KOMISIJOS ĮGYVENDINIMO SPRENDIMAS (ES) 2023/1795

2023 m. liepos 10 d.

priimtas pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679, dėl tinkamo asmens duomenų apsaugos lygio pagal ES ir JAV duomenų privatumo sistemą

(pranešta dokumentu Nr. C(2023) 4745)

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas) ([1]), ypač į jo 45 straipsnio 3 dalį,

kadangi:

1. ĮVADAS

(1) Reglamentu (ES) 2016/679 ([2]) nustatytos asmens duomenų perdavimo iš Sąjungoje esančių duomenų valdytojų arba duomenų tvarkytojų į trečiąsias valstybes ir tarptautinėms organizacijoms taisyklės, susijusios su tomis duomenų perdavimo operacijomis, kurioms taikomas tas Reglamentas. Tarptautinio duomenų perdavimo taisyklės nustatytos to Reglamento V skyriuje. Nors asmens duomenų srautas į Europos Sąjungai nepriklausančias valstybes ir iš jų yra labai svarbus siekiant plėsti tarpvalstybinę prekybą ir tarptautinį bendradarbiavimą, Sąjungoje užtikrinamas asmens duomenų apsaugos lygis negali sumažėti duomenis perduodant į trečiąsias valstybes arba tarptautines organizacijas ([3]).

(2) Pagal Reglamento (ES) 2016/679 45 straipsnio 3 dalį Komisija, priimdama įgyvendinimo aktą, gali nuspręsti, kad trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių toje trečiojoje valstybėje užtikrina tinkamo lygio apsaugą. Tokiu atveju asmens duomenys į trečiąją valstybę gali būti perduodami nereikalaujant papildomo leidimo, kaip nustatyta Reglamento (ES) 2016/679 45 straipsnio 1 dalyje ir 103 konstatuojamojoje dalyje.

(3) Kaip nurodyta Reglamento (ES) 2016/679 45 straipsnio 2 dalyje, priimant sprendimą dėl tinkamumo turi būti remiamasi išsamia trečiosios valstybės teisinės tvarkos analize, apimančia ir duomenų importuotojams taikomas taisykles, ir apribojimus bei apsaugos priemones, taikomas valdžios institucijoms gaunant galimybę susipažinti su asmens duomenimis. Atlikdama vertinimą Komisija turi nustatyti, ar atitinkama trečioji valstybė garantuoja tokio lygio apsaugą, kuri yra „iš esmės lygiavertė“ Sąjungoje užtikrinamai apsaugai (Reglamento (ES) 2016/679104 konstatuojamoji dalis). Ar taip yra, turi būti vertinama pagal Sąjungos teisės aktus, visų pirma Reglamentą (ES) 2016/679, taip pat Europos Sąjungos Teisingumo Teismo (toliau – Teisingumo Teismas) praktiką ([4]).

([1]) OL L 119, 2016 5 4, p. 1.
([2]) Dėl patogumo VIII priede pateikiamas šiame sprendime vartojamų santrumpų sąrašas.
([3]) Žr. Reglamento (ES) 2016/679101 konstatuojamąją dalį.
([4]) Žr. naujausią Sprendimą *Facebook Ireland ir Schrems* (*Schrems II*), C-311/18, ECLI:EU:C:2020:559.

(4) Kaip Teisingumo Teismas išaiškino savo 2015 m. spalio 6 d. Sprendime *Maximillian Schrems / Data Protection Commissioner* ([5]) (*Schrems*), C-362/14, tam nereikia nustatyti tokio paties apsaugos lygio. Visų pirma, priemonės, kurių siekdama apsaugoti asmens duomenis gali imtis atitinkama trečioji valstybė, gali skirtis nuo Sąjungoje taikomų priemonių, jeigu šios priemonės praktiškai padeda veiksmingai užtikrinti tinkamo lygio apsaugą ([6]). Todėl pagal tinkamumo standartą nėra reikalaujama Sąjungos taisykles atkartoti papunkčiui. Veikiau pagal šį kriterijų turi būti patikrinta, ar visoje užsienio valstybės sistemoje užtikrinamas reikiamas apsaugos lygis – teisių į privatumą esmė, veiksmingas jų įgyvendinimas, priežiūra ir vykdymo užtikrinimas ([7]). Be to, pagal tą sprendimą Komisija, taikydama šį standartą, visų pirma turėtų įvertinti, ar atitinkamos trečiosios valstybės teisinėje sistemoje nustatytos taisyklės, kuriomis siekiama apriboti asmenų, kurių duomenys perduodami iš Sąjungos, pagrindinių teisių apribojimus, kuriuos tos valstybės valstybiniams subjektams būtų leidžiama taikyti siekiant teisėtų tikslų, pvz., nacionalinio saugumo, ir užtikrinama veiksminga teisinė apsauga nuo tokio pobūdžio apribojimų ([8]). Gairių šiuo klausimu pateikiama ir Europos duomenų apsaugos valdybos orientaciniuose tinkamumo kriterijuose, kuriais siekiama išsamiau paaiškinti šį standartą ([9]).

(5) Tokiam pagrindinių teisių į privatumą ir duomenų apsaugą apribojimui taikytiną standartą Teisingumo Teismas išsamiau išaiškino savo 2020 m. liepos 16 d. Sprendime *Data Protection Commissioner / Facebook Ireland Limited ir Maximillian Schrems (Schrems II)*, C-311/18, kuriuo Komisijos įgyvendinimo sprendimas (ES) 2016/1250 ([10]) dėl ankstesnės transatlantinės duomenų srautų reglamentavimo sistemos – ES ir JAV privatumo skydo (toliau – privatumo skydas) – pripažintas negaliojančiu. Teisingumo Teismas nusprendė, kad asmens duomenų apsaugos apribojimai, kurie kyla iš Jungtinių Amerikos Valstijų nacionalinės teisės aktų, susijusių su JAV valdžios institucijų prieiga prie tokių duomenų, perduodamų iš Sąjungos į Jungtines Amerikos Valstijas nacionalinio saugumo tikslais, ir šių institucijų atliekamu jų naudojimu, nėra sureglamentuoti taip, kad atitiktų reikalavimus, iš esmės lygiaverčius Sąjungos teisėje nustatytiems reikalavimams, kiek tai susiję su tokių teisės į duomenų apsaugą apribojimų būtinumu ir proporcingumu ([11]). Teisingumo Teismas taip pat nusprendė, kad nesuteikiama teisių gynimo priemonė institucijoje, kurioje asmenims, kurių duomenys buvo perduoti į Jungtines Amerikos Valstijas, būtų suteiktos garantijos, iš esmės lygiavertės toms, kurių reikalaujama pagal Chartijos 47 straipsnį dėl teisės į veiksmingą teisinę gynybą ([12]).

(6) Po to, kai buvo priimtas Sprendimas *Schrems II*, Komisija pradėjo derybas su JAV vyriausybe dėl galimo naujo sprendimo dėl tinkamumo, kuris atitiktų Reglamento (ES) 2016/679 45 straipsnio 2 dalies reikalavimus, kaip juos išaiškino Teisingumo Teismas. Po šių diskusijų 2022 m. spalio 7 d. Jungtinės Amerikos Valstijos priėmė Vykdomąjį potvarkį Nr. 14086 dėl JAV signalų žvalgybos veiklos apsaugos priemonių griežtinimo (toliau – VP 14086), o jį papildo JAV generalinio prokuroro paskelbtas Reglamentas dėl Duomenų apsaugos apeliacinio teismo (toliau – GP reglamentas) ([13]). Be to, atnaujinta komerciniams subjektams, tvarkantiems iš Sąjungos pagal šį Sprendimą perduodamus duomenis, taikoma sistema – ES ir JAV duomenų privatumo sistema (toliau – ES ir JAV DPS arba DPS).

