priežiūrą, visapusišką šios veiklos skaidrumą ir bendras privatumo ir pilietinių laisvių apsaugos priemonės siekiant padėti Europos Komisijai nustatyti, ar šios apsaugos priemonės yra tinkamos, nes jos susijusios su „privatumo skydo“ principuose nustatyta nacionalinio saugumo išimtimi. Šiame dokumente apibendrinama pateiktoji informacija.

I. PPD-28 IR JAV SIGNALŲ ŽVALGYBOS VEIKLOS VYKDYMAS

JAV žvalgybos bendruomenė užsienio žvalgybos duomenis renka taikydama griežtas kontrolės priemones, griežtai laikydamosi JAV įstatymų ir taikydama daugialypę priežiūrą, kurioje daugiausia dėmesio skiriama svarbiems užsienio žvalgybos ir nacionalinio saugumo prioritetams. JAV signalų žvalgybos duomenų rinkimą reglamentuoja įvairūs įstatymai ir politika, įskaitant JAV Konstituciją, Užsienio žvalgybos stebėsenos aktą (JAV kodekso 50 antraštinės dalies 1801 ir kiti straipsniai) (FISA), Vykdomąjį įsaką 12333 ir jo įgyvendinimo procedūras, prezidento gaires ir įvairias FISA teismo ir generalinio advokato patvirtintas procedūras ir rekomendacijas, kuriose nustatytos papildomos taisyklės dėl užsienio žvalgybos informacijos rinkimo, saugojimo, naudojimo ir skleidimo ribojimo ⁽¹⁾.

a. PPD-28 apžvalga

Prezidentas B. Obama savo 2014 m. sausio mėn. pasakytoje kalboje bendrais bruožais apibūdino įvairias JAV signalų žvalgybos veiklos reformas ir paskelbė Prezidento politinę direktyvą Nr. 28 (PPD-28) dėl šios veiklos ⁽²⁾. Prezidentas pabrėžė, kad JAV signalų žvalgybos veikla padeda užtikrinti ne tik mūsų šalies ir laisvių apsaugą, bet ir kitų šalių saugumą ir laisves, įskaitant ES valstybes nares, besiremiančias informacija, kurią JAV žvalgybos agentūros gavo siekdamos apsaugoti savo piliečius.

PPD-28 nustatyti įvairūs principai ir reikalavimai, kurie taikomi visai JAV signalų žvalgybos veiklai ir visiems žmonėms, nepaisant jų pilietybės ar buvimo vietos. Visų pirma joje nustatyti tam tikri procedūriniai reikalavimai, susiję su asmeninės informacijos apie ne JAV asmenis, kuri buvo gauta pagal JAV signalų žvalgybą, rinkimu, saugojimu ir skleidimu. Šie reikalavimai išsamiau aptariami toliau, tačiau apibendrinant:

- PPD pakartojama, kad Jungtinės Amerikos Valstijos signalų žvalgybos duomenis renka tik įstatyme, vykdomajame įsake arba kitoje prezidento direktyvoje nustatytais atvejais.

⁽¹⁾ Daugiau informacijos apie JAV užsienio žvalgybos veiklą pateikiama internete per viešai prieinamą žvalgybos bendruomenės svetainę (www.icontherecord.tumblr.com), ODNI viešą svetainę, kurios paskirtis – didinti Vyriausybės žvalgybinės veiklos matomumą visuomenėje.

⁽²⁾ Skelbiama adresu <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

- PPD nustatytos procedūros, kuriomis siekiama užtikrinti, kad signalų žvalgybos veikla būtų vykdoma tik siekiant teisėtų ir leistinų nacionalinio saugumo tikslų.
- PPD taip pat reikalaujama, kad planuojant signalų žvalgybos duomenų veiklą būtų paisoma privatumo ir pilietinių laisvių. Visų pirma Jungtinės Amerikos Valstijos nerenka žvalgybos duomenų, kad nuslopintų kritiką arba kitokią nuomonę, siekdama pakenkti kitokios tautybės, rasės, lyties, lytinės orientacijos arba religijos asmenims arba suteikti JAV bendrovėms ir JAV verslo sektoriams konkurencinį pranašumą prekybos srityje.
- PPD nurodoma, kad signalų žvalgybos duomenų rinkimas turi būti kuo tikslingesnis ir kad masiškai renkami signalų žvalgybos duomenys gali būti naudojami tik konkrečiai nustatytais tikslais.
- PPD nustatyta, kad žvalgybos bendruomenės subjektai turi nustatyti procedūras „kuriomis būtų pagrįstai platinimas ir saugomas minimalus per signalų žvalgybą surinktos asmeninės informacijos kiekis“ ir visų pirma praplečiamas tam tikrų apsaugos priemonių, taikomų JAV asmenų asmeninės informacijos apsaugai, galiojimas ne JAV asmenų informacijai.
- Agentūros procedūros, kuriomis įgyvendinama PPD-28, yra patvirtintos ir paskelbtos viešai.

Šioje direktyvoje nustatytų procedūrų ir apsaugos priemonių taikymas „privatumo skydo“ sistemai yra aiškus. Kai duomenys Jungtinių Amerikos Valstijų korporacijoms perduodami pagal „privatumo skydą“ arba bet kuriomis priemonėmis, JAV žvalgybos agentūros gali gauti tuos duomenis iš šių korporacijų tik jeigu prašymas atitinka FISA arba pateikiamas pagal vieno iš nacionalinio saugumo rašto įstatymines nuostatas, kurios aptariamos toliau ⁽¹⁾. Be to, nepatvirtinant ar nepaneigiant žiniasklaidos pranešimų apie tai, kad JAV žvalgybos bendruomenė tariamai renka duomenis iš transatlantinių kabelių, kol jie perduodami į Jungtines Amerikos Valstijas, jeigu JAV žvalgybos bendruomenė turi rinkti duomenis iš transatlantinių kabelių, ji tai darytų taikydamą šiame rašte nustatytą apribojimų ir apsaugos priemonių, įskaitant PPD-28, reikalavimus.

b. Duomenų rinkimo apribojimai

PPD-28 nustatyti įvairūs svarbūs bendrieji principai, kuriais reglamentuojamas signalų žvalgybos duomenų rinkimas.

- Signalų žvalgybos duomenų rinkimas turi būti pagrįstas įstatymu arba prezidento leidimu, be to, tokie duomenys turi būti renkami laikantis Konstitucijos ir teisės.
- Privatumas ir pilietinės laisvės turi būti esminiai aspektai, į kuriuos atsižvelgiama planuojant signalų žvalgybos veiklą.
- Signalų žvalgybos duomenys bus renkami tik esant pagrįstam užsienio žvalgybos arba kontržvalgybos tikslui.
- Jungtinės Amerikos Valstijos nerinks signalų žvalgybos duomenų siekdamas nuslopinti kritiką arba kitokią nuomonę.
- Jungtinės Amerikos Valstijos nerinks signalų žvalgybos duomenų, kad pakenktų kitokios tautybės, rasės, lyties, lytinės orientacijos arba religijos asmenims.
- Jungtinės Amerikos Valstijos nerinks signalų žvalgybos duomenų, kad suteiktų JAV bendrovėms ir verslo sektoriams konkurencinį pranašumą prekybos srityje.
- JAV signalų žvalgybos veikla *visada* turi būti kuo tikslingesnė, o ją vykdant turi būti atsižvelgiama į kitus prieinamus informacijos šaltinius. Tai, be kita ko, reiškia, kad, kai įmanoma, užuot masiškai rinkus signalų žvalgybos duomenis, vykdoma tikslinga signalų žvalgybos duomenų rinkimo veikla.

Reikalavimas, pagal kurį signalų žvalgybos veikla turi būti „kuo tikslingesnė“, taikomas signalų žvalgybos duomenų rinkimo būdui ir faktiškai renkamiems duomenims. Pavyzdžiui, nustatydamą, ar verta rinkti signalų žvalgybos duomenis, žvalgybos bendruomenė privalo išnagrinėti kitos informacijos prieinamumą, įskaitant diplomatinį ar viešą

⁽¹⁾ Jungtinių Amerikos Valstijų teisėsaugos arba reguliavimo institucijos, vadovaudamosi kitais baudžiamosios ar civilinės teisės ir reguliavimo įgaliojimais nacionalinio saugumo srityje, kurie neaptariami šiame dokumente, gali prašyti, kad korporacijos pateiktų jų tyrimams svarbią informaciją.

šaltinius, ir teikti pirmenybę duomenų rinkimui tokiomis priemonėmis, kai tai yra tinkama ir pagrįsta. Be to, žvalgybos bendruomenės subjektų politikoje turėtų būti reikalaujama, kad, jei įmanoma, renkant duomenis daugiausia dėmesio būtų skiriama konkretiems užsienio žvalgybos tikslams arba temoms ir būtų naudojami diskriminantai (pvz., konkretūs įrenginiai, atrankos sąlygos ir identifikatoriai).

Svarbu vertinti Komisijai pateiktos informacijos visumą. Sprendimai dėl to, kas yra „įmanoma“ ar „praktiška“, ne paliekami asmenų diskrečiai, bet priimami remiantis viešai paskelbta politika, kurią agentūros nustatė pagal PPD-28, ir kitais šioje direktyvoje aprašytais procesais ⁽¹⁾. Kaip nurodyta PPD-28, masinis signalų žvalgybos duomenų rinkimas yra rinkimas, kuris „dėl techninių arba veiklos aplinkybių, vykdomas nenaudojant diskriminantų (pvz., specialių identifikatorių, atrankos sąlygų ir pan.)“. Šiuo atžvilgiu PPD-28 pripažįstama, jog žvalgybos bendruomenės subjektai signalų žvalgybos duomenis privalo masiškai rinkti tam tikromis aplinkybėmis, kad nustatytų naujas arba kylančias grėsmes ir kitą gyvybiškai svarbią nacionalinio saugumo informaciją, kuri dažnai slepiama didelėje ir sudėtingoje šiuolaikinėje pasaulinių ryšių sistemoje. Joje taip pat pripažįstami su privatumu ir pilietinėmis laisvėmis susiję klausimai, kurie kyla masiškai renkant signalų žvalgybos duomenis. Todėl PPD-28 nurodoma, kad žvalgybos bendruomenė turi pirmenybę teikti alternatyvoms, kurios leistų atlikti tikslingą signalų žvalgybą, o ne masiškai rinkti signalų žvalgybos duomenis. Todėl žvalgybos bendruomenės subjektai, kai įmanoma, turėtų vykdyti tikslingą signalų žvalgybos duomenų rinkimo veiklą, o ne masiškai rinkti signalų žvalgybos duomenis ⁽²⁾. Šiais principais masinio duomenų rinkimo išimtis netaptų viršesnė už bendrąją taisyklę.

Kalbant apie „pagrįstumo“ koncepciją, pažymėtina, kad tai yra esminis JAV teisės principas. Jis reiškia, kad žvalgybos bendruomenės subjektai neturės nustatyti bet kokios teoriškai įmanomos priemonės, tačiau turės suderinti savo veiksmus su praktiniais signalų žvalgybos veiklos poreikiais, kad apsaugotų teisėtus su privatumu ir pilietinėmis laisvėmis susijusius interesus. Šiuo atveju agentūros politika taip pat yra prieinama, ir joje gali būti pateikiamas patikinimas, kad formuluote „pagrįstai sukurta siekiant platinti ir saugoti kuo mažiau asmeninės informacijos“ nepažeidžiama pagrindinė taisyklė.

PPD-28 taip pat nustatyta, kad masiškai surinkti signalų žvalgybos duomenys gali būti naudojami tik šešiais konkrečiais tikslais: tam tikrai užsienio valstybių veiklai atskleisti ir jai nutraukti, kovai su terorizmu, kovai su ginklų platinimu, kibernetiniam saugumui užtikrinti, grėsmėms JAV arba sąjungininkų ginkluotosioms pajėgoms nustatyti ir pašalinti ir kovai su tarptautinėmis nusikalstamumo grėsmėmis, įskaitant sankcijų vengimą. Prezidento patarėjas nacionalinio saugumo klausimais, pasikonsultavęs su Nacionalinės žvalgybos direktoriumi (DNI), kasmet peržiūri šiuos leistinus masiškai surinkti signalų žvalgybos duomenų naudojimo tikslus, kad nustatytų, ar jų nereikėtų pakeisti. DNI, atsižvelgdamas į nacionalinio saugumo aspektus, šį sąrašą paskelbs viešai. Tai yra svarbus ir skaidrus masiškai surinktų signalų žvalgybos duomenų apribojimas.

Be to, PPD-28 įgyvendinantys žvalgybos bendruomenės subjektai sugriežtino galiojančią analizės praktiką ir standartus, susijusius su užklausa dėl neįvertintų signalų žvalgybos duomenų ⁽³⁾. Analitikai privalo struktūrizuoti savo užklausas arba kitas paieškos sąlygas ir būdus ir užtikrinti, kad jie būtų tinkami žvalgybos informacijai, susijusiai su teisėta užsienio žvalgybos arba teisėsaugos užduotimi, nustatyti. Šiuo atžvilgiu žvalgybos bendruomenės subjektai savo užklausas apie asmenis turi orientuoti į signalų žvalgybos informacijos kategorijas, atitinkančias užsienio žvalgybos arba teisėsaugos reikalavimą, kad būtų užkirstas kelias asmeninės informacijos, nesusijusios su užsienio žvalgybos arba teisėsaugos reikalavimais, naudojimui.

Svarbu pabrėžti, kad bet kokia masinio duomenų rinkimo veikla, susijusi su interneto ryšiais, kurią JAV žvalgybos bendruomenė vykdo pasitelkdama signalų žvalgybą, atliekama tik nedidelėje interneto dalyje. Be to, naudojant tikslingas užklausas, kaip aprašyta pirmiau, užtikrinama, kad analitikams būtų pateikti tik tie duomenys, kurie, kaip manoma, gali turėti žvalgybinę vertę. Šiais apribojimais siekiama apsaugoti visų asmenų privatumą ir pilietines laisves, nepaisant jų pilietybės ir gyvenamosios vietos.

⁽¹⁾ Skelbiama adresu www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Šiomis procedūromis šiame rašte aptartos tikslingumo ir pritaikymo koncepcijos įgyvendinamos atsižvelgiant į kiekvieną žvalgybos bendruomenės subjektą.

⁽²⁾ Vienas iš pavyzdžių: NSA procedūrose, kuriomis įgyvendinama PPD-28, nustatyta, kad „kai įmanoma, duomenys bus renkami naudojantis viena arba daugiau atrankos sąlygų, siekiant orientuotis į duomenų apie konkrečius užsienio žvalgybos objektus rinkimą (pvz., konkreči, žinoma tarptautinė teroristų arba teroristinė grupė) arba konkrečius užsienio žvalgybos klausimus (pvz., užsienio valstybės ar jos agentų platinami masinio naikinimo ginklai)“.