(7) Komisija atidžiai išnagrinėjo JAV teisę ir praktiką, įskaitant VP 14086 ir GP reglamentą. Remdamasi 9-200 konstatuojamosiose dalyse išdėstytomis faktinėmis aplinkybėmis, Komisija daro išvadą, kad Jungtinės Amerikos Valstijos užtikrina tinkamą asmens duomenų, pagal ES ir JAV DPS Sąjungos ([14]) duomenų valdytojų arba duomenų tvarkytojų perduodamų Jungtinių Amerikos Valstijų sertifikuotoms organizacijoms, apsaugos lygį.

([5]) Sprendimas *Maximilian Schrems / Data Protection Commissioner* (*Schrems*), C-362/14, ECLI:EU:C:2015:650, 73 punktas.

([6]) Sprendimas *Schrems*, 74 punktas.

([7]) Žr. 2017 m. sausio 10 d. Komisijos komunikato Europos Parlamentui ir Tarybai „Keitimasis asmens duomenimis ir jų apsauga globalizuotame pasaulyje“ (COM(2017) 7) 3.1 skirsnį, p. 6–7.

([8]) Sprendimas *Schrems*, 88 ir 89 punktai.

([9]) Europos duomenų apsaugos valdybos darbinis dokumentas „Tinkamumo pavyzdžiai“ (WP 254, 1-oji peržiūrėta versija), pateikiamas adresu https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

([10]) 2016 m. liepos 12 d. Komisijos įgyvendinimo sprendimas (ES) 2016/1250 dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB (OL L 207, 2016 8 1, p. 1.).

([11]) Sprendimas *Schrems II*, 185 punktas.

([12]) Sprendimas *Schrems II*, 197 punktas.

([13]) Federalinių reglamentų kodekso 28 antraštinės dalies 302 dalis.

([14]) Šis sprendimas svarbus EEE. Europos ekonominės erdvės susitarime (toliau – EEE susitarimas) nustatyta, kad Europos Sąjungos vidaus rinkos taisyklės galioja ir trijose EEE valstybėse: Islandijoje, Lichtenšteine ir Norvegijoje. 2018 m. liepos 6 d. EEE jungtinis komitetas priėmė Jungtinio komiteto sprendimą, kuriuo Reglamentas (ES) 2016/679 buvo įtrauktas į EEE susitarimo XI priedą. Šis sprendimas įsigaliojo 2018 m. liepos 20 d. Todėl ta sutartis apima minėtąjį Reglamentą. Todėl šiame sprendime nuorodos į ES ir ES valstybes nares turėtų būti suprantamos kaip apimančios ir EEE valstybes.

(8) Šiuo sprendimu nustatoma, kad Sąjungoje esantys ([15]) duomenų valdytojai ir duomenų tvarkytojai gali perduoti asmens duomenis sertifikuotoms organizacijoms Jungtinėse Amerikos Valstijose be papildomo leidimo. Sprendimas nedaro poveikio Reglamento (ES) 2016/679 tiesioginiam taikymui tokioms organizacijoms, kai tenkinamos to Reglamento teritorinės taikymo srities sąlygos, nustatytos to Reglamento 3 straipsnyje.

2. ES IR JAV DUOMENŲ PRIVATUMO SISTEMA

2.1. Subjektinė ir materialinė taikymo sritis

2.1.1. *Sertifikuotos organizacijos*

(9) ES ir JAV DPS yra pagrįsta sertifikavimo sistema, pagal kurią JAV organizacijos įsipareigoja laikytis tam tikrų privatumo principų – ES ir JAV duomenų privatumo sistemos principų, įskaitant papildomus principus (toliau kartu – Principai), – kuriuos paskelbė JAV Prekybos departamentas ir kurie yra pateikti šio sprendimo I priede ([16]). Kad atitiktų sertifikavimo pagal ES ir JAV DPS reikalavimus, organizacijos atžvilgiu turi būti galima naudotis Federalinės prekybos komisijos (FPK) arba JAV Transporto departamento tyrimo ir vykdymo užtikrinimo įgaliojimais ([17]). Principai taikomi iš karto nuo sertifikavimo momento. Kaip išsamiau paaiškinta 48–52 konstatuojamosiose dalyse, ES ir JAV DPS organizacijos privalo kasmet iš naujo atlikdamos sertifikavimą patvirtinti, kad laikosi Principų ([18]).

2.1.2. *Asmens duomenų apibrėžtis ir duomenų valdytojo ir atstovo sąvokos*

(10) Pagal ES ir JAV DPS užtikrinama apsauga taikoma visiems asmens duomenims, kurie iš Sąjungos perduodami JAV organizacijoms, Prekybos departamentui patvirtinusioms, kad laikosi Principų, išskyrus duomenis, kurie yra renkami siekiant paskelbti, transliuoti ar kitaip viešai perduoti žurnalistinę medžiagą ir informaciją, esančią anksčiau paskelbtoje medžiagoje, platinamoje iš žiniasklaidos archyvų ([19]). Todėl tokia informacija negali būti perduodama remiantis ES ir JAV DPS.

(11) Principuose asmens duomenys ir (arba) asmeninė informacija apibrėžiami taip pat, kaip ir Reglamente (ES) 2016/679, t. y. kaip „į BDAR taikymo sritį patenkantys duomenys apie asmenį, kurio tapatybė nustatyta arba gali būti nustatyta, kuriuos organizacija Jungtinėse Amerikos Valstijose gauna iš ES ir kurie yra įrašyti bet kokia forma“ ([20]). Atitinkamai jie taip pat apima pseudoniminius (arba raktu užkoduotus) mokslinių tyrimų duomenis (įskaitant atvejus, kai šifro raktu su gaunančiąja JAV organizacija nesidalijama) ([21]). Be to, tvarkymo sąvoka apibrėžiama taip – „automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, saugojimas, pritaikymas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas ar platinimas, taip pat ištrynimas arba sunaikinimas“ ([22]).

(12) ES ir JAV DPS taikoma JAV organizacijoms, laikomoms duomenų valdytojais (t. y. asmuo ar organizacija, kuris (-i) vienas (-a) ar drauge su kitais nustato asmens duomenų tvarkymo tikslus ir priemones) ([23]) arba duomenų tvarkytojais (t. y. duomenų valdytojo vardu veikiantis atstovas) ([24]). JAV duomenų tvarkytojai pagal sutartį privalo veikti tik laikydamiesi ES duomenų valdytojo nurodymų ir padėti jam atsakyti asmenims, kurie naudojasi savo

([15]) Šis sprendimas nedaro poveikio Reglamento (ES) 2016/679 reikalavimams, taikomiems duomenis perduodantiems Sąjungos subjektams (duomenų valdytojams ir duomenų tvarkytojams), pvz., dėl tikslo apribojimo, duomenų kiekio mažinimo, skaidrumo ir duomenų saugumo (taip pat žr. Reglamento (ES) 2016/679 44 straipsnį).

([16]) Šiuo klausimu žr. Sprendimo *Schrems* 81 punktą, kuriame Teisingumo Teismas patvirtino, kad įsipareigojimo sistema gali užtikrinti tinkamą apsaugos lygį.

([17]) I priedo I skirsnio 2 dalis. FPK turi plačią jurisdikciją prekybos srityje, tačiau yra išimčių, pvz., susijusių su bankais, oro vežėjais, draudimo bendrovėmis ir bendra telekomunikacijų paslaugų teikėjų vežimo veikla (nors 2018 m. vasario 26 d. JAV Devintosios apygardos apeliacinio teismo sprendimu byloje *FTC / AT&T* patvirtinta, kad FPK jurisdikcija apima tokių subjektų vežėjų veiklą, kuri nėra bendra). Taip pat žr. IV priedo 2 išnašą. Transporto departamentas yra kompetentingas užtikrinti, kad oro vežėjai ir bilietų pardavėjai laikytųsi reikalavimų (oro transporto srityje); žr. V priedo A skirsnį.

([18]) I priedo III skirsnio 6 dalis.

([19]) I priedo III skirsnio 2 dalis.

([20]) I priedo I skirsnio 8 dalies a punktas.

([21]) I priedo III skirsnio 14 dalies g punktas.

([22]) I priedo I skirsnio 8 dalies b punktas.

([23]) I priedo I skirsnio 8 dalies c punktas.

([24]) Žr., pvz., I priedo II skirsnio 2 dalies b punktą, taip pat II skirsnio 3 dalies b punktą ir 7 dalies d punktą, iš kurių aišku, kad atstovai veikia duomenų valdytojo vardu, laikydamiesi jo nurodymų ir konkrečių sutartinių įsipareigojimų.

teisėmis pagal Principus ([25]). Be to, duomenų tvarkymo subrangos atveju duomenų tvarkytojas privalo sudaryti sutartį su duomenų tvarkymo subrangovu, kuria garantuojamas toks pat apsaugos lygis, koks užtikrinamas pagal Principus, ir imtis priemonių, kad tokia sutartis būtų tinkamai vykdoma ([26]).

2.2. **ES ir JAV duomenų privatumo sistemos principai**

2.2.1. ***Tikslo apribojimas ir pasirinkimas***

(13) Asmens duomenys turėtų būti tvarkomi teisėtai ir sąžiningai. Jie turėtų būti renkami konkrečiu tikslu ir vėliau naudojami tik tiek, kiek tai nėra nesuderinama su jų tvarkymo tikslu.

(14) Pagal ES ir JAV DPS tai užtikrinama įvairiais Principais. Pirma, pagal *duomenų vientisumo ir tikslo apribojimo principą*, panašiai kaip pagal Reglamento (ES) 2016/679 5 straipsnio 1 dalies b punktą, organizacija negali tvarkyti asmens duomenų tokiu būdu, kuris yra nesuderinamas su tikslu, kuriuo jie iš pradžių buvo surinkti arba duomenų subjektas vėliau leido juos tvarkyti ([27]).

(15) Antra, prieš naudodama asmens duomenis nauju (pakeistu) tikslu, kuris yra iš esmės kitas, bet vis vien suderinamas su pradiniu tikslu, arba atskleisti juos trečiajai šaliai, organizacija pagal *pasirinkimo principą* ([28]) turi suteikti duomenų subjektams galimybę nesutikti (atsisakyti sutikti), taikydama aiškų, suprantamą ir lengvai prieinamą mechanizmą. Svarbu pažymėti, kad šis principas nėra viršesnis už aiškų draudimą tvarkyti duomenis nesuderinamais tikslais ([29]).

([25]) I priedo III skirsnio 10 dalies a punktas. Taip pat žr. gaires, kurias Prekybos departamentas parengė konsultuodamasis su Europos duomenų apsaugos valdyba pagal privatumo skydą ir kuriose paaiškintos JAV duomenų tvarkytojų, pagal tą sistemą gaunančių asmens duomenis iš Sąjungos, prievolės. Kadangi šios taisyklės nepasikeitė, šios gairės ir (arba) DUK tebėra aktualūs pagal ES ir JAV DPS (https://www.privacyshield.gov/article?id=Processing-FAQs).

([26]) I priedo II skirsnio 3 dalies b punktas.

([27]) I priedo II skirsnio 5 dalies a punktas. Suderinami tikslai gali apimti auditą, sukčiavimo prevenciją arba kitus tikslus, atitinkančius racionalaus asmens lūkesčius, atsižvelgiant į duomenų rinkimo aplinkybes (žr. I priedo 6 išnašą).

([28]) I priedo II skirsnio 2 dalies a punktas. Tai netaikoma, kai organizacija pateikia asmens duomenis duomenų tvarkytojui, veikiančiam jos vardu ir pagal jos nurodymus (I priedo II skirsnio 2 dalies b punktas). Vis dėlto šiuo atveju organizacija turi būti sudariusi sutartį ir užtikrinti, kad būtų laikomasi *atskaitomybės už tolesnį duomenų perdavimą principo*, kaip išsamiau aprašyta 43 konstatuojamojoje dalyje. Be to, *pasirinkimo principas* (taip pat *pranešimo principas*) gali būti apribotas, kai asmens duomenys tvarkomi atliekant išsamų patikrinimą (dėl galimo susijungimo ar perėmimo) arba auditą tokiu mastu ir tol, kol tai būtina vykdant teisės aktų ar viešojo intereso reikalavimus, arba tokiu mastu ir tol, kol taikant šiuos Principus būtų pažeisti teisėti organizacijos interesai konkrečiomis išsamaus patikrinimo tyrimų ar audito aplinkybėmis (I priedo III skirsnio 4 dalis). Pagal 15 papildomą principą (I priedo III skirsnio 15 dalies a ir b punktai) taip pat numatyta *pasirinkimo* principo (be to, *pranešimo* ir *atskaitomybės už tolesnį duomenų perdavimą* principų) išimtis, taikoma iš viešai prieinamų šaltinių gautiems asmens duomenims (išskyrus atvejus, kai ES duomenų eksportuotojas nurodo, kad informacijai taikomi apribojimai, dėl kurių tie principai turi būti taikomi) arba iš įrašų, su kuriais visuomenė apskritai gali viešai susipažinti, gautiems asmens duomenims (jei jie nėra derinami su neviešų įrašų informacija ir yra laikomasi susipažinimo su informacija sąlygų). Be to, pagal 14 papildomą principą (I priedo III skirsnio 14 dalies f punktas) numatyta *pasirinkimo* principo (taip pat *pranešimo* ir *atskaitomybės už tolesnį duomenų perdavimą* principų) išimtis, taikoma farmacijos arba medicinos priemonių bendrovei tvarkant asmens duomenis produktų saugos ir veiksmingumo stebėsenos tikslais tiek, kiek laikantis Principų nepavyksta laikytis reguliavimo reikalavimų.

([29]) Tai taikoma visiems pagal ES ir JAV DPS perduodamiems duomenims, įskaitant duomenis, surinktus darbo santykių aplinkybėmis. Nors sertifikuota JAV organizacija iš esmės gali naudoti žmogiškųjų išteklių duomenis kitais, su įdarbinimu nesusijusiais tikslais (pvz., tam tikriems rinkodaros pranešimams), ji privalo paisyti draudimo tvarkyti duomenis nesuderinamais tikslais, be to, gali tai daryti tik laikydamasi *pranešimo* ir *pasirinkimo* principų. Išimtiniais atvejais organizacija gali naudoti asmens duomenis papildomu suderinamu tikslu *nepranešdama* ir nesuteikdama galimybės *rinktis*, tačiau tik tokiu mastu ir tol, kol tai būtina, kad nebūtų sumažintos organizacijos galimybės paaukštinti pareigas, skirti į pareigas ar priimti kitus panašius darbo santykių sprendimus (žr. I priedo III skirsnio 9 dalies b punkto iv papunktį). Draudimas JAV organizacijai imtis bet kokių baudžiamųjų veiksmų prieš darbuotoją, kuris pasinaudoja tokia pasirinkimo teise, įskaitant bet kokį įsidarbinimo galimybių ribojimą, padės užtikrinti, kad, nepaisant subordinacijos santykio ir būdingos priklausomybės, darbuotojas nejaus spaudimo, todėl iš tikrųjų galės laisvai pasirinkti. Žr. I priedo III skirsnio 9 dalies b punkto i papunktį.

2.2.2. ***Specialių kategorijų asmens duomenų tvarkymas***

(16) Tvarkant specialių kategorijų duomenis turėtų būti taikomos konkrečios apsaugos priemonės.