⁽³⁾ Skelbiama adresu http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Jungtinės Amerikos Valstijos nustatė procedūras, kad užtikrintų signalų žvalgybos veiklos vykdymą tik siekiant tinkamų nacionalinio saugumo tikslų. Kiekvienais metais prezidentas po išsamių ir oficialių tarpagentūrinių procedūrų nustato svarbiausius valstybės prioritetus užsienio žvalgybos duomenų rinkimo srityje. DNI turi pareigą šiuos žvalgybos prioritetus paversti Nacionalinės žvalgybos prioritetų sistema arba NIPF. PPD-28 sustiprinti ir patobulinti agentūrų sąveikos procedūras siekiant užtikrinti, kad visi žvalgybos bendruomenės prioritetai būtų peržiūrėti ir tvirtinami aukštu politiniu lygmeniu. Žvalgybos bendruomenės direktyvoje (ICD) Nr. 204 pateikiamos papildomos rekomendacijos dėl NIPF ir ji buvo atnaujinta 2015 m. sausio mėn., siekiant į ją įtraukti PPD-28 reikalavimus ⁽¹⁾. Nors NIPF yra išlaptintas, su konkrečiais JAV užsienio žvalgybos prioritetais susijusi informacija kasmet aptariama DNI išslaptintame *Pasauliniame grėsmių vertinime* (angl. *Worldwide Threat Assessment*), kuris taip pat skelbiamas ODNI svetainėje.

NIPF prioritetai yra gana abstraktūs. Jie apima tokias temas kaip branduolinių ir balistinių raketų pajėgumų stiprinimas konkrečiose priešiškos užsienio šalyse, narkotikų kartelio korupcijos padarinius ir piktnaudžiavimą žmogaus teisėmis konkrečiose šalyse. Prioritetai taikomi ne tik signalų žvalgybai, bet ir visai žvalgybos veiklai. Už NIPF prioritetų įgyvendinimą renkant faktinius signalų žvalgybos duomenis atsakinga organizacija vadinama Nacionaliniu signalų žvalgybos komitetu, arba SIGCOM. Jis yra pavaldus Nacionalinio saugumo agentūros (NSA) direktoriui, kuris pagal Vykdomąją įsaką 12333 skiriamas kaip „funkcinis signalų žvalgybos valdytojas“, atsakingas už signalų žvalgybos priežiūrą ir koordinavimą visoje žvalgybos bendruomenėje prižiūrint gynybos sekretoriui ir DNI. SIGCOM sudaro visų žvalgybos bendruomenės subjektų atstovai, ir, kadangi Jungtinės Amerikos Valstijos visiškai įgyvendina PPD-28, jame taip pat dalyvauja visų kitų departamentų ir agentūrų, politiškai suinteresuotų signalų žvalgyba, atstovai.

Visi JAV departamentai ir agentūros, kurios naudoja užsienio žvalgybos duomenis, prašymus dėl duomenų rinkimo teikia SIGCOM. SIGCOM išnagrinėja šiuos prašymus, užtikrina, kad jie atitinka NIPF, ir suteikia jiems prioritetus, vadovaudamasi toliau nurodytais kriterijais.

- Ar signalų žvalgyba šiuo atveju gali pateikti naudingos informacijos, o gal yra geresnių arba ekonomiškai veiksmingesnių informacijos atitinkamu klausimu šaltinių, pvz., vaizdų arba atvirojo šaltinio informacijos?
- Kaip skubiai ši informacija reikalinga? Jeigu tai yra svarbus NIPF prioritetas, dažniausiai tai bus svarbus signalų žvalgybos prioritetas.
- Kokios rūšies signalų žvalgybą būtų galima naudoti?
- Ar duomenų rinkimas yra pagrįstai tikslingas? Ar reikėtų taikyti laiko, geografinius arba kitus apribojimus?

Pagal JAV signalų žvalgybos reikalavimus taip pat reikia atidžiai išnagrinėti kitus aspektus, t. y.:

- Ar duomenų rinkimo objektas arba taikoma duomenų rinkimo metodika yra ypač konfidenciali? Jeigu taip, ši klausimą turi peržiūrėti vyresnieji politiką formuojantys pareigūnai.
- Ar dėl duomenų rinkimo privatumui ir pilietinėms laisvėms gali kilti nepateisinama rizika, nepaisant pilietybės?
- Ar būtina nustatyti papildomas duomenų platinimo ir saugojimo priemones, kad būtų apsaugoti privatumo arba nacionalinio saugumo interesai?

Galiausiai proceso pabaigoje apmokytas NSA personalas perima SIGCOM patvirtintus prioritetus ir išnagrinėja bei nustato konkrečias atrankos sąlygas, pvz., telefono numerius arba e. pašto adresus, kuriuos tikimasi panaudoti renkant šiuos prioritetus atitinkančią užsienio žvalgybos informaciją. Kiekvieną sekamą įrenginį reikia peržiūrėti ir patvirtinti prieš jį įtraukiant į NSA duomenų rinkimo sistemas. Tačiau net ir tuomet tai, ar faktinis duomenų rinkimas vyks ir kada,

⁽¹⁾ Skelbiama adresu <http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf>.

iš dalies priklausys nuo papildomų aplinkybių, pvz., atitinkamų duomenų rinkimo šaltinių prieinamumo. Šiuo procesu užtikrinama, kad JAV signalų žvalgybos duomenų rinkimo objektai atitiktų teisėtus ir svarbius užsienio žvalgybos poreikius. Žinoma, tais atvejais, kai duomenys renkami pagal FISA, NSA ir kitos agentūros privalo paisyti papildomų apribojimų, kuriuos patvirtino Užsienio žvalgybos stebėjimo teismas. Trumpai tariant, nei NSA, nei kuri nors kita JAV žvalgybos agentūra pati nenusprendžia, kokius duomenis rinkti.

Iš esmės šiuo procesu užtikrinama, kad visus JAV žvalgybos prioritetus nustatytų vyresnieji politikos pareigūnai, kurie geriausiai gali nustatyti JAV užsienio žvalgybos reikalavimus, ir kad šie politikos pareigūnai atsižvelgtų ne tik į potencialią renkamų žvalgybos duomenų vertę, bet ir į su tokia rinkimo veikla susijusią riziką, įskaitant riziką privatumui, nacionaliniams ekonominiais interesams ir užsienio santykiams.

Kalbant apie į Jungtines Amerikos Valstijas pagal „privatumo skydą“ perduotus duomenis, pažymėtina, kad nors Jungtinės Amerikos Valstijos negali patvirtinti arba paneigti konkrečių žvalgybos metodų arba operacijų, PPD-28 reikalavimai taikomi bet kurioms Jungtinių Amerikos Valstijų vykdomoms signalų žvalgybos operacijoms, nepaisant renkamų duomenų rūšies arba šaltinio. Be to, signalų žvalgybos duomenų rinkimui taikytini apribojimai ir apsaugos priemonės, taikomos signalų žvalgybos duomenims, surinktiems bet kuriuo kitu teisėtu tikslu, įskaitant užsienio santykius ir nacionalinio saugumo tikslus.

Iš pirmiau aptartų procedūrų matyti aiškus įsipareigojimas užkirsti kelią savavališkam ir masiškam signalų žvalgybos informacijos rinkimui ir aukščiausiu mūsų Vyriausybės lygmeniu įgyvendinti pagrįstumo principą. PPD-28 ir agentūros įgyvendinimo procedūrose paaiškinami nauji ir esami apribojimai, taikomi tikslui, kuriuo Jungtinės Amerikos Valstijos renka ir naudoja signalų žvalgybos duomenis, be to, šis tikslas aprašomas išsamiau. Šiose procedūrose turėtų būti įtvirtintas patikrinimas, kad signalų žvalgybos veikla yra ir toliau bus vykdoma tik siekiant teisėtų užsienio žvalgybos tikslų.

c. Duomenų saugojimo ir platinimo apribojimai

PPD-28 4 skirsnyje reikalaujama, kad kiekvienas žvalgybos bendruomenės subjektas turėtų nustatęs aiškas asmeninės informacijos apie ne JAV asmenis, surinktos naudojant signalų žvalgybą, saugojimo ir platinimo ribas, kurios būtų panašios į informacijai apie JAV asmenis taikomas ribas. Šios taisyklės yra įtrauktos į kiekvienos žvalgybos bendruomenės procedūras, kurios paskelbtos 2015 m. vasario mėn. ir yra viešai prieinamos. Kad asmeninė informacija atitiktų saugojimo arba platinimo užsienio žvalgybos tikslais sąlygas, ji turi būti susijusi su teisėtu žvalgybos reikalavimu, kaip nustatyta pirmiau aprašytame NIPF procese; turi būti pagrįstai manoma, kad bus gauta nusikaltimo įrodymų, arba įgyvendintas vienas iš kitų JAV asmens duomenų saugojimo standartų, nustatytų Vykdomojo įsako 12333 2.3 skirsnyje.

Informacija, dėl kurios nebuvo priimtas toks sprendimas, gali būti saugoma ne ilgiau nei penkerius metus, išskyrus atvejus, kai DNI aiškiai nustato, kad nuolatinis saugojimas atitinka Jungtinių Amerikos Valstijų nacionalinio saugumo interesus. Todėl žvalgybos bendruomenės subjektai privalo ne JAV asmenų informaciją, surinktą signalų žvalgybos metu, ištrinti praėjus penkeriems metams nuo surinkimo, išskyrus atvejus, kai, pvz., yra nustatyta, kad informacija yra svarbi vykdant nustatytą žvalgybos reikalavimą, arba jeigu DNI, atsižvelgęs į ODNI pilietinių laisvių apsaugos pareigūno ir agentūros privatumo ir pilietinių laisvių pareigūno nuomonę, nustato, kad nuolatinis saugojimas atitinka nacionalinio saugumo interesus.

Be to, visoje agentūros politikoje, kuria įgyvendinama PPD-28, dabar aiškiai reikalaujama, kad informacija apie asmenį nebūtų platinama vien todėl, kad jis nėra JAV asmuo, o ODNI priėmė visiems žvalgybos bendruomenės subjektams skirtą direktyvą⁽¹⁾, kurioje atsispindi šis reikalavimas. Aiškiai reikalaujama, kad žvalgybos bendruomenės personalas, rengdamas ir platindamas žvalgybos ataskaitas, atsižvelgtų į ne JAV asmenų privatumo interesus. Visų pirma signalų žvalgybos duomenys apie kasdienę užsienio asmens veiklą neturėtų būti laikomi užsienio žvalgybos duomenimis, kuriuos būtų galima platinti arba saugoti nuolat, atsižvelgiant vien į tą faktą, nebent kitu atveju juo tenkinamas teisėtas užsienio žvalgybos reikalavimas. Šia nuostata pripažįstamas svarbus apribojimas, kuris atitinka Europos Komisijos išreikštą susirūpinimą dėl užsienio žvalgybos sąvokos apibrėžties platumo, kaip nustatyta Vykdomajame įsake 12333.

⁽¹⁾ Žvalgybos bendruomenės direktyva (ICD) Nr. 203, skelbiama adresu <http://www.dni.gov/files/documents/ICD/ICD%202023%20Analytic%20Standards.pdf>.

d. Atitiktis ir priežiūra

JAV užsienio žvalgybos priežiūros sistemoje nustatyta efektyvi ir daugialypė priežiūra siekiant užtikrinti atitiktį taikytiniams įstatymams ir procedūroms, įskaitant su ne JAV asmens informacijos, gautos vykdant signalų žvalgybą, kaip nustatyta PPD-28, rinkimu, saugojimu ir platinimu susijusias procedūras. Tai apima:

- Šimtus žvalgybos bendruomenėje dirbančių priežiūros darbuotojų. Vien NSA dirba daugiau nei 300 žmonių, užtikrinančių reikalavimų laikymąsi, be to, kiti subjektai taip pat turi priežiūros biurus. Be to, Teisingumo departamentas vykdo plačią žvalgybos priežiūros veiklą ir ją taip pat vykdo Gynybos departamentas.
- Kiekvienas žvalgybos bendruomenės subjektas turi savo generalinio inspektoriaus biurą, kuris, be kitų pareigų, turi pareigą prižiūrėti užsienio žvalgybos veiklą. Generaliniai inspektoriai pagal įstatymą yra nepriklausomi; turi plačius įgaliojimus atlikti tyrimus, auditą ir peržiūrėti programas, įskaitant sukčiavimo ir piktnaudžiavimo arba teisės pažeidimo atvejų peržiūras, ir gali rekomenduoti imtis taisomųjų veiksmų. Nors generalinio inspektoriaus rekomendacijos nėra privalomos, jo ataskaitos dažnai skelbiamos viešai ir bet kuriuo atveju teikiamos Kongresui; tai pasakytina ir apie vėlesnes ataskaitas, jeigu dar neatlikti taisomieji veiksmai, kuriuos rekomenduota atlikti ankstesnėse ataskaitose. Todėl Kongresas yra informuojamas apie bet kokių reikalavimų nesilaikymo atvejį ir gali daryti spaudimą, įskaitant biudžetinį spaudimą, kad užtikrintų taisomųjų veiksmų vykdymą. Paskelbta nemažai generalinio inspektoriaus ataskaitų apie žvalgybos programas ⁽¹⁾.
- ODNI Pilietinių laisvių ir privatumo biuras (CLPO) turi pareigą užtikrinti žvalgybos bendruomenės veikimą tokiu būdu, kad būtų ginamas nacionalinis saugumas kartu apsaugant piliečių laisves ir privatumo teises. ⁽²⁾ Kiti žvalgybos bendruomenės subjektai turi savo atskirus privatumo pareigūnus.
- Privatumo ir pilietinių laisvių priežiūros valdyba (PCLOB) (nepriklausoma įstatymu įsteigta įstaiga) turi pareigą analizuoti ir peržiūrėti kovos su terorizmu programas ir politiką, įskaitant signalų žvalgybos naudojimą, kad užtikrintų tinkamą privatumo ir pilietinių laisvių apsaugą jomis. Ji priėmė keletą viešų žvalgybos veiklos ataskaitų.
- Kaip išsamiau aptarta toliau, Užsienio žvalgybos priežiūros teismas, kurį sudaro nepriklausomi federaliniai teisėjai, turi pareigą prižiūrėti visus pagal FISA vykdomus signalų žvalgybos duomenų rinkimo veiksmus ir laikytis jų.
- Galiausiai JAV Kongresas, t. y. Atstovų Rūmų ir Senato žvalgybos ir teismų komitetai, turi svarbias pareigas prižiūrėti visą JAV užsienio žvalgybos veiklą, įskaitant JAV signalų žvalgybą.

Be šių oficialių priežiūros mechanizmų, žvalgybos bendruomenė yra nustačiusi įvairius mechanizmus, kuriais užtikrina, kad žvalgybos bendruomenėje būtų laikomasi su pirmiau aprašytu duomenų rinkimu susijusių apribojimų. Pavyzdžiui:

- Kabineto pareigūnai turi kasmet patvirtinti savo signalų žvalgybos reikalavimus.
- NSA tikrina signalų žvalgybos taikinius taikydama duomenų rinkimo procedūrą, kad nustatytų, ar jie iš tikrųjų teikia vertingą užsienio žvalgybos informaciją, atitinkančią prioritetus, ir neberinks prioritetų neatitinkančių taikinių duomenų. Papildomomis procedūromis užtikrinama, kad atrankos sąlygos būtų periodiškai peržiūrimos.

⁽¹⁾ Žr., pvz., JAV teisingumo departamento generalinio inspektoriaus ataskaitą „A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008“ (2012 m. rugsėjo mėn.), skelbiama adresu <https://oig.justice.gov/reports/2016/o1601a.pdf>.

⁽²⁾ Žr. www.dni.gov/clpo.

- Remdamasis Prezidento B. Obamos sudarytos nepriklausomos peržiūros grupės rekomendacija, DNI sukūrė naują mechanizmą, kurio paskirtis – stebėti signalų žvalgybos duomenų, kurie dėl taikinio pobūdžio arba duomenų rinkimo būdų yra ypač konfidencialūs, siekiant užtikrinti, kad jie atitiktų politikos formuotojų sprendimus.
- Galiausiai ODNI kasmet peržiūri, kaip žvalgybos bendruomenė paskirsto išteklius NIPF prioritetams ir visai žvalgybos misijai. Per šią peržiūrą nustatoma visų renkamų žvalgybos duomenų vertė, įskaitant signalų žvalgybą, ir nagrinėjama, kaip žvalgybos bendruomenei pavyko pasiekti nustatytus tikslus. Ir ko žvalgybos bendruomenei reikės ateityje? Taip užtikrinama, kad signalų žvalgybos ištekliai būtų taikomi svarbiausiems nacionaliniams prioritetams.

Kaip matyti iš šios išsamios apžvalgos, žvalgybos bendruomenė savarankiškai nesprendžia, kokių pokalbių klausytis, nebando rinkti visos informacijos ar veikti be priežiūros. Jos veikla orientuota į politikos formuotojų nustatytus prioritetus, taikomas procesas, kurio metu savo indėlį įneša Vyriausybės įstaigos ir kuris yra prižiūrimas ir pačioje NSA, ir ODNI, Teisingumo departamento ir Gynybos departamento.

PPD-28 taip pat yra įvairių nuostatų, kuriomis užtikrinama, kad būtų apsaugota pagal signalų žvalgybą surinkta asmeninė informacija, nepaisant pilietybės. Pavyzdžiui, PPD-28 nustatytos duomenų saugumo, prieigos ir kokybės procedūros, kuriomis apsaugoma asmeninė informacija, surinkta renkant signalų žvalgybos duomenis, ir rengiami privalomi mokymai siekiant užtikrinti, kad darbuotojai suvoktų pareigą apsaugoti asmeninę informaciją, nepaisant pilietybės. PPD taip pat nustatyti papildomi priežiūros ir atitikties mechanizmai. Tai apima periodinį signalų žvalgybos metu surinktos asmeninės informacijos apsaugos praktikos auditą ir peržiūras, kurias atlieka atitinkami priežiūros ir atitikties pareigūnai. Peržiūrų metu taip pat turi būti nagrinėjama, kaip agentūros laikosi tokios informacijos apsaugos procedūrų.

Be to, PPD-28 nustatyta, kad svarbūs atitikties klausimai, susiję su ne JAV asmenimis, bus sprendžiami Vyriausybės vyresniųjų pareigūnų lygmeniu. Kilus svarbiam atitikties klausimui, susijusiam su bet kurio asmens asmenine informacija, surinkta vykdant signalų žvalgybos veiklą, apie jį nedelsiant turi būti pranešama DNI laikantis visų galiojančių pranešimo reikalavimų. Jeigu klausimas yra susijęs su ne JAV asmens asmenine informacija, DNI, pasikonsultavęs su valstybės sekretoriumi ir atitinkamo žvalgybos bendruomenės subjekto direktoriumi, nustatys, ar reikėtų imtis veiksmų, kad būtų informuota atitinkama užsienio Vyriausybė, kartu laikantis šaltinių, metodų ir JAV personalo apsaugos. Be to, kaip nurodyta PPD-28, valstybės sekretorius paskyrė vyresniąją pareigūnę, sekretorę Catherine Novelli, kuri veikia kaip užsienio Vyriausybių kontaktinis centras, sprendžiantis klausimus dėl Jungtinių Amerikos Valstijų vykdomos signalų žvalgybos veiklos. Šis aukšto lygmens išpareigojimas atspindi JAV Vyriausybės pastarųjų kelerių metų pastangas didinti pasitikėjimą įvairiomis ir iš dalies sutampančiomis privatumo apaugos priemonėmis, taikomomis JAV ir ne JAV asmenų informacijos apsaugai.

e. Santrauka

Jungtinių Amerikos Valstijų nustatytoje užsienio žvalgybos duomenų rinkimo, saugojimo ir platinimo procedūrose numatytos svarbios privatumo apsaugos priemonės, kurios taikomos visų asmenų, nepaisant jų pilietybės, asmeninei informacijai. Visų pirma šiomis procedūromis užtikrinama, kad mūsų žvalgybos bendruomenė daugiausia dėmesio skirtų savo nacionalinio saugumo misijai, kaip ji apibrėžta taikomuose įstatymuose, vykdomuosiuose įsakuose ir prezidento direktyvose, apsaugotų informaciją nuo neteisėtos prieigos, naudojimo ir atskleidimo ir vykdytų savo veiklą taikydama daugialypę peržiūrą ir priežiūrą, įskaitant Kongreso priežiūros komitetus. PPD-28 ir jį įgyvendinančiose procedūrose atsispindi mūsų pastangos plėsti tam tikrą minimalios informacijos ir kitų esminių duomenų apsaugos principų taikymo sritį, kad ji apimtų visų asmenų asmeninę informaciją, nepaisant jų pilietybės. Asmeninei informacijai, kuri buvo gauta renkant JAV signalų žvalgybos duomenis, taikomi JAV teisės ir prezidento direktyvų principai ir reikalavimai, įskaitant PPD-28 nustatytas apsaugos priemones. Šiais principais ir reikalavimais užtikrinama, kad su visais asmenimis būtų elgiamasi oriai ir pagarbiai, nepaisant jų pilietybės ar gyvenamosios vietos, ir pripažįstama, kad visi asmenys turi teisėtus privatumo interesus tvarkant jų asmeninę informaciją.

II. UŽSIENIO ŽVALGYBOS STEBĖJIMO AKTO 702 STRAIPSNIS

Duomenų rinkimas pagal Užsienio žvalgybos stebėjimo akto 702 straipsnį ⁽¹⁾ nėra „masinis ir be atrankos“, tačiau jis konkrečiai orientuotas į užsienio žvalgybos duomenų rinkimą iš individualių teisėtai nustatytų taikinių, aiškiai sankcionuotas remiantis aiškiais įstatyme nustatytais įgaliojimais ir gali būti nepriklausomos teisminės priežiūros ir esminės peržiūros ir priežiūros vykdomosios valdžios institucijose ir Kongrese dalyku. Duomenų rinkimas pagal 702 straipsnį laikomas signalų žvalgyba, kuriai taikomi PPD-28 reikalavimai ⁽²⁾.

Duomenų rinkimas pagal 702 straipsnį yra vienas vertingiausių žvalgybos duomenų, kuriais apsaugomos Jungtinės Amerikos Valstijos ir Europos partneriai, šaltinių. Išsami informacija apie 702 straipsnio veikimą ir priežiūrą yra vieša. Įvairios teismo bylos, teismo sprendimai ir priežiūros ataskaitos, susijusios su programa, buvo išslaptintos ir paskelbtos ODNI viešojoje informacijos atskleidimo svetainėje (www.icontherecord.tumblr.com). Be to, 702 straipsnį išsamiai išanalizavo PCLOB, o šios analizės ataskaita skelbiama adresu <https://www.pclob.gov/library/702-Report.pdf> ⁽³⁾.

702 straipsnis buvo nustatytas 2008 m., po išsamių viešų diskusijų priėmus FISA pakeitimų aktą ⁽⁴⁾. Šiuo straipsniu leidžiama įgyti užsienio žvalgybos informaciją stebint ne JAV piliečius, esančius ne Jungtinėse Amerikos Valstijose, įskaitant būtinąją JAV elektroninių ryšių paslaugų teikėjų pagalbą. 702 straipsnyje leidžiama generaliniam advokatui ir DNI – dviem kabinetinio lygio pareigūnams, kuriuos Senato pritarimu paskyrė prezidentas, – teikti FISA teismui metinius sertifikatus ⁽⁵⁾. Šiuose sertifikatuose nustatomos konkrečios užsienio žvalgybos duomenų, kurie bus renkami, kategorijos, pvz., su kova su terorizmu arba masinio naikinimo ginklais susiję žvalgybos duomenys, kurie turi patekti į užsienio žvalgybos duomenų, kaip jie apibrėžti FISA, kategorijas ⁽⁶⁾. Kaip pažymėjo PCLOB, „[š]iais apribojimais neleidžiama neribotai rinkti informacijos apie užsieniečius“ ⁽⁷⁾.

Į sertifikatus taip pat reikalaujama įtraukti „tikslingumo“ ir „minimalios informacijos“ procedūras, kurias turi peržiūrėti ir patvirtinti FISA teismas ⁽⁸⁾. Sekimo procedūrų paskirtis – užtikrinti, kad duomenys būtų renkami tik pagal įstatymą ir kaip nustatyta sertifikatuose; minimalios informacijos procedūrų paskirtis – riboti informacijos apie JAV asmenis įgijimą, platinimą ir saugojimą, tačiau jose taip pat yra nuostatų, kuriose numatyta esminė informacijos apie ne JAV asmenis apsauga, kaip aprašyta toliau. Be to, kaip aprašyta pirmiau, PPD-28 prezidentas nurodė, kad žvalgybos bendruomenė nustato papildomas asmeninės informacijos apie ne JAV asmenis apsaugos priemones, kurios taikomos pagal 702 straipsnį surinktai informacijai.

Teismui patvirtinus sekimo ir minimalios informacijos procedūras, duomenys pagal 702 straipsnį nerenkami masiškai ar be atrankos, tačiau renkami duomenys, kuriuos „sudaro vien konkrečių asmenų, dėl kurių buvo priimtas individualus sprendimas, sekimo metu gauta informacija“, kaip nustatyta PCLOB ⁽⁹⁾. Duomenys tikslingai renkami naudojant

⁽¹⁾ JAV kodekso 50 antraštinės dalies 1881a straipsnis.

⁽²⁾ Jungtinės Amerikos Valstijos taip pat gali gauti teismo nutarties pagal kitas FISA nuostatas, kad rinktų duomenis, įskaitant perduotuosius pagal „privatumo skydą“. Žr. JAV kodekso 50 antraštinės dalies 1801 ir kitus straipsnius. FISA I ir III antraštinėse dalyse, kuriose atitinkamai leidžiama vykdyti elektroninę stebėseną ir atlikti fizines kratas, reikalaujama teismo nutarties (išskyrus skubius atvejus) ir visada reikalaujama, kad būtų pagrįsta priežastis tikėti, kad taikiny yra užsienio valstybė arba užsienio valstybės agentas. Pagal FISA IV antraštinę dalį remiantis teismo nutartimi (išskyrus skubius atvejus) sankcionuotuose užsienio žvalgybos, kontržvalgybos ar kovos su terorizmu tyrimuose leidžiama naudoti renkamų numerių registratorių arba spąstų ir sekimo prietaisus. Pagal FISA V antraštinę dalį FTB teismo nutartimi (išskyrus skubius atvejus) leidžiama gauti įmonių įrašus, kurie yra susiję su sankcionuotais užsienio žvalgybos, kontržvalgybos ar kovos su terorizmu tyrimais. Kaip aptarta toliau, JAV laisvės akte konkrečiai draudžiama naudoti renkamų numerių registratorių arba įmonės įrašo nutarties siekiant masiškai rinkti duomenis ir nustatomas privalomas reikalavimas naudoti „konkrečią atrankos sąlygą“ ir taip užtikrinti, kad šiais įgaliojimais būtų naudojamasi tikslingai.

⁽³⁾ Privatumo ir pilietinių laisvių valdyba, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2014 m. liepos 2 d.) (PCLOB ataskaita).

⁽⁴⁾ Žr. oficialųjį leidinį Nr. 110–261, § 122, 129 Stat. 2436 (2008).

⁽⁵⁾ Žr. JAV kodekso 50 antraštinės dalies 1881a straipsnio a ir b dalis.

⁽⁶⁾ Žr. ten pat 1801 straipsnio e dalį.

⁽⁷⁾ Žr. PCLOB ataskaitos 99 punktą.

⁽⁸⁾ Žr. JAV kodekso 50 antraštinės dalies 1881 straipsnio a dalies d ir e punktus.

⁽⁹⁾ Žr. PCLOB ataskaitos 111 punktą.

individualius įrenginius, pvz., e. pašto adresus arba telefonų numerius, kurie, JAV žvalgybos personalo manymu, gali būti naudojami perduodant užsienio žvalgybos informaciją, kuriai taikomas teismui pateiktas sertifikatas ⁽¹⁾. Taikinio atrankos pagrindas turi būti dokumentuojamas, o kiekvieno sekamo įrenginio dokumentaciją vėliau peržiūri Teisingumo departamentas ⁽²⁾. JAV Vyriausybė atskleidė informaciją, iš kurios matyti, kad 2014 m. pagal 702 straipsnį buvo sekama apytiksliai 90 000 asmenų, – tai tik maža dalis, palyginti su daugiau nei 3 mlrd. interneto naudotojų visame pasaulyje ⁽³⁾.