(17) Laikantis *pasirinkimo principo*, tvarkant neskelbtiną informaciją, t. y. asmens duomenis apie sveikatos būklę, rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, narystę profesinėse sąjungose, informaciją apie asmens lytinį gyvenimą arba bet kokią kitą iš trečiosios šalies gautą informaciją, kurią ta šalis laiko neskelbtina ir tvarko kaip neskelbtiną, taikomos konkrečios apsaugos priemonės ([30]). Tai reiškia, kad visi duomenys, kurie laikomi neskelbtinais pagal Sąjungos duomenų apsaugos teisės aktus (įskaitant duomenis apie seksualinę orientaciją, genetinius duomenis ir biometrinius duomenis), sertifikuotų organizacijų bus laikomi neskelbtinais ir pagal ES ir JAV DPS.

(18) Paprastai organizacijos turi gauti aiškų asmens sutikimą (t. y. pasirinktą sutikimą), kad neskelbtina informacija būtų naudojama kitais tikslais nei tie, kuriais ta informacija iš pradžių buvo surinkta ar vėliau asmuo ją leido naudoti (pasirinkęs sutikimą), arba atskleidžiama trečiosioms šalims ([31]).

(19) Tokio sutikimo nereikia tik tam tikromis aplinkybėmis, kurios yra panašios į Sąjungos duomenų apsaugos teisės aktuose numatytas panašias išimtis, pvz., kai neskelbtini duomenys tvarkomi siekiant apsaugoti asmens gyvybinį interesą, duomenis tvarkyti būtina pareiškiant teisinius reikalavimus arba duomenis tvarkyti reikia vykdant sveikatos priežiūrą ar siekiant nustatyti diagnozę ([32]).

2.2.3. ***Duomenų tikslumas, jų kiekio mažinimas ir saugumas***

(20) Duomenys turėtų būti tikslūs ir, jei reikia, atnaujinami. Duomenys taip pat turi būti tinkami, susiję ir neperteklinai atsižvelgiant į jų tvarkymo tikslus ir iš esmės saugomi ne ilgiau, nei būtina atsižvelgiant į asmens duomenų tvarkymo tikslus.

(21) Pagal *duomenų vientisumo ir tikslo apribojimo principą* ([33]) asmens duomenys turi būti susiję tik su tuo, kas yra aktualu duomenų tvarkymo tikslu. Be to, tiek, kiek būtina tvarkymo tikslais, organizacijos privalo imtis pagrįstų priemonių užtikrinti, kad asmens duomenys patikimai atitiktų numatomą jų naudojimo paskirtį, būtų tikslūs, išsamūs ir naujausi.

(22) Be to, asmeninė informacija tokia forma, kokia nustatoma asmens tapatybė arba sudaromos sąlygos nustatyti asmens tapatybę (t. y. asmens duomenų forma) ([34]), gali būti saugoma tik tol, kol yra naudojama tikslui (-ams), dėl kurio (-ių) iš pradžių buvo surinkta arba vėliau asmuo leido ją naudoti pagal *pasirinkimo principą*. Ši prievolė neužkerta kelio organizacijoms toliau tvarkyti asmeninę informaciją ilgiau, bet tik tol ir tokiu mastu, kokiu toks tvarkymas pagrįstai padeda siekti vieno iš šių konkrečių tikslų, panašių į Sąjungos duomenų apsaugos teisės aktuose numatytas panašias išimtis: archyvavimo dėl viešojo intereso, žurnalistikos, literatūros ir meno, mokslinių ir istorinių tyrimų ir statistinės analizės ([35]). Kai asmens duomenys saugomi vienu iš šių tikslų, jų tvarkymui taikomos pagal Principus nustatytos apsaugos priemonės ([36]).

(23) Asmens duomenys taip pat turėtų būti tvarkomi taip, kad būtų užtikrintas jų saugumas, įskaitant apsaugą nuo neleidžiamo ar neteisėto tvarkymo ir netyčinio praradimo, sunaikinimo ar sugadinimo. Todėl duomenų valdytojai ir duomenų tvarkytojai turėtų imtis tinkamų techninių ar organizacinių priemonių, kad apsaugotų asmens duomenis nuo galimų grėsmių. Šios priemonės turėtų būti vertinamos atsižvelgiant į techninių galimybių išsivystymo lygį, susijusias sąnaudas ir duomenų tvarkymo pobūdį, aprėptį, aplinkybes ir tikslus, taip pat į asmenų teisėms kylančius pavojus.

([30]) I priedo II skirsnio 2 dalies c punktas.
([31]) I priedo II skirsnio 2 dalies c punktas.
([32]) I priedo III skirsnio 1 dalis.
([33]) I priedo II skirsnio 5 dalis.
([34]) Žr. I priedo 7 išnašą, kurioje paaiškinama, kad laikoma, jog asmens tapatybę galima nustatyti, jeigu atsižvelgiant į tapatybės nustatymo priemones, kurios, kaip pagrįstai galima tikėtis, veikiausiai bus naudojamos (be kita ko, atsižvelgiant į tapatybės nustatymo sąnaudas ir reikiamą laiką, taip pat į duomenų tvarkymo metu prieinamas technologijas), organizacija arba trečioji šalis pagrįstai galėtų nustatyti to asmens tapatybę.
([35]) I priedo II skirsnio 5 dalies b punktas.
([36]) *Ten pat*.

(24) Pagal ES ir JAV DPS tai užtikrinama *saugumo principu*, pagal kurį, panašiai kaip pagal Reglamento (ES) 2016/679 32 straipsnį, reikalaujama imtis pagrįstų ir tinkamų saugumo priemonių, atsižvelgiant į tvarkant duomenis kylančią riziką ir duomenų pobūdį ([37]).

2.2.4. ***Skaidrumas***

(25) Duomenų subjektai turėtų būti informuoti apie pagrindinius jų asmens duomenų tvarkymo aspektus.

(26) Tai užtikrinama taikant *pranešimo principą* ([38]), pagal kurį, panašiai kaip laikantis skaidrumo reikalavimų pagal Reglamentą (ES) 2016/679, reikalaujama, kad organizacijos informuotų duomenų subjektus apie, *inter alia*, i) organizacijos dalyvavimą DPS, ii) renkamų duomenų rūšį, iii) duomenų tvarkymo tikslą, iv) trečiųjų šalių, kurioms asmens duomenys gali būti atskleisti, tipą ar tapatybę ir tokio atskleidimo tikslus, v) jų asmens teises, vi) kreipimosi į organizaciją būdus, taip pat vii) galimus teisių gynimo būdus.

(27) Toks pranešimas turi būti pateikiamas aiškia ir suprantama kalba, kai asmenų pirmą kartą prašoma pateikti asmens duomenis arba kuo greičiau po to, tačiau bet kuriuo atveju prieš naudojant duomenis iš esmės kitu (bet vis vien suderinamu) tikslu nei tas, kuriuo jie buvo surinkti, arba prieš juos atskleidžiant trečiajai šaliai ([39]).

(28) Be to, organizacijos privalo viešai paskelbti Principus atitinkančią savo privatumo politiką (arba, žmogiškųjų išteklių duomenų atveju, užtikrinti, kad ji būtų lengvai prieinama atitinkamiems asmenims) ir pateikti nuorodas į Prekybos departamento interneto svetainę (kurioje pateikiama išsamesnės informacijos apie sertifikavimą, duomenų subjektų teises ir galimus teisių gynimo mechanizmus), Duomenų privatumo sistemos sąrašą (DPS sąrašą), kuriame nurodytos dalyvaujančios organizacijos, ir atitinkamo alternatyvaus ginčų sprendimo paslaugų teikėjo interneto svetainę ([40]).

2.2.5. ***Asmens teisės***

(29) Duomenų subjektai turėtų turėti tam tikras teises, kurias duomenų valdytojui arba duomenų tvarkytojui gali būti nurodyta įgyvendinti, visų pirma teisę susipažinti su duomenimis, teisę nesutikti su duomenų tvarkymu ir teisę ištaisyti arba ištrinti duomenis.