Pagal 702 straipsnį surinktai informacijai taikomos teismo patvirtintos minimalios informacijos procedūros, kuriose nustatytos ne JAV asmenims ir JAV asmenims taikomos apsaugos priemonės; šios procedūros yra viešos ⁽⁴⁾. Pavyzdžiui, pagal 702 straipsnį perimti ryšiai – nesvarbu, ar jie yra JAV asmenų, ar ne JAV asmenų, – saugomi duomenų bazėse, kuriose prieiga suteikiama griežtomis sąlygomis. Juos gali peržiūrėti tik žvalgybos darbuotojai, kurie buvo apmokyti taikyti privatumo apsaugos ir minimalios informacijos procedūras ir kuriems suteikta konkreti prieiga prie ryšių duomenų, kad galėtų atlikti jiems pavestas funkcijas ⁽⁵⁾. Duomenų naudojimui taikomi apribojimai, susiję su užsienio žvalgybos informacijos arba nusikaltimo įrodymų nustatymu ⁽⁶⁾. Pagal PPD-28 ši informacija gali būti platinama tik jeigu yra pateisinamas užsienio žvalgybos arba teisėsaugos tikslas; vien tai, kad viena ryšių šalis nėra JAV asmuo, nėra pakankamas pagrindas rinkti informaciją ⁽⁷⁾. Minimalios informacijos procedūrose ir PPD-28 taip pat nustatyti pagal 702 straipsnį surinktų duomenų saugojimo terminai ⁽⁸⁾.

702 straipsnio priežiūra yra išsami ir ją atlieka trys mūsų vykdomosios valdžios šakos. Įstatymą įgyvendinančios agentūros taiko daugialypę vidaus peržiūrą, įskaitant nepriklausomų generalinių inspektorių atliekamą peržiūrą, ir technologinę prieigos prie duomenų kontrolę. Teisingumo departamentas ir ODNI atidžiai peržiūri ir stebi, kaip taikomas 702 straipsnis, kad patikrintų atitiktį teisinėms taisyklėms; agentūros taip pat turi nepriklausomą pareigą pranešti apie galimus reikalavimų nesilaikymo incidentus. Šie incidentai tiriami, o apie visus atitikties incidentus pranešama užsienio žvalgybos stebėsenos teismui. Prezidento žvalgybos priežiūros valdybai ir Kongresui, įskaitant, kai tinkama, tokių incidentų pasekmių šalinimą ⁽⁹⁾. Iki šiol nebuvo jokių incidentų, susijusių su sąmoningais bandymais pažeisti teisę arba apeiti teisinius reikalavimus ⁽¹⁰⁾.

FISA teismas atlieka svarbų vaidmenį įgyvendinant 702 straipsnį. Jį sudaro nepriklausomi federaliniai teisėjai, kurie pareigas FISA teisme eina septynerių metų kadenciją, tačiau, kaip ir visi federaliniai teisėjai, į teisėjo pareigas skiriami iki gyvos galvos. Kaip minėta, Teismas privalo peržiūrėti metinius sertifikatus ir sekimo bei minimalios informacijos procedūras ir patikrinti, ar jos atitinka įstatymą. Be to, kaip minėta, Vyriausybė turi nedelsdama informuoti Teismą apie atitikties klausimus ⁽¹¹⁾, o iš kelių Teismo išslaptintų ir atskleistų nuomonių matyti, kad, peržiūredamas šiuos incidentus, Teismas vadovaujasi ypač aukštais atidumo ir nepriklausomumo standartais.

Griežtas Teismo procedūras nustatė buvęs jo pirmininkas savo rašte Kongresui, kuris yra paskelbtas viešai ⁽¹²⁾. Todėl pagal toliau aprašytą JAV laisvės aktą Teismas dabar turi aiškius įgaliojimus paskirti išorės advokatą, kaip nepriklausomą advokatą, veikiantį privatumo bylose, kuriose sprendžiami nauji arba svarbūs teisiniai klausimai ⁽¹³⁾. Šis šalies nepriklausomo teisėjo dalyvavimo užsienio žvalgybos veikloje, nukreiptoje į asmenis, kurie nėra nei tos šalies piliečiai, nei joje gyvena, laipsnis yra neįprastas, gal net beprecedentis, ir padeda užtikrinti, kad duomenys pagal 702 straipsnį būtų renkami laikantis tinkamų teisinių ribų.

⁽¹⁾ Ten pat.

⁽²⁾ Ten pat, 8 punktas; JAV kodekso 50 antraštinės dalies 1881a straipsnio 1 dalis; taip pat žr. NSA pilietinių laisvių ir privatumo direktoriaus ataskaitos *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* (toliau – NSA ataskaita) 4 punktą, skelbiama adresu <http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties>.

⁽³⁾ Nacionalinės žvalgybos direktoriaus 2014 m. skaidrumo ataskaita, skelbiama adresu <http://icontherecord.tumblr.com/transparency/odni-transparencyreport-cy2014>.

⁽⁴⁾ Minimalios informacijos procedūras galima rasti: <http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf> (NSA minimalios informacijos procedūros); <http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf>; ir <http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf>.

⁽⁵⁾ Žr. NSA ataskaitos 4 punktą.

⁽⁶⁾ Žr., pvz., NSA minimalios informacijos procedūrų 6 punktą.

⁽⁷⁾ Žvalgybos agentūros PPD-28 procedūros skelbiamos adresu <http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties>.

⁽⁸⁾ Žr., pvz., NSA minimalios informacijos procedūras, PPD-28 4 skirsnį.

⁽⁹⁾ Žr. JAV kodekso 50 antraštinės dalies 1881 straipsnio 1 dalį, taip pat PCLOB ataskaitos 66–76 punktus.

⁽¹⁰⁾ Žr. atitikties procedūroms ir gairėms pagal Užsienio žvalgybos stebėsenos akto 702 straipsnį pusmečio vertinimo, kurį teikia generalinis direktorius ir Nacionalinės žvalgybos direktorius, 2–3 punktus, skelbiama adresu <http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf>.

⁽¹¹⁾ Užsienio žvalgybos stebėsenos teismo darbo tvarkos taisyklių 13 taisyklė, darbo tvarkos taisyklės skelbiamos adresu <http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf>.

⁽¹²⁾ 2013 m. liepos 29 d. Reggie B. Walton raštas Patrickui J. Leahy, skelbiamas adresu <http://fas.org/irp/news/2013/07/fisc-leahy.pdf>.

⁽¹³⁾ Žr. JAV laisvės akto 401 straipsnį oficialusis leidinys Nr. 114–23.

Kongresas priežiūrą vykdo rengdamas pagal įstatymą reikalaujamas ataskaitas ir teikdamas jas žvalgybos ir teismų komitetams, taip pat dažnai rengdamas trumpus informacinius susitikimus ir posėdžius. Tai apima generalinio advokato pusmečio ataskaitą apie 702 straipsnio taikymą ir visus atitikties incidentus ⁽¹⁾, atskirą generalinio advokato ir DNI pusmečio ataskaitą, kurioje dokumentuojama atitiktis sekimo ir minimalios informacijos procedūroms, įskaitant atitiktį procedūroms, kuriomis siekiama užtikrinti, kad duomenys būtų renkami teisėtu užsienio žvalgybos tikslu ⁽²⁾, ir žvalgybos subjektų direktorių metinę ataskaitą, kurioje patvirtinama, kad pagal 702 straipsnį renkamuose duomenyse toliau pateikiama užsienio žvalgybos informacija ⁽³⁾.

Trumpai tariant, duomenų rinkimas pagal 702 straipsnį leidžiamas įstatymu, tačiau tokiai duomenų rinkimo veiklai taikoma daugialypė peržiūra, teisminė priežiūra ir stebėseną ir, kaip nurodė FISA teismas neseniai priimtoje išslaptintoje nuomonėje, „duomenys renkami ne masiškai ir be atrankos“, bet „priimant <..> konkrečius sprendimus dėl asmeninės [ryšių] įrangos sekimo“ ⁽⁴⁾.

III. JAV LAISVĖS AKTAS

2015 m. birželio mėn. įsigaliojusi JAV laisvės aktu iš esmės pakeisti JAV stebėjimo ir kiti nacionalinio saugumo įgaliojimai ir padidintas skaidrumas dėl šių įgaliojimų naudojimo ir FISA teismo sprendimų, kaip nurodyta toliau ⁽⁵⁾. Aktu užtikrinama, kad mūsų žvalgybos ir teisėsaugos specialistams būtų suteikti įgaliojimai, kurių jiems reikia tautai apsaugoti, kartu užtikrinant, kad naudojantis šiais įgaliojimais būtų tinkamai apsaugotas asmenų privatumas. Juo sustiprinamas privatumas ir pilietinės laisvės ir padidinamas skaidrumas.

Aktu draudžiama masiškai rinkti bet kokius įrašus, įskaitant JAV ir ne JAV asmenų įrašus, pagal įvairias FISA nuostatas arba naudojant Nacionalinio saugumo raštus, pagal įstatymą leidžiamų administracinių potvarkių forma ⁽⁶⁾. Šis draudimas visų pirma taikomas telefonų metaduomenims, susijusiems su skambučiais tarp JAV esančių ir užsienyje esančių asmenų, ir bus svarbus pagal šiuos įgaliojimus renkant „privatumo skydo“ informaciją. Pagal aktą reikalaujama, kad Vyriausybė kiekvieną prašymą dėl įrašų suteikimo pagal šiuos įgaliojimus pagrįstų „konkrečia atrankos sąlyga“, t. y. sąlyga, kuria aiškiai apibūdinamas asmuo, sąskaita, adresas arba asmeninis prietaisas, kuriuo ribojamas renkamos informacijos kiekis tiek tai pagrįstai įmanoma ⁽⁷⁾. Taip užtikrinama, kad informacijos rinkimas žvalgybos tikslais būtų konkretus ir tikslingas.

Aktu taip pat padaryti svarbūs FISA teismo procedūrų pakeitimai, kuriais užtikrinamas didesnis skaidrumas ir suteikiamos papildomos garantijos dėl privatumo apsaugos. Kaip minėta, šiuo aktu leidžiama sudaryti nuolatinės saugumo leidimus turinčių advokatų, besispecializuojančių privatumo ir pilietinių laisvių, žvalgybos duomenų rinkimo, komunikacijų technologijų ir kitose susijusiose srityse, komisijas, ir šie advokatai gali būti paskiriami į teismą kaip *amicus curiae* bylose, susijusiose su svarbiu arba nauju teisės aiškinimu. Šiems advokatams leidžiama pateikti teisinius argumentus, kuriais ginamas asmens privatumas ir pilietinės laisvės, ir susipažinti su visa informacija, įskaitant išslaptintą informaciją, kuri, teismo manymu, yra būtina jų pareigoms vykdyti ⁽⁸⁾.

Aktas taip pat pagrįstas beprecedenčiu JAV Vyriausybės įsipareigojimu užtikrinti skaidrumą žvalgybos veiklos srityje reikalaujant, kad DNI, pasikonsultavęs su generaliniu advokatu, išslaptintų arba paskelbtų išslaptintą santrauką kiekvieno sprendimo, nutarties ar nuomonės, kurią priėmė FISA teismas arba Apeliacinis užsienio žvalgybos stebėsenos teismas, kurioje pateikiamas svarbus bet kurios teisės nuostatos vertinimas arba aiškinimas.

⁽¹⁾ Žr. JAV kodekso 50 antraštinės dalies 1881 straipsnio f dalį.

⁽²⁾ Žr. ten pat. 1881 straipsnio a dalies 1 punkto 1 papunktis.

⁽³⁾ Žr. ten pat. 1881 straipsnio a dalies 1 punkto 3 papunktis. Kai kurios iš šių ataskaitų yra išslaptintos.

⁽⁴⁾ Nario nuomonė ir įsako 26 punktas (FISC 2014), skelbiama adresu <http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf>.

⁽⁵⁾ Žr. 2015 m. JAV laisvės aktą, oficialusis leidinys Nr. 114–23, § 401, 129 Stat. 268.

⁽⁶⁾ Žr. ten pat. 103, 201, 501 straipsniai. Nacionalinio saugumo raštai yra numatyti įvairiuose įstatymuose ir pagal juos FTB gali gauti informaciją, esančią kredito ataskaitose, finansiniuose įrašuose ir elektroninius abonentų ir sandorių įrašus iš tam tikrų rūšių bendrovių, siekdama tik užtikrinti apsaugą nuo tarptautinio terorizmo arba neteisėtos žvalgybos veiklos. Žr. JAV kodekso 12 antraštinės dalies 3414 straipsnį, 15 antraštinės dalies 1681u–1681v straipsnius, 18 antraštinės dalies 2709 straipsnį. Nacionalinius saugumo raštus paprastai naudoja FTB siekdamas rinkti svarbią su turiniu nesusijusią informaciją ankstyvais kovos su terorizmu ir kontržvalgybos tyrimo etapais, pvz., sąskaitos abonentas, kuris gali palaikyti ryšius su teroristinės grupės, pvz., ISIL, nariais. Nacionalinio saugumo rašto gavėjai turi teisę juos ginčyti teisme. Žr. JAV kodekso 18 antraštinės dalies 3511 straipsnį.

⁽⁷⁾ Žr. ten pat.

⁽⁸⁾ Žr. ten pat. 401 straipsnis.

Be to, akte nustatyta daugybė atvejų, kai turi būti atskleidžiami prašymai dėl FISA duomenų rinkimo arba nacionalinio saugumo raštų. Jungtinės Amerikos Valstijos kasmet, be kitos informacijos, privalo atskleisti Kongresui ir visuomenei įvairias FISA nutartis ir sertifikatus, dėl kurių pateiktas prašymas buvo patenkintas, apytikslių sekamų ir stebimų JAV ir ne JAV asmenų skaičių ir paskirtų *amici curiae* skaičių ⁽¹⁾. Pagal aktą taip pat reikalaujama, kad Vyriausybė teiktų papildomas viešas ataskaitas apie prašymų išduoti nacionalinio saugumo raštus dėl JAV ir ne JAV asmenų skaičių ⁽²⁾.

Kalbant apie įmonių skaidrumą, pažymėtina, kad minėtu aktu bendrovėms suteikiamos įvairios galimybės teikti viešas ataskaitas apie bendrą FISA nutarčių ir direktyvų arba nacionalinio saugumo raštų, kuriuos jos gauna iš Vyriausybės, skaičių, taip pat pagal šias nutartis sekamų vartotojų sąskaitų skaičių ⁽³⁾. Keletas bendrovių jau atskleidė tokius duomenis, iš kurių matyti, kad prašymai pateikti įrašus buvo susiję su nedideliu klientų skaičiumi.