(30) Pagal ES ir JAV DPS *susipažinimo su duomenimis principą* ([41]) tokios teisės asmenims suteikiamos. Visų pirma duomenų subjektai turi teisę be pagrindimo gauti organizacijos patvirtinimą, ar ji tvarko su jais susijusius asmens duomenis, gauti tuos duomenis ir gauti informacijos apie duomenų tvarkymo tikslą, tvarkomų asmens duomenų kategorijas ir duomenų gavėjus (jų kategorijas), kuriems atskleidžiami duomenys ([42]). Organizacijos privalo atsakyti į prašymus leisti susipažinti su duomenimis per pagrįstą laikotarpį ([43]). Organizacija gali nustatyti pagrįstas ribas, kiek kartų per

([37]) I priedo II skirsnio 4 dalies a punktas. Be to, dėl žmogiškųjų išteklių duomenų ES ir JAV DPS reikalaujama, kad darbdaviai atsižvelgtų į darbuotojų privatumo pageidavimus apribodami galimybę susipažinti su asmens duomenimis, nuasmenindami tam tikrus duomenis arba priskirdami kodus ar pseudonimus (I priedo III skirsnio 9 dalies b punkto iii papunktis).

([38]) I priedo II skirsnio 1 dalis.

([39]) I priedo II skirsnio 1 dalies b punktas. Pagal 14 papildomą principą (I priedo III skirsnio 14 dalies b ir c punktai) nustatytos konkrečios asmens duomenų tvarkymo vykdant medicininius mokslinius tyrimus ir klinikinius tyrimus nuostatos. Visų pirma pagal šį principą organizacijoms leidžiama tvarkyti klinikinių tyrimų duomenis net asmeniui pasitraukus iš tyrimo, jei tai buvo aiškiai nurodyta pranešime, pateiktame tuo metu, kai asmuo sutiko dalyvauti. Panašiai, gavusi asmens duomenis medicininių mokslinių tyrimų tikslais, ES ir JAV DPS organizacija juos gali naudoti tik naujai mokslinių tyrimų veiklai, laikydamasi *pranešimo* ir *pasirinkimo principų*. Šiuo atveju pranešime asmeniui iš esmės turėtų būti pateikta informacija apie bet kokį būsimą konkretų duomenų naudojimą (pvz., susijusius tyrimus). Jeigu iš pat pradžių įtraukti visų būsimų duomenų naudojimo atvejų neįmanoma (nes naujai naudoti duomenis moksliniams tyrimams gali prireikti dėl naujų įžvalgų arba medicinos ir (arba) mokslinių tyrimų pažangos), turi būti pateiktas paaiškinimas, kad duomenys ateityje gali būti naudojami nenumatytoje medicinos ir farmacijos mokslinių tyrimų veikloje. Jeigu toks tolesnis naudojimas nesuderinamas su bendraisiais mokslinių tyrimų tikslais, kuriais duomenys buvo surinkti (t. y., jeigu naujas tikslas, kuris yra iš esmės kitas, bet vis vien suderinamas su pradiniu tikslu, žr. 14 ir 15 konstatuojamąsias dalis), reikia gauti naują sutikimą (t. y. pasirinktą sutikimą). Taip pat žr. 28 išnašoje apibūdintus konkrečius *pranešimo* principo apribojimus ir (arba) išimtis.

([40]) I priedo III skirsnio 6 dalies d punktas.

([41]) Taip pat žr. papildomą susipažinimo su duomenimis principą (I priedo III skirsnio 8 dalis).

([42]) I priedo III skirsnio 8 dalies a punkto i–ii papunkčiai.

([43]) I priedo III skirsnio 8 dalies i punktas.

tam tikrą laikotarpį patenkins konkretaus asmens prašymus leisti susipažinti su duomenimis, ir gali imti ne pernelyg didelį mokestį, jeigu, pvz., prašymai yra akivaizdžiai pertekliniai, visų pirma dėl to, kad yra kartotiniai ([44]).

(31) Teisė susipažinti su duomenimis gali būti ribojama tik išimtinėmis aplinkybėmis, panašiomis į numatytąsias pagal Sąjungos duomenų apsaugos teisę, visų pirma tais atvejais, kai būtų pažeistos kitų asmenų teisėtos teisės; kai konkrečiu atveju susiklosčiusiomis aplinkybėmis galimybės susipažinti su duomenimis suteikimo našta ar išlaidos būtų neproporcingos, palyginti su asmens privatumui kylančia rizika (nors išlaidos ir našta nėra lemiami veiksniai nustatant, ar suteikti galimybę susipažinti su duomenimis yra pagrįsta); tiek, kiek atskleidus tokią informaciją veikiausiai kiltų sunkumų apsaugoti svarbius priešingus viešuosius interesus, pvz., nacionalinio saugumo, visuomenės saugumo ar gynybos; informacija apima konfidencialią komercinę informaciją; informacija tvarkoma tik mokslinių tyrimų ar statistikos tikslais ([45]). Bet koks šios teisės nesuteikimas arba apribojimas turi būti būtinas ir tinkamai pagrįstas, o pareiga įrodyti, kad šie reikalavimai yra įvykdyti, šiuo atveju tenka organizacijai ([46]). Atlikdama šį vertinimą organizacija visų pirma turi atsižvelgti į asmens interesus ([47]). Jeigu įmanoma informaciją atskirti nuo kitų duomenų, kuriems taikomas apribojimas, organizacija turi pašalinti saugomą informaciją ir atskleisti likusią informaciją ([48]).

(32) Be to, duomenų subjektai turi teisę reikalauti ištaisyti ar pakeisti netikslius duomenis ir reikalauti ištrinti duomenis, kurie buvo tvarkomi pažeidžiant Principus ([49]). Be to, kaip paaiškinta 15 konstatuojamojoje dalyje, asmenys turi teisę nesutikti ar atsisakyti sutikti, kad jų duomenys būtų tvarkomi iš esmės kitais (bet suderinamais) tikslais nei tie, kuriais duomenys buvo surinkti, ir kad jų duomenys būtų atskleisti trečiosioms šalims. Kai asmens duomenys naudojami tiesioginės rinkodaros tikslais, asmenys turi bendrą teisę bet kuriuo metu atsisakyti sutikti, kad duomenys būtų tvarkomi ([50]).

(33) Duomenų subjektui poveikį darančių tik automatizuotu asmens duomenų tvarkymu grindžiamų sprendimų klausimui Principai konkrečiai netaikomi. Tačiau Sąjungoje surinktų asmens duomenų atveju bet kokį automatizuotu duomenų tvarkymu grindžiamą sprendimą paprastai priima duomenų valdytojas Sąjungoje (turintis tiesioginį ryšį su atitinkamu duomenų subjektu), todėl jų tvarkymui tiesiogiai taikomas Reglamentas (ES) 2016/679 ([51]). Tai apima duomenų perdavimo atvejus, kai duomenis tvarko užsienio valstybės (pvz., JAV) verslo subjektas, veikiantis kaip Sąjungos duomenų valdytojo atstovas (duomenų tvarkytojas) (arba kaip duomenų tvarkymo subrangovas, veikiantis Sąjungos duomenų tvarkytojo, gavusio duomenis iš juos surinkusio Sąjungos duomenų valdytojo, vardu), todėl šiuo pagrindu sprendimą priima tas duomenų valdytojas.

(34) Tai patvirtinta atliekant antrą metinę privatumo skydo veikimo peržiūrą 2018 m. Komisijos užsakytu tyrimu ([52]), kuriame padaryta išvada, kad tuo metu nebuvo įrodymų, jog privatumo skydo organizacijos įprastai automatizuotai priimtų sprendimus remdamosi pagal privatumo skydo sistemą perduotais asmens duomenimis.

([44]) I priedo III skirsnio 8 dalies f punkto i–ii papunkčiai ir g punktas.
([45]) I priedo III skirsnio 4 dalis, 8 dalies b, c ir e punktai, 14 dalies e ir f punktai ir 15 dalies d punktas.
([46]) I priedo III skirsnio 8 dalies e punkto ii papunktis. Organizacija privalo informuoti asmenį apie nesutikimo ir (arba) apribojimo priežastis ir nurodyti kontaktinį asmenį tolesnėms užklausoms pateikti (III skirsnio 8 dalies a punkto iii papunktis).
([47]) I priedo III skirsnio 8 dalies a punkto ii–iii papunkčiai.
([48]) I priedo III skirsnio 8 dalies a punkto i papunktis.
([49]) I priedo II skirsnio 6 dalis ir III skirsnio 8 dalies a punkto i papunktis.
([50]) I priedo III skirsnio 8 dalies 12 punktas.
([51]) Vis dėlto išskirtiniu atveju, kai JAV organizacija turi tiesioginį ryšį su Sąjungos duomenų subjektu, taip veikiausiai yra dėl to, kad ji tam asmeniui Sąjungoje siūlė prekes ar paslaugas arba stebėjo jo elgesį. Tokiu atveju JAV organizacijai pačiai bus taikomas Reglamentas (ES) 2016/679 (3 straipsnio 2 dalis), todėl ji turės tiesiogiai laikytis ES duomenų apsaugos teisės nuostatų.
([52]) SWD(2018) 497 *final*, 4.1.5 skirsnis. Tyrime daugiausia nagrinėta i) kokiu mastu JAV esančios privatumo skydo organizacijos priima asmenims poveikį darančius sprendimus, grindžiamus automatizuotu pagal privatumo skydo sistemą iš ES bendrovių perduotų asmens duomenų tvarkymu, taip pat ii) JAV federalinėje teisėje numatytos apsaugos priemonės, taikomos asmenims tokiose situacijose, ir sąlygos, kuriomis tos apsaugos priemonės taikomos.

(35) Bet kuriuo atveju srityse, kuriose bendrovės veikiausiai naudos automatizuoto asmens duomenų tvarkymo priemones, kad priimtų asmeniui poveikį darančius sprendimus (pvz., paskolų, hipotekos garantijų, užimtumo, būsto ir draudimo srityse), galioja JAV teisėje nustatytos konkrečios apsaugos nuo neigiamų sprendimų priemonės ([53]). Tuose teisės aktuose paprastai nustatyta, kad asmenys turi teisę būti informuoti apie konkrečias priimto sprendimo priežastis (pvz., atmetus paskolos prašymą), kad galėtų ginčyti neišsamią arba netikslią informaciją (taip pat remtis neteisėtumo aplinkybėmis) ir siekti apginti savo teises. Vartojimo paskolų srityje Sąžiningo kredito informacijos teikimo akte (FCRA) ir Lygių galimybių gauti kreditą akte (ECOA) nustatytomis apsaugos priemonėmis vartotojams suteikiama tam tikra teisė gauti paaiškinimą ir teisė ginčyti sprendimą. Šie aktai aktualūs įvairiose srityse, be kita ko, paskolų, užimtumo, būsto ir draudimo. Be to, tam tikrais kovos su diskriminacija teisės aktais, pvz., Civilinių teisių akto VII antraštine dalimi ir Sąžiningo apsirūpinimo būstu aktu, asmenims suteikiama apsaugos priemonių, susijusių su automatizuotai priimant sprendimus naudojamais modeliais, kurie galėtų lemti diskriminaciją dėl tam tikrų ypatybių, ir asmenims suteikiamos teisės ginčyti tokius sprendimus, be kita ko, priimtus automatizuotai. Dėl informacijos apie sveikatą, Sveikatos draudimo perkeliamumo ir atskaitomybės akto (HIPAA) taisykle dėl privatumo nustatytos tam tikros teisės, kurios dėl galimybės susipažinti su asmens sveikatos informacija yra panašios į nustatytąsias Reglamente (ES) 2016/679. Be to, JAV valdžios institucijų pateiktose gairėse reikalaujama, kad medicinos paslaugų teikėjai gautų informaciją, leidžiančią jiems informuoti asmenis apie medicinos sektoriuje naudojamas automatizuotas sprendimų priėmimo sistemas ([54]).

(36) Taigi menkai tikėtinoje situacijoje, kurioje automatizuotus sprendimus priimtų pati ES ir JAV DPS organizacija, šiomis taisyklėmis suteikiama apsauga, panaši į numatytąją pagal Sąjungos duomenų apsaugos teisę.

2.2.6. ***Tolesnio duomenų perdavimo ribojimas***

(37) Iš Sąjungos organizacijoms Jungtinėse Amerikos Valstijose perduodamų asmens duomenų apsaugos lygis negali sumažėti tokius duomenis toliau perduodant gavėjui Jungtinėse Amerikos Valstijose arba kitoje trečiojoje valstybėje.

(38) Pagal *atskaitomybės už tolesnį duomenų perdavimą principą* ([55]) tolesniam duomenų perdavimui taikomos specialios taisyklės; tai yra ES ir JAV DPS organizacijos atliekamas asmens duomenų perdavimas trečiajai šaliai duomenų valdytojui arba duomenų tvarkytojui, nepaisant to, ar pastaroji yra Jungtinėse Amerikos Valstijose, ar už Jungtinių Amerikos Valstijų (ir Sąjungos) ribų esančioje trečiojoje valstybėje. Bet koks tolesnis duomenų perdavimas gali būti vykdomas tik i) ribotais ir konkrečiai nurodytais tikslais, ii) remiantis ES ir JAV DPS organizacijos ir trečiosios šalies sutartimi ([56]) (arba panašiu susitarimu įmonių grupėje ([57])) ir iii) tik tuo atveju, jeigu pagal tą sutartį reikalaujama, kad trečioji šalis užtikrintų tokį patį apsaugos lygį, koks yra garantuojamas pagal Principus.

(39) Ši prievolė užtikrinti tokį pat apsaugos lygį, koks yra garantuojamas pagal Principus, vertinama kartu su *duomenų vientisumo ir tikslo apribojimo principu*, visų pirma reiškia, kad trečioji šalis gali tvarkyti jai perduotą asmeninę informaciją tik tais tikslais, kurie nėra nesuderinami su tikslais, kuriais ta informacija buvo surinkta arba vėliau asmuo leido ją naudoti (pagal *pasirinkimo principą*).

([53]) Žr., pvz., Vienodų galimybių gauti kreditą aktą (JAV kodekso 15 antraštinės dalies 1691 ir paskesni straipsniai), Sąžiningo kredito informacijos teikimo aktą (JAV kodekso 15 antraštinės dalies 1681 ir paskesni straipsniai) arba Sąžiningo apsirūpinimo būstu aktą (JAV kodekso 42 antraštinės dalies 3601 ir paskesni straipsniai). Be to, Jungtinės Amerikos Valstijos pritarė Ekonominio bendradarbiavimo ir plėtros organizacijos dirbtinio intelekto principams, kurie, *inter alia*, apima skaidrumo, paaiškinamumo, saugumo ir atskaitomybės principus.

([54]) Žr., pvz., gaires 2042 „Kokią informaciją apie asmens sveikatą pagal HIPAA asmenys turi teisę gauti iš savo sveikatos priežiūros paslaugų teikėjų ir pagal savo sveikatos planus?“ (*What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans?*). | HHS.gov.

([55]) Žr. I priedo II skirsnio 3 dalį ir papildomą privalomų sutarčių dėl tolesnio duomenų perdavimo principą (I priedo III skirsnio 10 dalis).

([56]) Taikydama šio bendrojo principo išimtį, organizacija gali toliau perduoti nedidelio skaičiaus darbuotojų asmens duomenis nesudarydama sutarties su gavėju dėl atsitiktinių su darbu susijusių veiklos poreikių, pvz., skrydžio užsakymo, viešbučio kambario užsakymo ar draudimo. Tačiau ir šiuo atveju organizacija turi laikytis *pranešimo* ir *pasirinkimo principų* (žr. I priedo III skirsnio 9 dalies e punktą).