Iš šių įmonių skaidrumo ataskaitų matyti, kad JAV žvalgybos prašymai daro poveikį tik nedidelei duomenų daliai. Pavyzdžiui, iš vienos didelės įmonės vėliausiai pateiktų skaidrumo ataskaitų matyti, kad ji gavo nacionalinius saugumo prašymus (pagal FISA arba nacionalinio saugumo raštus), susijusius su mažiau nei 20 000 jos sąskaitų, o jos abonentų skaičius buvo 400 mln. Kitaip tariant, visi JAV nacionalinio saugumo prašymai, apie kuriuos pranešė ši įmonė, buvo susiję su mažiau nei 0,05 % jos abonentų. NET jeigu kiekvienas iš šių prašymų būtų susijęs su „saugaus uosto“ duomenimis, – o tai, žinoma, nėra tas atvejis, – akivaizdu, kad prašymai yra tikslingi, jų mastas tinkamas ir jie nėra masiški arba pateikti be atrankos.

Galiausiai, nors įstatymais, kuriais leidžiama išduoti nacionalinio saugumo raštus, jau apribojamos aplinkybės, kuriomis tokio rašto gavėjui būtų galima jį atskleisti, akte taip pat nustatyta, kad toks konfidencialumo reikalavimas turi būti periodiškai peržiūrimas; reikalaujama, kad nacionalinio saugumo raštų gavėjai būtų informuoti, kai, atsižvelgiant į faktus, konfidencialumo reikalavimas nebegalioja, ir informuoti apie kodifikavimo procedūras, kuriomis gavėjai galėjo ginčyti konfidencialumo reikalavimą ⁽⁴⁾.

Apibendrinant, svarbūs JAV laisvės akto pakeitimai, susiję su JAV žvalgybos įgaliojimais, aiškiai įrodo dideles Jungtinių Amerikos Valstijų pastangas užtikrinti, kad, laikantis JAV žvalgybos praktikos, visada būtų paisoma asmeninės informacijos, privatumo, pilietinių laisvių apsaugos ir skaidrumo.

IV. SKAIDRUMAS

Be JAV laisvės akte nustatytų skaidrumo reikalavimų, JAV žvalgybos bendruomenė teikia daug daugiau papildomos informacijos ir taip rodo deramą pavyzdį savo žvalgybos veiklos srityje. Žvalgybos bendruomenė paskelbė nemažai savo politikos, procedūrų, Užsienio žvalgybos stebėsenos teismo sprendimų ir kitos išslaptintos medžiagos, taip užtikrindama ypač didelį skaidrumo lygį. Be to, žvalgybos bendruomenė iš esmės padidino atskleidžiamų statistinių duomenų apie tai, kaip Vyriausybė naudoja nacionalinio saugumo žvalgybos įgaliojimus, kiekį. 2015 m. balandžio 22 d. žvalgybos bendruomenė paskelbė savo antrąją metinę ataskaitą, kurioje pateikė statistinius duomenis apie tai, kaip dažnai Vyriausybė naudoja šiais įgaliojimais. ODNI savo svetainėje ir IC *On the Record* svetainėje taip pat paskelbė konkrečių skaidrumo principų rinkinį ⁽⁵⁾ ir įgyvendinimo planą, kuris padės principus paversti konkrečiomis, įvertinamomis iniciatyvomis ⁽⁶⁾. 2015 m. spalio mėn. Nacionalinės žvalgybos direktorius nurodė, kad kiekviena žvalgybos agentūra pati paskirtą joje veikiančią žvalgybos skaidrumo pareigūną, kuris skatintų skaidrumą ir vadovautų skaidrumo iniciatyvoms ⁽⁷⁾. Skaidrumo pareigūnas glaudžiai dirbs su kiekvienu žvalgybos agentūros privatumo ir pilietinių laisvių pareigūnu ir užtikrins, kad skaidrumas, privatumas ir pilietinės laisvės toliau liktų pagrindiniais prioritetais.

⁽¹⁾ Žr. ten pat, 602 straipsnis.

⁽²⁾ Žr. ten pat.

⁽³⁾ Žr. ten pat, 603 straipsnis.

⁽⁴⁾ Žr. ten pat. 502 straipsnio f dalį – 503 straipsnį.

⁽⁵⁾ Skelbiama adresu <http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles>.

⁽⁶⁾ Skelbiama adresu <http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf>.

⁽⁷⁾ Žr. ten pat.

Siekdamas pažangos šioje srityje, NSA vyriausiasis privatumo ir pilietinių laisvių pareigūnas per pastaruosius metus atskleidė keletą išslaptintų ataskaitų, įskaitant ataskaitas apie veiklą pagal 702 straipsnį, Vykdomąjį įsaką 12333 ir JAV laisvės aktą⁽¹⁾. Be to, žvalgybos bendruomenė glaudžiai dirba su PCLOB, Kongresu ir JAV privatumo advokatų bendruomene, kad dar labiau didintų JAV žvalgybos veiklos skaidrumą, kai tai įmanoma ir atsižvelgdama į konfidencialių žvalgybos šaltinių ir metodų apsaugą. Iš esmės JAV žvalgybos veikla yra tokia pat skaidri, kaip bet kurios kitos pasaulio valstybės, arba skaidresnė, ir ji skaidri tiek, kiek įmanoma atsižvelgiant į poreikį apsaugoti konfidencialius šaltinius ir metodus.

Apibendrinant visapusišką skaidrumą JAV žvalgybos veiklos srityje, galima atkreipti dėmesį į toliau nurodytus aspektus.

- Žvalgybos bendruomenė atskleidė ir internete paskelbė didelį kiekį medžiagos, susijusios su teismo nuomonėmis ir agentūros procedūromis, kuriose apibūdinamos konkrečios mūsų žvalgybinės veiklos procedūros ir reikalavimai. Taip pat atskleidė ataskaitas apie tai, kaip žvalgybos agentūros laikosi taikomų apribojimų.
- Vyresnieji žvalgybos pareigūnai reguliariai viešai praneša apie savo organizacijų vaidmenį ir veiklą, įskaitant atitikties režimo aprašymus ir jų darbe taikomas apsaugos priemones.
- Žvalgybos bendruomenė pagal Informacijos laisvės aktą paskelbė daugybę papildomų dokumentų apie žvalgybos veiklą.
- Prezidentas paskelbė PPD-28, kurioje viešai išdėstyti papildomi mūsų žvalgybos veiklai taikomi apribojimai, o ODNI paskelbė dvi viešas šių apribojimų laikymosi ataskaitas.
- Šiuo metu žvalgybos bendruomenė pagal įstatymą turi paskelbti svarbias FISA teismo priimtas teises nuomones arba šių nuomonių santraukas.
- Vyriausybė turi kasmet teikti ataskaitas apie tai, kaip naudojasi tam tikrais nacionalinio saugumo įgaliojimais, o bendrovės taip pat įgaliotos tai daryti.
- PCLOB paskelbė keletą išsamių viešų žvalgybos veiklos ataskaitų ir tai darys ateityje.
- Žvalgybos bendruomenė teikia išsamią išslaptintą informaciją Kongreso priežiūros komitetams.
- DNI paskelbė skaidrumo principus, kuriais reglamentuojama žvalgybos bendruomenės veikla.

Šie skaidrumo įsipareigojimai ateityje tik didės. Žinoma, kiekviena viešai paskelbta informacija bus prieinama Komercijos departamentui ir Europos Komisijai. Komercijos departamento ir Europos Komisijos atliekama „privatumo skydo“ įgyvendinimo metinė peržiūra bus puiki proga Europos Komisijai aptarti visus klausimus, galinčius kilti dėl bet kurios naujai paskelbtos informacijos, taip pat kitus klausimus, susijusius su „privatumo skydu“ ir jo veikimu, ir suprantame, kad Departamentas gali savo nuožiūra kviesti kitų agentūrų, įskaitant žvalgybos bendruomenę, atstovus dalyvauti toje peržiūroje. Žinoma, tai papildo PPD-28 nustatytą mechanizmą, pagal kurį ES valstybės narės gali kelti su stebėjimu susijusius klausimus ir pateikti juos paskirtam Valstybės departamento pareigūnui.

V. TEISIŲ GYNIMO BŪDAI

JAV teisėje nustatyti įvairūs teisių gynimo būdai, kuriais asmenys gali pasinaudoti tais atvejais, kai jų elektroninis susirašijimas buvo neteisėtai stebimas nacionalinio saugumo tikslais. Pagal FISA teisę ginti savo teises JAV teisme gali naudotis ne tik JAV asmenys. Asmeniui, kuris gali pagrįsti savo ieškinį, turi būti suteikiamos teisių gynimo priemonės teisėtam

⁽¹⁾ Skelbiama adresais: https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

elektroninių ryšių stebėjimui pagal FISA ginčyti. Pavyzdžiui, pagal FISA asmenims, kurių elektroniniai ryšiai buvo stebimi neteisėtai, leidžiama pareikšti ieškinį JAV Vyriausybės pareigūnams kaip fiziniams asmenims dėl piniginės kompensacijos, įskaitant baudinių nuostolių ir advokato mokesčių atlyginimą. Žr. JAV kodekso 50 antraštinės dalies 1810 straipsnį. Asmenys, kurie gali pagrįsti savo ieškinį, taip pat gali reikalauti iš Jungtinių Amerikos Valstijų civiline tvarka atlyginti piniginius nuostolius, įskaitant bylinėjimosi išlaidų atlyginimą, kai informacija apie juos, gauta pagal FISA stebint elektroninius ryšius, buvo neteisėtai ir sąmoningai atskleista. Žr. JAV kodekso 18 antraštinės dalies 2712 straipsnį. Jeigu Vyriausybė ketina naudoti arba atskleisti bet kokią nukentėjusio asmens informaciją, gautą arba perimtą pagal FISA stebint elektroninius ryšius, prieš tą asmenį teisminiame arba administraciniame procese Jungtinėse Amerikos Valstijose, ji privalo iš anksto informuoti apie savo ketinimą teismą ir asmenį, kuris tuomet gali ginčyti stebėjimo teisėtumą ir siekti panaikinti informaciją. Žr. JAV kodekso 50 antraštinės dalies 1806 straipsnį. Galiausiai FISA taip pat skiria baudžiamąsias sankcijas asmenims, kurie tyčia neteisėtai stebi elektroninius ryšius pagal įvairius įstatymus arba kurie tyčia naudoja arba atskleidžia neteisėtomis stebėjimo priemonėmis gautą informaciją. Žr. JAV kodekso 50 antraštinės dalies 1809 straipsnį.

ES piliečiai gali pasinaudoti ir kitais teisių gynimo būdais JAV Vyriausybės pareigūnų atžvilgiu, kai Asmeniui, kuris gali pagrįsti savo ieškinį, turi būti suteikiamos teisių gynimo priemonės teisėtam elektroninių ryšių stebėjimui pagal FISA ginčyti Vyriausybė neteisėtai naudoja arba tikrina duomenis, įskaitant Vyriausybės pareigūnus, kurie įstatymą pažeidžia neteisėtai tikrindami arba naudodami informaciją tariamais nacionalinio saugumo tikslais. Kompiuterinio sukčiavimo ir piktnaudžiavimo akte draudžiama tyčinė neteisėta prieiga (arba teisėtos prieigos ribų viršijimas) siekiant gauti informaciją iš finansų įstaigos, JAV Vyriausybės kompiuterinės sistemos arba prie interneto prijungto kompiuterio, taip pat grasinimai sugadinti saugomus kompiuterius siekiant daryti poveikį arba apgaulės būdu. Žr. JAV kodekso 18 antraštinės dalies 1030 straipsnį. Kiekvienas asmuo, nepaisant jo pilietybės, kuris dėl šio įstatymo pažeidimo patiria žalos arba nuostolių, gali pareikšti ieškinį pažeidėjui (įskaitant Vyriausybės pareigūną) dėl žalos kompensavimo ir draudimo arba kitų lygiaverčių teisių gynimo priemonių pagal 1030 straipsnio g dalį, nepaisant to, ar buvo pradėtas baudžiamasis persekiojimas, jeigu elgesys yra susijęs bent su keliomis įstatyme išvardytomis aplinkybėmis. Elektroninių ryšių privatumo aktu (ECPA) reglamentuojama Vyriausybės prieiga prie saugomų elektroninių ryšių ir sandorių įrašų ir abonento informacijos, kurią turi ryšių paslaugas teikiančios trečiosios šalys. Žr. JAV kodekso 18 antraštinės dalies 2701–2712 straipsnius. Pagal ECPA nukentėjusiam asmeniui leidžiama pareikšti ieškinį Vyriausybės pareigūnams dėl tyčinės neteisėtos prieigos prie saugomų duomenų. ECPA taikomas visiems asmenims, nepaisant jų pilietybės, ir nukentėjusiems asmenims gali būti priteisiamas žalos ir advokato mokesčių atlyginimas. Teisės į finansinių duomenų privatumą aktu (RFPA) ribojama JAV Vyriausybės prieiga prie banko ir tarpininkų prekiautojų įrašų, susijusių su individualiais klientais. Žr. JAV kodekso 12 antraštinės dalies 3401–3422 straipsnius. Pagal RFPA banko arba tarpininko prekiautojo klientas gali pareikšti JAV Vyriausybei ieškinį dėl įstatymuose nustatytos žalos, faktinės žalos ir baudinių nuostolių, atsiradusių gavus prieigą prie kliento įrašų, atlyginimo, o padarius išvadą, kad tokia neteisėta prieiga buvo tyčinė, prieš atitinkamus Vyriausybės darbuotojus automatiškai pradedamas tyrimas dėl galimų drausminių veiksmų. Žr. JAV kodekso 12 antraštinės dalies 3417 straipsnį.

Galiausiai Informacijos laisvės akte (FOIA) nustatytos priemonės, kuriomis kiekvienas asmuo gali pasinaudoti siekdamas gauti prieigą prie esamų federalinės agentūros įrašų bet kuriuo klausimu, atsižvelgiant į tam tikrų kategorijų išimtis. Žr. JAV kodekso 5 antraštinės dalies 552 straipsnio b dalį. Šios išimties apima prieigos prie įslaptintos nacionalinio saugumo informacijos, kitų asmenų duomenų ir informacijos, susijusios su teisėsaugos tyrimais, ribas ir yra panašios į valstybės nustatytus apribojimus, galiojančius pagal jų prieigos prie informacijos įstatymus. Šie apribojimai amerikiečiams ir užsieniečiams taikomi vienodai. Ginčai dėl įrašų atskleidimo, kurio prašoma pagal FOIA, gali būti skundžiami administracine tvarka, o vėliau – ir federaliniame teisme. Reikalaujama, kad teismas iš naujo nustatytų, ar įrašai tinkamai saugomi (JAV kodekso 5 antraštinės dalies 552 straipsnio a dalies 4 punkto B papunktis), ir gali įpareigoti Vyriausybę suteikti prieigą prie įrašų. Kai kuriais atvejais teismai panaikino Vyriausybės pareiškimus, kad informacija turėtų būti saugoma kaip įslaptinta.⁽¹⁾ Nors piniginės kompensacijos negalima gauti, teismai gali priteisti atlyginti advokato mokesčius.