([57]) Žr. papildomą privalomų sutarčių dėl tolesnio duomenų perdavimo principą (I priedo III skirsnio 10 dalies b punktas). Nors pagal šį principą duomenų perdavimas taip pat gali būti grindžiamas nesutartinėmis priemonėmis (pvz., reikalavimų laikymosi grupės viduje ir kontrolės programomis), tekste aiškiai nurodoma, kad šiomis priemonėmis visada būtina „užtikrinti nuolatinę asmeninės informacijos apsaugą pagal Principus“. Be to, atsižvelgiant į tai, kad sertifikuota JAV organizacija liks atsakinga už Principų laikymąsi, ji bus ypač suinteresuota naudoti priemones, kurios iš tikrųjų yra praktiškai veiksmingos.

(40) Atskaitomybės už tolesnį duomenų perdavimą principą taip pat reikėtų vertinti kartu su *pranešimo principu* ir, jeigu duomenys toliau perduodami trečiajai šaliai duomenų valdytojai ([58]), *pasirinkimo principu*, pagal kurį duomenų subjektai turi būti informuojami (be kita ko) apie bet kurios trečiosios šalies gavėjos tipą ir (arba) tapatybę, tolesnio duomenų perdavimo tikslą ir siūlomą galimybę rinktis ir gali nesutikti (atsisakyti sutikti) arba, jeigu perduodami neskelbtini duomenys, turi duoti „aiškų sutikimą“ (pasirinktą sutikimą), kad duomenys būtų perduodami toliau.

(41) Prievolė užtikrinti tokį pat apsaugos lygį, kokio reikalaujama pagal Principus, taikoma visoms trečiosioms šalims, dalyvaujančioms tvarkant taip perduotus duomenis, nepaisant jų buvimo vietos (JAV ar kitoje trečiojoje valstybėje), be kita ko, kai pradinė trečioji šalis gavėja pati tuos duomenis perduoda kitai trečiajai šaliai gavėjai, pvz., duomenų tvarkymo subrangos tikslais.

(42) Visais atvejais sutartyje su trečiąja šalimi gavėja turi būti nustatyta, kad pastaroji praneš ES ir JAV DPS organizacijai, jeigu nustatys, kad nebegali vykdyti šios prievolės. Tai nustačiusi, trečioji šalis privalo nutraukti duomenų tvarkymą arba turi būti imamasi kitų pagrįstų ir tinkamų priemonių padėčiai ištaisyti ([59]).

(43) Jeigu duomenys toliau perduodami trečiajai šaliai, kuri veikia kaip atstovas (t. y. duomenų tvarkytojui), taikomos papildomos apsaugos priemonės. Tokiu atveju JAV organizacija privalo užtikrinti, kad atstovas veiktų tik pagal jos nurodymus, ir imtis pagrįstų ir tinkamų priemonių siekdama i) užtikrinti, kad atstovas veiksmingai tvarkytų asmeninę informaciją, kuri buvo perduota organizacijos prievoles pagal Principus atitinkančiu būdu, ir ii) gavusi pranešimą sustabdyti neleidžiamą duomenų tvarkymą ir ištaisyti susidariusią padėtį ([60]). Prekybos departamentas gali reikalauti, kad organizacija pateiktų sutarties nuostatų dėl privatumo santrauką arba reprezentatyvią kopiją ([61]). Jeigu problemų dėl reikalavimų laikymosi kyla duomenų tvarkymo (subrangos) grandinėje, iš esmės atsakomybė tenka organizacijai, kuri veikia kaip asmens duomenų valdytoja, kaip nustatyta pagal *teisių gynimo, vykdymo užtikrinimo ir atsakomybės principą*, nebent ji įrodo, kad nėra atsakinga už įvykį, dėl kurio buvo padaryta žala ([62]).

2.2.7. ***Atskaitomybė***

(44) Pagal atskaitomybės principą duomenis tvarkantys subjektai privalo nustatyti tinkamas technines ir organizacines priemones, kad veiksmingai laikytųsi savo duomenų apsaugos prievolių ir galėtų įrodyti (visų pirma kompetentingai priežiūros institucijai), kad jų laikosi.

(45) Savanoriškai nusprendusi atlikti sertifikavimą ([63]) pagal ES ir JAV DPS, organizacija privalo veiksmingai laikytis Principų ir užtikrinti, kad jų būtų laikomasi. Pagal *teisių gynimo, vykdymo užtikrinimo ir atsakomybės principą* ([64]) ES ir JAV DPS organizacijos turi parūpinti veiksmingus mechanizmus Principų laikymuisi užtikrinti. Be to, organizacijos privalo imtis priemonių, kad patikrintų ([65]), ar jų privatumo politika atitinka Principus ir ar jos iš tikrųjų laikomasi. Tai galima padaryti naudojant įsivertinimo sistemą, būtinai apimančią vidaus procedūras, kuriomis užtikrinama, kad darbuotojams būtų rengiami mokymai organizacijos privatumo politikos įgyvendinimo klausimais ir kad būtų periodiškai objektyviai tikrinama, kaip laikomasi reikalavimų, arba vykdant išorės reikalavimų laikymosi peržiūras, pvz., atliekant auditą, vykdant atsitiktines patikras ar naudojantis technologinėmis priemonėmis.

([58]) Asmenys neturi teisės atsisakyti sutikti, jeigu asmens duomenys perduodami trečiajai šaliai, kuri veikia kaip atstovas, vykdantis užduotis JAV organizacijos vardu ir pagal jos nurodymus. Tačiau šiuo atveju reikalaujama, kad su atstovu būtų sudaryta sutartis, o JAV organizacija, naudodamasi įgaliojimais duoti nurodymus, bus atsakinga už tai, kad būtų užtikrinta pagal Principus numatyta apsauga.

([59]) Padėtis skiriasi priklausomai nuo to, ar trečioji šalis yra duomenų valdytoja, ar duomenų tvarkytoja (atstovė). Pirmuoju atveju sutartyje su trečiąja šalimi turi būti nustatyta, kad ši nustoja tvarkyti duomenis arba imasi kitų pagrįstų ir tinkamų priemonių padėčiai ištaisyti. Antruoju atveju tokių priemonių turi imtis ES ir JAV DPS organizacija, kaip duomenų tvarkymą kontroliuojantis subjektas, kurio nurodymais vadovaujasi atstovas. Žr. I priedo II skirsnio 3 dalį.

([60]) I priedo II skirsnio 3 dalies b punktas.

([61]) *Ten pat*.

([62]) I priedo II skirsnio 7 dalies d punktas.

([63]) Taip pat žr. papildomą savarankiško sertifikavimo principą (I priedo III skirsnio 6 dalis).

([64]) Taip pat žr. papildomą ginčų sprendimo ir vykdymo užtikrinimo principą (I priedo III skirsnio 11 dalis).

([65]) Taip pat žr. papildomą patikrinimo principą (I priedo III skirsnio 7 dalis).

(46) Be to, organizacijos turi saugoti įrašus, kaip įgyvendina ES ir JAV DPS praktiką ir, gavusios prašymą, pateikti juos nepriklausomai ginčų sprendimo įstaigai arba kompetentingai vykdymo užtikrinimo institucijai, kai atliekamas tyrimas arba nagrinėjamas skundas dėl reikalavimų nesilaikymo ([66]).

2.3. **Administravimas, priežiūra ir vykdymo užtikrinimas**

(47) ES ir JAV DPS administruos ir stebės Prekybos departamentas. Šioje sistemoje numatyti priežiūros ir vykdymo užtikrinimo mechanizmai, skirti tikrinti ir užtikrinti, kad ES ir JAV DPS organizacijos laikytųsi Principų ir kad būtų reaguojama į bet kokį jų nesilaikymo atvejį. Šie mechanizmai apibūdinti Principų nuostatose (I priedas), taip pat Prekybos departamento (III priedas), FPK (IV priedas) ir Transporto departamento (V priedas) prisiimtuose įsipareigojimuose.