VI. IŠVADA

Jungtinės Amerikos Valstijos pripažįsta, kad, vykdydama signalų žvalgybos ir kitą žvalgybos veiklą, privalo atsižvelgti į tai, kad su visais asmenimis turi būti elgiamasi oriai ir pagarbiai, nepaisant jų pilietybės arba gyvenamosios vietos, ir kad visi asmenys turi teisėtus privatumo interesus, susijusius su jų asmeninės informacijos tvarkymu. Jungtinės Amerikos Valstijos signalų žvalgybą naudoja tik siekdama ginti savo nacionalinio saugumo ir užsienio politikos interesus ir apsaugoti savo piliečius ir savo sąjungininkų ir partnerių piliečius nuo žalos. Trumpai tariant, žvalgybos bendruomenė neužsiima masine visų asmenų stebėseną, įskaitant paprastus Europos piliečius. Signalų žvalgybos duomenys renkami tik tinkamai sankcionuotais atvejais ir tokiu būdu, kuris griežtai atitinka šiuos apribojimus, tik išnagrinėjus alternatyvių

⁽¹⁾ Žr., pvz., *New York Times v. Department of Justice*, 756 F.3d 100 (2d Cir. 2014); *American Civil Liberties Union v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

šaltinių prieinamumą, įskaitant diplomatinčius ir viešus šaltinius, ir tokiu būdu, kuriuo pirmenybė teikiama tinkamoms ir pagrįstoms alternatyvoms. Kai įmanoma, signalų žvalgybos duomenys renkami tik renkant tikslingus duomenis apie konkrečius užsienio žvalgybos taikinius arba temas naudojant diskriminantus.

Šiuo atžvilgiu JAV politika patvirtinta PPD-28. Šioje sistemoje JAV žvalgybos agentūros neturi teisinių įgaliojimų, išteklių, techninių gebėjimų arba noro perimti visus pasaulio ryšius. Tos agentūros neskaito visų Jungtinių Amerikos Valstijų ar pasaulyje parašomų e. laiškų. Laikydamosi PPD-28 Jungtinės Amerikos Valstijos teikia tinkamas ne JAV asmenų asmeninės informacijos, kuri renkama vykdant signalų žvalgybos veiklą, apsaugos priemones. Kiek įmanoma atsižvelgiant į nacionalinį saugumą, tai apima politiką ir procedūras, kuriomis siekiama asmeninę informaciją, susijusią su ne JAV asmenimis, kuo trumpiau saugoti ir kuo mažiau platinti, palyginti su JAV asmenims taikoma apsauga. Be to, kaip atarta pirmiau, išsamus priežiūros režimas, tikslingai taikomas pagal FISA 702 straipsnį suteiktiems įgaliojimams, neturi sau analogų. Galiausiai svarbūs JAV žvalgybos teisės pakeitimai, kurie buvo nustatyti JAV laisvės akte ir ODNI, lėmė iniciatyvas, kuriomis skatinamas žvalgybos bendruomenėje skaidrumas, iš esmės padidino visų asmenų privatumą ir pilietines laisves, nepaisant jų pilietybės.

Pagarbiai
Robertas S. Littas

2016 m. birželio 21 d.

Justinui S. Antonipillai,
JAV komercijos departamento
advokatui
1401 Constitution Avenue, N.W.
Vašingtonas, DC 20230

Tedui Deanui,
Tarptautinės prekybos administracijos
sekretoriaus pavaduotojui
1401 Constitution Avenue, N.W.
Vašingtonas, DC 20230

Gerbiami J. Antonipillai ir T. Deanai,

šiam rašte pateikiama išsamesnė informacija apie tai, kaip Jungtinės Amerikos Valstijos masiškai renka signalų žvalgybos duomenis. Kaip paaiškinta Prezidento politinės direktyvos (toliau – PPD-28) 5 išnašoje, „masinis“ duomenų rinkimas reiškia gana didelio signalų žvalgybos informacijos kiekio arba duomenų gavimą tais atvejais, kai žvalgybos bendruomenė negali panaudoti identifikatoriaus, susijusio su konkrečiu taikiniu (pvz., sekamo asmens e. pašto adresas arba telefono numeris), kad galėtų tikslingai rinkti duomenis. Tačiau tai nereiškia, kad šios rūšies duomenų rinkimas yra „masinis“ ar „vykdomas be atrankos“. Tiesą sakant, pagal PPD-28 taip pat reikalaujama, kad „[s]ignalų žvalgybos veikla būtų kuo tikslingesnė“. Toliau naudodamasi savo įgaliojimais, žvalgybos bendruomenė imasi priemonių užtikrinti, kad net ir tais atvejais, kai tikslingo duomenų rinkimo tikslais negalima panaudoti konkrečių identifikatorių, turi būti įsitikinama, kad duomenyse, kuriuos reikia surinkti, bus užsienio žvalgybos duomenų, atitinkančių JAV politikos formuotojų pagal ankstesniame mano rašte aprašytas procedūras nustatytus reikalavimus, ir kuo labiau sumažinamas renkamos nesusijusios informacijos kiekis.

Pavyzdžiui, žvalgybos bendruomenės gali būti prašoma gauti signalų žvalgybos duomenų apie Artimųjų Rytų regiono šalyje veikiančios teroristų grupės veiksmus, kuri, kaip manoma, planuoja atakas Vakarų Europos šalyse, tačiau žvalgybos bendruomenė gali nežinoti su šia teroristų grupe susijusių asmenų vardų, telefono numerių, e. pašto adresų ar kitų konkrečių identifikatorių. Tą grupę galime nuspręsti sekti rinkdami duomenis apie abipusius ryšių srautus į tą regioną ir iš jo, kuriuos vėliau peržiūrėsime ir analizuosime, kad nustatytume su grupės susijusius ryšius. Tai darydama žvalgybos bendruomenė turėtų stengtis užtikrinti kuo tikslingesnę duomenų rinkimą. Tokia veikla būtų laikoma „masiniu“ duomenų rinkimu, nes neįmanoma naudoti diskriminantų, tačiau ji nėra nei „masinė“, nei „vykdoma be atrankos“; tiesą sakant, stengiamasi užtikrinti kuo didesnę tokios veiklos tikslingumą.

Todėl net jeigu tikslingas duomenų rinkimas naudojant konkrečius įrenginius neįmanomas, Jungtinės Amerikos Valstijos nerenka ryšių duomenų iš visų pasaulio ryšių įrenginių, tačiau taiko filtrus ir kitas technines priemones, kad orientuotų duomenų rinkimo veiklą į įrangą, iš kurios, tikėtina, galima gauti užsienio žvalgybos vertę turinčių ryšių. Šiuo atveju Jungtinių Amerikos Valstijų signalų žvalgybos veikla yra susijusi tik su dalimi internete perduodamų ryšių.

Be to, kaip nurodyta ankstesniame mano rašte, kadangi dėl „masinio“ duomenų rinkimo kyla didesnė rizika surinkti nesusijusius ryšių duomenis, PPD-28 nustatyta, kad žvalgybos bendruomenė surinktus masinius signalų žvalgybos duomenis gali naudoti tik šešiais tikslais. PPD-28 ir agentūros nustatytoje PPD-28 įgyvendinimo politikoje taip pat nustatyti asmeninės informacijos, gytos signalų žvalgybos metu, saugojimo ir platinimo ribojimai, nepaisant to, ar informacija buvo renkama masiškai ar tikslingai ir nepaisant asmens pilietybės.

Todėl žvalgybos „masinis“ duomenų rinkimas nėra „masinis“ ar „vykdomas be atrankos“, tačiau yra susijęs su taikomais metodais ir priemonėmis, kuriomis filtruojami renkami duomenys, siekiant tikslingai rinkti tuos duomenis, kurie atitinka politikos formuotojų nustatytus užsienio žvalgybos reikalavimus, kartu kuo labiau sumažinant nesusijusios informacijos

rinkimą, ir atliekamas laikantis griežtų taisyklių, kurių paskirtis – apsaugoti nesusijusią informaciją, kuri gali būti surinkta. Šiame rašte aprašyta politika ir procedūra taikoma visai masinei signalų žvalgybos duomenų rinkimo veiklai, įskaitant bet koki masinį į Europą ir iš Europos perduodamų ryšių rinkimą nepatvirtinant ar nepaneigiant fakto, ar tokie duomenys apskritai renkami.

Taip pat prašėte pateikti daugiau informacijos apie Privatumo ir pilietinių laisvių priežiūros valdybos (PCLOB) ir generalinius inspektorius ir jų įgaliojimus. PCLOB yra nepriklausoma vykdomosios valdžios agentūra. Ją sudaro Senato pritarimu prezidento šešerių metų kadencijai paskirta dvipartinė penkių narių valdyba ⁽¹⁾. Kiekvienas valdybos narys skiriamas šešerių metų kadencijai. Valdybos nariams ir darbuotojams taikomi atitinkami saugumo patikrinimai, kad jie galėtų visapusiškai vykdyti savo pareigas pagal įstatymą ⁽²⁾.

PCLOB misija – užtikrinti, kad federalinės Vyriausybės pastangos užkirsti kelią terorizmui būtų suderintos su poreikiu apsaugoti privatumą ir pilietines laisves. Valdybos pareigos yra susijusios su dviem pagrindinėmis atsakomybės sritimis – priežiūra ir konsultavimu. PCLOB pati nustato savo darbotvarkę ir tai, kokios priežiūros veiklos ji nori imtis ar kokias konsultacijas teikti.

Vykdydama savo priežiūros funkcijas, PCLOB peržiūri ir analizuoja vykdomosios valdžios veiksmus, kurių ji imasi, kad apsaugotų tautą nuo terorizmo, ir užtikrina, kad tokių veiksmų poreikis būtų suderinamas su poreikiu apsaugoti privatumą ir pilietines laisves ⁽³⁾. Vėliausioje PCLOB užbaigtoje priežiūros peržiūroje daugiausia dėmesio skirta stebėjimo programoms, kurios buvo vykdomos pagal FISA 702 straipsnį ⁽⁴⁾. Šiuo metu ji atlieka pagal Vykdomąją įsaką 12333 atliktos žvalgybos veiklos peržiūrą ⁽⁵⁾.

Vykdydama savo konsultavimo funkciją, PCLOB užtikrina, kad rengiant ir įgyvendinant įstatymus, reglamentus ir politiką, susijusią su pastangomis apsaugoti tautą nuo terorizmo, būtų paisoma su laisve susijusių aspektų ⁽⁶⁾.

Kad galėtų vykdyti savo misiją, valdybai suteikiami įstatyme nustatyti įgaliojimai susipažinti su visais susijusiais agentūros įrašais, ataskaitomis, audito dokumentais, peržiūromis, dokumentais, raštais, rekomendacijomis ir visa kita susijusia medžiaga, įskaitant pagal įstatymą įslaptintą informaciją ⁽⁷⁾. Be to, valdyba gali apklausti bet kurį vykdomosios valdžios institucijos pareigūną ar darbuotoją, gauti iš jo pareiškimus ar prašyti viešai liudyti ⁽⁸⁾. Valdyba taip pat gali raštu prašyti, kad generalinis prokuroras valdybos vardu priimtų įsakymus, kuriais vykdomajai valdybai nepavaldžios šalys būtų įpareigojamos pateikti susijusią informaciją ⁽⁹⁾.

Galiausiai PCLOB pagal įstatymą turi laikytis skaidrumo reikalavimų. Tai reiškia, kad visuomenė turi būti informuojama apie valdybos veiklą rengiant viešus posėdžius ir viešai skelbiant valdybos ataskaitas ir visapusiškai atsižvelgiant į būtinybę apsaugoti konfidencialią informaciją ⁽¹⁰⁾. Be to, reikalaujama, kad PCLOB praneštų, kai vykdomosios valdžios agentūra atsisako vadovautis jos rekomendacijomis.

Žvalgybos bendruomenės generaliniai inspektoriai atlieka žvalgybos bendruomenės programų ir veiklos auditą, patikrinimus ir peržiūras, kad nustatytų ir šalintų sisteminę riziką, silpnąsias vietas ir trūkumus. Be to, generaliniai inspektoriai tiria skundus ar informaciją dėl tariamų teisės, taisyklių ar reglamentų pažeidimų ar netinkamo valdymo;

⁽¹⁾ JAV kodekso 42 antraštinės dalies 2000ee straipsnio a ir h dalys.

⁽²⁾ JAV kodekso 42 antraštinės dalies 2000ee straipsnio k dalis.

⁽³⁾ JAV kodekso 42 antraštinės dalies 2000ee straipsnio d dalies 2 punktas.

⁽⁴⁾ Žr. bendrą informaciją <https://www.pclob.gov/library.html#oversightreports>.

⁽⁵⁾ Žr. bendrą informaciją <https://www.pclob.gov/events/2015/may13.html>.

⁽⁶⁾ JAV kodekso 42 antraštinės dalies 2000ee straipsnio d dalies 1 punktas; taip pat žr. PCLOB konsultavimo funkcijos politiką ir procedūras, politika 2015–004, skelbiama adresu https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.

⁽⁷⁾ JAV kodekso 42 antraštinės dalies 2000ee straipsnio g dalies 1 punkto A papunktis.

⁽⁸⁾ JAV kodekso 42 antraštinės dalies 2000ee straipsnio g dalies 1 punkto B papunktis.

⁽⁹⁾ JAV kodekso 42 antraštinės dalies 2000ee straipsnio g dalies 1 punkto D papunktis.

⁽¹⁰⁾ JAV kodekso 42 antraštinės dalies 2000ee straipsnio f dalis.

lėšų švaistymo stambiu mastu; piktnaudžiavimo įgaliojimais, arba didelio ir konkretaus pavojaus visuomenės sveikatai ir saugumui, kuris kyla dėl žvalgybos bendruomenės programų ir veiklos. Generalinių inspektorių nepriklausomumas yra esminis aspektas, lemiantis kiekvienos generalinio inspektoriaus parengtos ataskaitos, išvados ir rekomendacijos objektyvumą ir patikimumą. Kai kurie iš svarbiausių generalinių inspektorių nepriklausomumo užtikrinimo komponentų apima generalinio inspektoriaus paskyrimą ir atleidimo iš pareigų tvarką; atskirtus įgaliojimus veiklos, biudžeto sudarymo ir personalo srityse, ir dvejopų ataskaitų teikimą vykdomosios valdžios agentūrai ir Kongresui.

Kongresas kiekvienoje vykdomosios valdžios agentūroje, įskaitant kiekvieną žvalgybos bendruomenės subjektą, įkūrė nepriklausomą generalinio inspektoriaus biurą ⁽¹⁾. Priėmus Žvalgybos įgaliojimų 2015 fiskalinius metais aktą, beveik visus generalinius inspektorių, kurie priežiūri žvalgybos bendruomenės subjektą, Teisingumo departamentą, Centrinę žvalgybos valdybą, Nacionalinio saugumo agentūrą ir žvalgybos bendruomenę, skiria prezidentas, o tvirtina Senatas ⁽²⁾. Be to, šie generaliniai inspektoriai yra nuolatiniai nepartiniai pareigūnai, kuriuos iš pareigų gali atleisti tik prezidentas. Nors pagal JAV Konstituciją reikalaujama, kad prezidentui būtų suteikti įgaliojimai atleisti generalinį inspektorių iš pareigų, tačiau jis šiais įgaliojimais retai naudojasi, be to, reikalaujama, kad prezidentas pateiktų Kongresui rašytinį pagrindimą likus 30 dienų iki generalinio inspektoriaus atleidimo ⁽³⁾. Šiuo generalinio inspektoriaus skyrimo procesu užtikrinama, kad vykdomosios valdžios pareigūnai nedarytų jokios netinkamos įtakos atrenkant, skiriant ar atleidžiant generalinį inspektorių.

Antra, generaliniai inspektoriai turi plačius įstatyme nustatytus įgaliojimus atlikti vykdomosios valdžios programų ir veiksmų auditą, tyrimus ir peržiūras. Be įstatyme nustatytų įgaliojimų vykdyti tyrimų ir peržiūrų priežiūrą, generaliniai inspektoriai turi plačią diskreiją naudotis priežiūros įgaliojimais ir pasirinkti, kurias programas ir veiksmus peržiūrėti ⁽⁴⁾. Šių įgaliojimų vykdymo srityje įstatymu užtikrinama, kad generaliniai inspektoriai, vykdydami savo pareigas, galėtų pasinaudoti nepriklausomais ištekliais, įskaitant galimybę savarankiškai samdyti darbuotojus ir teikti Kongresui atskirus prašymus dėl biudžeto ⁽⁵⁾. Įstatymu užtikrinama, kad generaliniai inspektoriai galėtų susipažinti su informacija, kurios reikia jų pareigoms įvykdyti. Tai apima įgaliojimus tiesiogiai susipažinti su visais agentūros įrašais ir informacija, kurioje išsamiau aprašomos agentūros programos ir veiksmai, nepaisant informacijos slaptumo; įgaliojimus susipažinti su šaukimo į teismą informacija ir dokumentais, ir įgaliojimus prisaikdinti asmenis ⁽⁶⁾. Konkrečiais atvejais vykdomosios valdžios agentūros direktorius gali uždrausti generalinio inspektoriaus veiklą, jeigu, pvz., generalinio inspektoriaus auditas arba tyrimas iš esmės pakenktų Jungtinių Amerikos Valstijų nacionalinio saugumo interesams. Vėgi, šiais naudojimais šiais įgaliojimais yra labai neįprastas reiškinys ir šiuo atveju agentūros direktorius iš anksto prieš 30 dienų informuoja Kongresą apie tokių įgaliojimų panaudojimo priežastis ⁽⁷⁾. Tiesą sakant, Nacionalinės žvalgybos direktorius niekada netaikė šių ribojančio pobūdžio įgaliojimų kurio nors generalinio inspektoriaus veiklai.

Trečia, generaliniai inspektoriai turi pareigą vykdomosios valdžios agentūrų direktorius ir Kongresą nuolat visapusiškai informuoti ir šiuo tikslu teikti ataskaitas apie sukčiavimą ir kitas rimtas problemas, piktnaudžiavimo atvejus ir su vykdomosios valdžios programomis ir veiksmais susijusius trūkumus ⁽⁸⁾. Dvejopų ataskaitų teikimas padeda sustiprinti generalinio inspektoriaus nepriklausomumą, nes užtikrina generalinio inspektoriaus priežiūros proceso skaidrumą ir sudaro sąlygas agentūros direktoriui įgyvendinti generalinio inspektoriaus rekomendacijas prieš Kongresui imantis teisėkūros veiksmų. Pavyzdžiui, pagal įstatymą reikalaujama, kad generaliniai inspektoriai parengtų pusmečio ataskaitas, kuriose aprašomos tokios problemos, taip pat naujausi taisomieji veiksmai, kurių buvo imtasi ⁽⁹⁾. Vykdomosios valdžios

⁽¹⁾ 1978 m. Generalinio inspektoriaus akto (iš dalies pakeistas) 2 ir 4 straipsniai (toliau – IG aktas); 1947 m. Nacionalinio saugumo akto (iš dalies pakeistas) 103H straipsnio b ir e dalys; Centrinės žvalgybos akto (toliau – CŽV aktas) 17 straipsnio a dalis.

⁽²⁾ Žr. oficialųjį leidinį Nr. 113–293, 128 Stat. 3990, (2014 m. gruodžio 19 d.). Prezidentas neskiria tik Gynybos žvalgybos agentūros ir Nacionalinės geoerdvinės žvalgybos agentūros generalinių inspektorių; tačiau Gynybos departamento generalinio inspektoriaus ir Žvalgybos bendruomenės generalinio inspektoriaus jurisdikcija šių agentūrų atžvilgiu sutampa.

⁽³⁾ 1978 m. IG akto (iš dalies pakeistas) 3 straipsnis; Nacionalinio saugumo akto 103H straipsnio c dalis ir CŽV akto 17 straipsnio b dalis.

⁽⁴⁾ Žr. 1947 m. IG akto 4 straipsnio a dalį ir 6 straipsnio a dalies 2 punktą; Nacionalinio saugumo akto 103J straipsnio e dalį ir g dalies 2 punkto A papunktį; CŽV akto 17 straipsnio a ir c dalis.

⁽⁵⁾ IG akto 3 straipsnio d dalis, 6 straipsnio a dalies 7 punktas ir 6 straipsnio f dalis; Nacionalinio saugumo akto 103H straipsnio d, i, j ir m dalys; CŽV akto 17 straipsnio e dalies 7 punktas ir f dalis.

⁽⁶⁾ IG akto 6 straipsnio a dalies 1, 3, 4, 5 ir 6 punktai; Nacionalinio saugumo akto 103H straipsnio g dalies 2 punktas; CŽV akto 17 straipsnio e dalies 1, 2, 4 ir 5 punktai.

⁽⁷⁾ Žr., pvz., IG akto 8 straipsnio b dalį ir 8E straipsnio a dalį; Nacionalinio saugumo akto 103H straipsnio f dalį; CŽV akto 17 straipsnio b dalį.

⁽⁸⁾ IG akto 4 straipsnio a dalies 5 punktas; Nacionalinio saugumo akto 103H straipsnio a dalis ir b dalies 3 ir 4 punktai; CŽV akto 17 straipsnio a dalies 2 ir 4 punktai.

⁽⁹⁾ IG akto 2 straipsnio 3 punktas, 4 straipsnio a dalis ir 5 straipsnis; Nacionalinio saugumo akto 103H straipsnio k dalis; CŽV akto 17 straipsnio d dalis. Teisingumo departamento generalinis inspektorius ataskaitas skelbia viešai internete adresu <http://oig.justice.gov/reports/all.htm>. Panašiai, Žvalgybos bendruomenės generalinis inspektorius skelbia pusmečio ataskaitas, kurios prieinamos adresu <https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig>.

agentūros rimtai vertina generalinio inspektoriaus išvadas ir rekomendacijas, be to, generaliniai inspektoriai šiose ir kitose Kongresui, o kartais ir visuomenei teikiamose ataskaitose dažnai gali aptarti, kaip buvo laikomasi jų rekomendacijų ir kaip jos įgyvendintos ⁽¹⁾. Be šios dvejopų ataskaitų teikimo sistemos, generaliniai inspektoriai taip pat turi pareigą nukreipti vykdomosios valdžios pranešėjus apie pažeidimus į Kongreso priežiūros komitetus, kad jie atskleistų tariamus sukčiavimo, lėšų švaistymo ar piktnaudžiavimo, susijusios su vykdomosios valdžios programomis ir veikla, atvejus. Pranešėjų apie pažeidimus tapatybės neatskleidžiamos vykdomajai valdžiai, taip pranešėjai apie pažeidimus apsaugomi nuo galimų draudžiamų personalo veiksmų arba saugumo patikrinimo veiksmų, kurių imamasi reaguojant į generaliniam inspektoriui atskleistus faktus ⁽²⁾. Kadangi pranešėjai apie pažeidimus dažnai yra generalinių inspektorių tyrimų šaltiniai, galimybė Kongresui pranešti jų nurodytus faktus nepatiriant vykdomosios valdžios įtakos padidina generalinio inspektoriaus priežiūros veiksmingumą. Dėl šio nepriklausomumo generaliniai inspektoriai gali objektyviai ir nuosekliai didinti vykdomosios valdžios agentūrų veiklos ekonomiškumą, veiksmingumą ir atskaitomybę.

Galiausiai Kongresas sukūrė Generalinių inspektorių integralumo ir veiksmingumo tarybą. Ši taryba, be kita ko, rengi generalinių inspektorių audito, tyrimų ir peržiūrų standartus; remia mokymą, turi įgaliojimus atlikti peržiūras dėl tariamo netinkamo generalinio inspektoriaus elgesio ir veikia kaip svarbi generalinių inspektorių, kuriems patikėta visų kitų subjektų priežiūra, stebėtoja. ⁽³⁾

Tikiuosi, kad ši informacija bus naudinga.

Pagarbiai
Robertas S. Littas
generalinis advokatas

⁽¹⁾ IG akto 2 straipsnio 3 punktas, 4 straipsnio a dalis ir 5 straipsnis; Nacionalinio saugumo akto 103H straipsnio k dalis; CŽV akto 17 straipsnio d dalis. Teisingumo departamento generalinis inspektorius ataskaitas skelbia viešai internete adresu <http://oig.justice.gov/reports/all.htm>. Panašiai, Žvalgybos bendruomenės generalinis inspektorius skelbia pusmečio ataskaitas, kurios prieinamos adresu <https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig>.

⁽²⁾ IG akto 7 straipsnis; Nacionalinio saugumo akto 103H straipsnio g dalies 3 straipsnis CŽV akto 17 straipsnio e dalies 3 punktas.

⁽³⁾ IG akto 11 straipsnis.

VII PRIEDAS

Generalinio advokato pavaduotojo ir tarptautinių reikalų patarėjo Bruce'o Swartzo raštas, JAV teisingumo departamentas

2016 m. vasario 19 d.

Justinui S. Antonipillai,
JAV komercijos departamento
advokatui
1401 Constitution Ave., NW
Vašingtonas, DC 20230

Tedui Deanui,
Tarptautinės prekybos administracijos
sekretoriaus pavaduotojui
1401 Constitution Ave., NW
Vašingtonas, DC 20230

Gerbiami J. Antonipillai ir T. Deanai,

šiam rašte pateikiama trumpa pagrindinių tyrimo priemonių, naudojamų komerciniams duomenims ir kitai įrašų informacijai iš Jungtinių Amerikos Valstijų gauti baudžiamosios teisės arba viešojo intereso (civilinio ir reguliavimo) tikslais, įskaitant šiuose įgaliojimuose nustatytus prieigos apribojimus ⁽¹⁾. Šie teisiniai procesai yra nediskriminuojamojo pobūdžio, nes naudojami informacijai iš Jungtinių Amerikos Valstijų korporacijų, įskaitant bendroves, kurios pagal ES ir JAV „privatumo skydą“ taiko autosertifikavimą, nepaisant duomenų subjekto pilietybės, gauti. Be to, korporacijos, prieš kurias Jungtinėse Amerikos Valstijose pradėti teisiniai procesai, gali juos ginčyti teisme, kaip aprašyta toliau ⁽²⁾.

Kalbant apie valdžios institucijų duomenų areštą, ypač svarbu atkreipti dėmesį į Jungtinių Amerikos Valstijų Konstitucijos Ketvirtąją pataisą, kurioje nustatyta, jog „[a]smenų teisė, kad būtų užtikrinta jų asmens, būsto, dokumentų ir turto apsauga nuo nepagrįstos kratos ar arešto, negali būti pažeidžiama, ir jokie orderiai, išskyrus pakankamu pagrindu pagrįstus orderius, pagrįsti priešaiška arba patvirtinimu, ypač orderiai, kuriuose aprašoma apieškoma vieta ir asmenys arba areštuotini daiktai, negali būti išduodami“. JAV Konstitucijos IV. Kaip nurodė Jungtinių Amerikos Valstijų Aukščiausiasis Teismas byloje *Berger prieš State of New York*, „[p]agrindinis šios Pataisos tikslas, kaip nurodyta įvairiuose Teismo sprendimuose, – apsaugoti asmenų privatumą ir saugumą nuo savavališkų Vyriausybės pareigūnų veiksmų“. 388 U.S. 41, 53 (1967) (*cituojamas sprendimas byloje Camara prieš Mun., San Francisco teismas*, 387 U.S. 523, 528 (1967)). Vidaus baudžiamuosiuose tyrimuose pagal Ketvirtąją pataisą paprastai reikalaujama, kad teisėsaugos pareigūnai, prieš atlikdami kratą, gautų teismo orderį. Žr. *Katz prieš United States*, 389 U.S. 347, 357 (1967). Kai reikalavimas išduoti orderį netaikomas, Vyriausybės veiklai pagal Ketvirtąją pataisą taikomas „pagrįstumo“ testas. Todėl pačia Konstitucija užtikrinama, kad JAV Vyriausybė neturėtų neribotų arba savavališkų įgaliojimų areštuoti privačią informaciją.

Baudžiamosios teisės teisėsaugos institucijos

Federaliniai prokurorai, kurie yra Teisingumo departamento (DOJ) pareigūnai, ir federalinių tyrimų agentai, įskaitant Federalinio tyrimų biuro (FTB) agentus (DOJ teisėsaugos institucija), kurie gali priversti parengti dokumentus ir kitą įrašų

⁽¹⁾ Šioje apžvalgoje neaprašomos nacionalinio saugumo tyrimo priemonės, kurias teisėsaugos institucijos naudoja terorizmo ir kitų nacionalinio saugumo tyrimų srityje, įskaitant nacionalinio saugumo raštus (NSL) dėl tam tikrų įrašų informacijos kredito ataskaitose, finansinių įrašų ir elektroninio abonento ir sandorių įrašų, žr. JAV kodekso 12 antraštinės dalies 3414 straipsnį; JAV kodekso 15 antraštinės dalies 1681u straipsnį; JAV kodekso 15 antraštinės dalies 1681v straipsnį; JAV kodekso 18 antraštinės dalies 2709 straipsnį, o dėl elektroninio stebėjimo, kratos orderių, verslo įrašų ir kitų ryšių duomenų rinkimo pagal Užsienio žvalgybos stebėjimo aktą žr. JAV kodekso 1801 ir kitus straipsnius.

⁽²⁾ Šiame rašte aptariami teisėsaugos ir reguliavimo institucijų įgaliojimai; valstijų teisės pažeidimus tiria valstijos, o bylos dėl pažeidimų nagrinėjamos valstijų teismuose. Valstijų teisėsaugos institucijos išduoda įsakymus ir šaukimus į teismą pagal valstijos teisę iš esmės tokiu pat būdu, kaip aprašyta šiame rašte, tačiau įskaitant galimybę valstijų teisiniam procesui taikyti valstijų konstitucijose nustatytas apsaugos priemones, kurios yra griežtesnės, palyginti su JAV Konstitucija. Valstijų teisėje nustatytos apsaugos priemonės turi būti bent jau lygiavertės JAV Konstitucijoje nustatytoms priemonėms, įskaitant Ketvirtąją pataisą, bet ja neapsiribojant.

informaciją iš korporacijų Jungtinėse Amerikos Valstijose baudžiamojo tyrimo tikslais taikant keletą privalomų teisinių procesų, įskaitant didžiosios žiuri šaukimus, administracinius potvarkius ir kratos orderius, ir gali reikalausti kitų ryšių pagal federalinius baudžiamuosius įgaliojimus bei klausytis pokalbių telefonu ir renkamų numerių registratorių srityje.

Didžiosios žiuri arba šaukimai į teismą. Šaukimai į baudžiamąją bylą naudojami siekiant padėti atlikti tikslingus teisėsaugos institucijų tyrimus. Didžiosios žiuri šaukimas į teismą yra oficialus didžiosios žiuri prašymas (papratai pateikiamas federalinio prokuroro prašymu) padėti atlikti didžiąjai žiuri konkretaus baudžiamojo įstatymo pažeidimo tyrimą. Didžioji žiuri veikia kaip teismo tiriamoji grupė, kurią išrenka teisėjas arba magistratas. Šaukime į teismą gali būti reikalaujama, kad tam tikras asmuo liudytų byloje arba pateiktų verslo įrašus, elektronine forma saugomą informaciją arba kitus materialius įrodymus arba leistų susipažinti su jais. Informacija turi būti susijusi su tyrimu, o šaukimas į teismą negali būti nepagrįstas dėl pernelyg plataus pobūdžio arba dėl to, kad yra neįvykdomas ar sukelia per didelę naštą. Gavėjas gali pateikti prašymą ginčyti šaukimą į teismą šiais pagrindais. Žr. Federalinio baudžiamojo proceso taisyklių 17 taisyklę. Tam tikromis aplinkybėmis teismo šaukimai dėl dokumentų gali būti naudojami po to, kai didžioji žiuri byloje priėmė sprendimą.

Įgaliojimai priimti administracinius potvarkius. Įgaliojimais priimti administracinius potvarkius galima pasinaudoti baudžiamuosiuose arba civiliniuose tyrimuose. Kalbant apie baudžiamąsias bylas, pažymėtina, kad pagal kai kuriuos federalinius įstatymus leidžiama naudoti administracinius potvarkius arba supažindinti su įmonių įrašais, elektronine forma saugoma informacija arba kitais materialiais tyrimo daiktais, susijusiais su sukčiavimu sveikatos srityje, vaiko išnaudojimu, slaptos tarnybos apsauga, kontroliuojamų medžiagų bylomis ir generalinių inspektorių tyrimais, kurie daro poveikį Vyriausybės agentūrom. Jeigu Vyriausybė siekia įvykdyti administracinį potvarkį teisme, administracinio potvarkio gavėjas, kaip ir didžiosios žiuri šaukimo į teismą gavėjas, gali teigti, jog potvarkis nepagrįstas dėl to, kad jis yra pernelyg plataus pobūdžio, neįvykdomas arba sukeliantis per didelę naštą.

Teismo nutartys dėl renkamų numerių registratorių arba spąstų ir sekimo prietaisų. Pagal baudžiamąsias renkamų numerių registratorių arba spąstų ir sekimo prietaisų naudojimo nuostatas teisėsaugos institucija, gavusi patvirtinimą, kad pateikta informacija yra susijusi su atliekamu baudžiamuoju tyrimu, gali gauti teismo nutartį, kad įgytų tikruoju laiku, su turiniu nesusijusius numerių rinkimo, maršruto parinkimo, adresavimo ir signalų informaciją apie telefono numerį arba e. paštą. Žr. JAV kodekso 18 antraštinės dalies 3121–3127 straipsnius. Tokio prietaiso naudojimas arba įdiegimas nesilaikant įstatymo yra federalinis nusikaltimas.

Elektroninių ryšių privatumo aktas (ECPA). Papildomomis taisyklėmis reglamentuojama Vyriausybės prieiga prie abonto informacijos, srauto duomenų ir saugomo ryšių turinio, kuri ISP telefonų bendrovės ir kitos paslaugas teikiančios trečiosios šalys turi pagal ECPA II antraštinę dalį, kuri taip pat vadinama Saugomų ryšių aktu (SCA), JAV kodekso 18 antraštinės dalies 2701–2712 straipsniai. SCA nustatyta įstatymu įtvirtinta privatumo teisių sistema, kuria ribojama teisėsaugos institucijų prieiga prie duomenų, nesusijusių su duomenimis, kurių pagal konstitucinę teisę reikalaujama iš klientų ir interneto paslaugų teikėjo abonentų. SCA nustatyti didesni privatumo apsaugos lygiai, kurie priklauso nuo duomenų rinkimo veiksmų intervencijos. Kalbant apie abonto registracijos informaciją, IP adresus ir susijusias laiko žymas bei sąskaitų informaciją, pažymėtina, kad šiuo klausimu baudžiamosios teisėsaugos institucijos turi kreiptis į teismą. Dėl didžiosios dalies kitos saugomos ir su turiniu nesusijusios informacijos, pvz., e. laiškų pavadinimų, be dalyko pavadinimo teisėsaugos institucijos privalo pateikti teisėjui konkrečius faktus, įrodančius, kad prašoma informacija yra svarbi ir esminė vykdomam baudžiamajam tyrimui. Siekiant gauti saugomą elektroninių ryšių turinį, paprastai baudžiamosios teisės institucijos gauna teisėjo orderį, remdamosi pakankamu pagrindu, jeigu manoma, kad atitinkamas įrodymas prilygsta nusikaltimo įrodymui. SCA taip pat nustatyta civilinė atsakomybė ir baudžiamosios sankcijos.

Teismo orderiai dėl stebėjimo pagal Federalinį slapto pokalbių klausymosi įstatymą. Be to, teisėsaugos institucijos gali tikruoju laiku perimti pokalbius, žodinius arba elektroninius ryšius baudžiamojo tyrimo tikslais pagal federalinį slapto pokalbių pasiklausymo įstatymą. Žr. JAV kodekso 18 antraštinės dalies 2510–2522 straipsnius. Šiais įgaliojimais galima

naudotis tik remiantis teismo nutartimi, kurioje teisėjas, be kita ko, nustato, kad yra pakankamas pagrindas manyti, jog slapto pokalbių pasiklausymas arba elektroninių ryšių perėmimas bus federalinio nusikaltimo įrodymai. Įstatyme nustatyta civilinė atsakomybė ir baudžiamosios sankcijos už slapto pokalbių klausymosi pažeidimus.

Kratos orderis – 41 taisyklė. Teisėsaugos institucijos gali fiziškai apieškoti patalpas Jungtinėse Amerikos Valstijose, kai leidimą tam išduoda teisėjas. Teisėsaugos institucijos, remdamosi „pakankamu pagrindu“, privalo teisėjui įrodyti, kad nusikaltimas buvo padarytas arba gali būti padarytas ir kad su nusikaltimu susiję elementai, tikėtina, gali būti rasti orderyje nurodytoje vietoje. Šis įgaliojimas dažnai naudojamas, kai būtina, kad policija atliktų patalpų apžiūrą dėl pavojaus, kad įrodymai gali būti sunaikinti, jeigu korporacijai įteikiamas šaukimas į teismą arba kitas orderis dėl įrodymų. Žr. JAV Konstitucijos Ketvirtąją pataisą (išsamiau aptarta pirmiau), Federalinių baudžiamojo proceso taisyklių 41 taisyklę. Jeigu orderio dalykas yra pernelyg platus, nepagrįstas arba kitaip netinkamai nustatytas, pagrįstą reikalavimą turinčios šalys gali atmesti bet kokius neteisėtos kratos metu gautus įrodymus. Žr. *Mapp prieš Ohio*, 367 U.S. 643 (1961).

DOJ rekomendacijos ir politika Be šių konstitucinių, įstatymais įtvirtintų ir taisyklėmis pagrįstų apribojimų dėl Vyriausybės prieigos prie duomenų, generalinis prokuroras priėmė gaires, kuriose nustatyti papildomi teisėsaugos institucijų prieigos prie duomenų apribojimai ir kuriose taip pat nustatytos privatumo ir pilietinių laisvių apsaugos priemonės. Pavyzdžiui, Generalinio advokato gairėse dėl Federalinio tyrimų biuro (FTB) vidaus operacijų (2008 m. rugsėjo mėn.) (toliau – AG FBI gairės), skelbiamose adresu <http://www.justice.gov/archive/opa/docs/guidelines.pdf>, nustatytos tyrimo priemonių naudojimo ribos siekiant gauti informaciją, susijusią su federalinių nusikaltimų tyrimais. Šiose gairėse reikalaujama, kad FTB naudotų kuo mažiau intervencines ir ribojančias priemones ir atsižvelgtų į poveikį privatumui, pilietinėms laisvėms ir galimą žalą reputacijai. Be to, jose pažymima, kad „paprastai FTB privalo tyrimus ir kitą veiklą vykdyti teisėtai ir pagrįstai, gerbdamas laisvę ir privatumą ir taip, kad išvengtų nereikalingo įstatymų besilaukiančių žmonių gyvenimo apribojimo.“ Žr. AG FBI gairių 5 punktą. FTB šias gaires įgyvendino FTB vidaus tyrimų ir operacijų gairėse (DIOG), kurios skelbiamos adresu [https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20\(DIOG\)](https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG)), t. y. išsamus vadovas, kuriame nurodomos konkrečios tyrimo priemonių ribos ir gairės, kuriomis užtikrinama, kad pilietinės laisvės ir privatumas būtų užtikrinami kiekviename tyrime. Papildomos taisyklės ir politika, kuria nustatomi federalinių prokurorų tyrimo veiklos apribojimai, išdėstytos **Jungtinių Amerikos Valstijų vadove** (USAM), kuris taip pat skelbiamas internete adresu <http://www.justice.gov/usam/united-states-attorneys-manual>.

Pilietiniai ir reguliavimo įgaliojimai (viešasis interesas)

Civilinei arba reguliavimo (t. y. viešojo intereso pagrindais suteikiamai) prieigai prie duomenų, kuriuos turi Jungtinių Amerikos Valstijų korporacijos, taip pat taikomi griežti apribojimai. Civilinės ir reguliavimo pareigas turinčios agentūros gali priimti korporacijoms skirtus šaukimus į teismą dėl įmonių įrašų, elektroniniu būdu saugomos informacijos ir kitų materialių daiktų. Šios agentūros, vykdydamos savo administracinius arba civilinius įgaliojimus išduoti šaukimą į teismą, turi vadovautis ne tik pagrindiniais įstatymais, bet ir nepriklausoma teismine šaukimų į teismą peržiūra prieš galimą teisminį vykdymą. Žr., pvz., Federalinių civilinio proceso taisyklių 45 taisyklę. Agentūros gali siekti gauti tik su jų reguliavimo įgaliojimais susijusius duomenis. Be to, administracinio potvarkio gavėjas gali ginčyti tą potvarkį teisme pateikdamas įrodymus, kad agentūra neveikė pagal pagrindinius pagrįstumo standartus, kaip aptarta pirmiau.

Bendrovės administracinių agentūrų prašymus dėl duomenų gali ginčyti remdamosi savo specifine pramone ir turimų duomenų rūšimi. Pavyzdžiui, finansų įstaigos gali ginčyti administracinius potvarkius, kuriais siekiama gauti tam tikrų rūšių informaciją, kuria patvirtinami Bankų paslapties akto ir jo įgyvendinimo taisyklių pažeidimai. Žr. JAV kodekso 31 antraštinės dalies 5318 straipsnį, 31 C.F.R. X dalį. Kitos įmonės gali remtis Sąžiningo kredito ataskaitų aktu, žr. JAV kodekso 15 antraštinės dalies 1681b straipsnį arba kitus sektoriaus įstatymus. Netinkamas agentūros šaukimo į teismą įgaliojimų naudojimas gali užtraukti agentūrai atsakomybę arba asmeninę agentūros pareigūnų atsakomybę. Žr., pvz., Teisės į finansinį privatumą aktą, JAV kodekso 12 antraštinės dalies 3401–3422 straipsnius. Todėl Jungtinių Amerikos Valstijų teismai vykdo netinkamų reguliavimo prašymų atranką ir nepriklausomą federalinių agentūrų veiksmų priežiūrą.

Galiausiai bet kokie įstatymais įtvirtinti įgaliojimai, kuriuos administracinės institucijos turi, kad fiziškai areštuotų Jungtinių Amerikos Valstijų įrašus pagal administracinę paiešką, privalo atitikti Ketvirtosios pataisos reikalavimus. Žr. *See prieš City of Seattle*, 387 U.S. 541 (1967).

Išvada

Visa teisėsaugos ir reguliavimo veikla Jungtinėse Amerikos Valstijose turi atitikti taikytiną teisę, įskaitant JAV Konstituciją, įstatymus, taisykles ir reglamentus. Tokia veikla taip pat turi atitikti taikytiną politiką, įskaitant Generalinio advokato rekomendacijas, kuriomis teisėsaugos institucijų veikla reglamentuojama federaliniu lygmeniu. Pirmiau aprašytoje teisinėje sistemoje nustatyti JAV teisėsaugos ir reguliavimo agentūrų apribojimai, kurie taikomi įgyjant informaciją iš Jungtinių Amerikos Valstijų korporacijų, nepaisant to, ar informacija yra susijusi su JAV asmenimis, ar su užsienio šalių piliečiais, be to, šioje sistemoje leidžiama atlikti bet kurio Vyriausybės prašymo dėl pagal šiuos įgaliojimus gautų duomenų peržiūrą.

Pagarbiai

Bruce'as C. Swartzas,

generalinio prokuroro padėjėjas ir patarėjas
tarptautinių reikalų klausimais