2.3.1. ***(Pakartotinis) sertifikavimas***

(48) Siekdamos būti sertifikuotos pagal ES ir JAV DPS (arba kasmet atnaujinti sertifikavimą), organizacijos privalo viešai pareikšti, kad įsipareigoja laikytis Principų, sudaryti sąlygas susipažinti su jų privatumo politika ir visapusiškai ją įgyvendinti ([67]). Teikdamos (pakartotinio) sertifikavimo prašymą, organizacijos turi Prekybos departamentui pateikti informaciją apie, *inter alia*, atitinkamos organizacijos pavadinimą, tikslų, kuriais organizacija tvarkys asmens duomenis, aprašymą, asmens duomenis, kuriuos apims sertifikavimas, taip pat pasirinktą patikrinimo metodą, atitinkamą nepriklausomą teisių gynimo mechanizmą ir valstybinę įstaigą, turinčią jurisdikciją užtikrinti, kad būtų laikomasi Principų ([68]).

(49) Organizacijos gali gauti asmens duomenis pagal ES ir JAV DPS nuo tos dienos, kurią Prekybos departamentas jas įtraukia į DPS sąrašą. Siekiant užtikrinti teisinį tikrumą ir išvengti neteisingų teiginių, pirmą kartą sertifikuojamoms organizacijoms neleidžiama viešai nurodyti, kad laikosi Principų, kol Prekybos departamentas nuspręs, kad organizacijos sertifikavimo dokumentai yra išsamūs, ir įtrauks organizaciją į DPS sąrašą ([69]). Kad joms ir toliau būtų leidžiama pagal ES ir JAV DPS gauti asmens duomenis iš Sąjungos, tokios organizacijos privalo kasmet pakartotinai atlikdamos sertifikavimą patvirtinti, kad dalyvauja sistemoje. Dėl bet kokių priežasčių pasitraukusi iš ES ir JAV DPS, organizacija privalo pašalinti visus pareiškimus, iš kurių galima suprasti, kad organizacija ir toliau dalyvauja sistemoje ([70]).

(50) Kaip matyti iš III priede išdėstytų įsipareigojimų, Prekybos departamentas tikrins, ar organizacijos atitinka visus sertifikavimo reikalavimus ir yra nustačiusios (viešą) privatumo politiką, apimančią pagal *pranešimo principą* reikalaujamą informaciją ([71]). Remdamasis patirtimi, įgyta vykdant (pakartotinio) sertifikavimo procesą pagal privatumo skydą, Prekybos departamentas vykdys tam tikras patikras, be kita ko, siekdamas patikrinti, ar organizacijų privatumo politikos dokumentuose yra saitas į tinkamą skundo formą atitinkamo ginčų sprendimo mechanizmo interneto svetainėje, ir, kai į sertifikavimo dokumentus įtraukiami keli vienos organizacijos subjektai ir patronuojamosios įmonės, ar kiekvieno iš tų subjektų privatumo politika atitinka sertifikavimo reikalavimus ir ar duomenų subjektai gali lengvai su ja susipažinti ([72]). Be to, prireikus Prekybos departamentas su FPK ir Transporto departamentu atliks kryžminės patikras, siekdami patikrinti, ar organizacijas prižiūri jų (pakartotinio) sertifikavimo dokumentuose nurodyta priežiūros įstaiga, ir bendradarbiaus su alternatyvaus ginčų sprendimo įstaigomis, kad patikrintų, ar organizacijos yra užsiregistravusios naudotis jų (pakartotinio) sertifikavimo dokumentuose nurodytu nepriklausomu teisių gynimo mechanizmu ([73]).

([66]) I priedo III skirsnio 7 dalis.
([67]) I priedo I skirsnio 2 dalis.
([68]) I priedo III skirsnio 6 dalies b punktas ir III priedas, žr. skirsnį „Tikrinti, kaip laikomasi savarankiško sertifikavimo reikalavimų“.
([69]) I priedo 12 išnaša.
([70]) I priedo III skirsnio 6 dalies h punktas.
([71]) I priedo III skirsnio 6 dalies a punktas ir 12 išnaša, taip pat III priedas, žr. skirsnį „Tikrinti, kaip laikomasi savarankiško sertifikavimo reikalavimų“.
([72]) III priedo skirsnis „Tikrinti, kaip laikomasi savarankiško sertifikavimo reikalavimų“.
([73]) Be to, Prekybos departamentas bendradarbiaus su trečiąja šalimi, kuri veiks kaip iš DAI kolegijos mokesčio surinktų lėšų saugotoja (žr. 73 konstatuojamąją dalį), kad patikrintų, ar organizacijos, kaip nepriklausomą teisių gynimo mechanizmą pasirinkusios DAI, sumokėjo mokestį už atitinkamus metus. Žr. III priedo skirsnį „Tikrinti, kaip laikomasi savarankiško sertifikavimo reikalavimų“.

(51) Prekybos departamentas informuos organizacijas, kad norėdamos užbaigti (pakartotinį) sertifikavimą, jos turi išspręsti visas atliekant peržiūrą nustatytas problemas. Jeigu organizacija per Prekybos departamento nustatytą laikotarpį nepateikia atsakymo (pvz., numatoma, kad pakartotinio sertifikavimo procesas atliekamas per 45 dienas) ([74]) arba kitaip nebaigia sertifikavimo, laikoma, kad proceso atsisakyta. Tokiu atveju FPK arba Transporto departamentas gali imtis vykdymo užtikrinimo veiksmų dėl bet kokio klaidingo faktų pateikimo apie dalyvavimą ES ir JAV DPS arba šios sistemos reikalavimų laikymąsi ([75]).

(52) Kad užtikrintų tinkamą ES ir JAV DPS taikymą, suinteresuotosios šalys, pvz., duomenų subjektai, duomenų eksportuotojai ir nacionalinės duomenų apsaugos institucijos (DAI), privalo turėti galimybę nustatyti organizacijas, kurios laikosi Principų. Siekdamas užtikrinti tokį skaidrumą pradiniame taške, Prekybos departamentas įsipareigojo tvarkyti ir viešai skelbti organizacijų, kurios atlikusios sertifikavimą patvirtino, kad laikosi Principų, ir kurios priklauso bent vienos šio sprendimo IV ir V prieduose nurodytų vykdymo užtikrinimo institucijų jurisdikcijai, sąrašą ([76]). Prekybos departamentas sąrašą atnaujins atsižvelgdamas į organizacijos metinio pakartotinio sertifikavimo dokumentus ir visais atvejais, kai organizacija pasitraukia ar yra pašalinama iš ES ir JAV DPS. Be to, siekdamas užtikrinti skaidrumą ir galutiniame taške, Prekybos departamentas tvarkys ir viešai skelbs iš sąrašo išbrauktų organizacijų registrą, kiekvienu atveju nurodydamas tokio išbraukimo priežastį ([77]). Galiausiai jis pateiks nuorodą į ES ir JAV DPS skirtą FPK tinklalapį, kuriame nurodomi FPK vykdymo užtikrinimo veiksmai pagal šią sistemą ([78]).

2.3.2. ***Atitikties stebėsena***

(53) Prekybos departamentas naudodamas įvairius mechanizmus nuolat stebės, ar ES ir JAV DPS organizacijos veiksmingai laikosi Principų ([79]). Visų pirma jis atliks atsitiktine tvarka atrinktų organizacijų patikrą vietoje, taip pat tam tikrų organizacijų *ad hoc* patikrą vietoje, jei nustatoma galimų problemų dėl atitikties (pvz., jei apie tai Prekybos departamentui pranešė trečiosios šalys), kad patikrintų, ar i) skundus ir duomenų subjektų prašymus nagrinėjantis (-ys) kontaktinis (-iai) punktas (-ai) yra lengvai pasiekiamas (-i) ir atsako; ii) su organizacijos privatumo politika galima patogiai susipažinti tiek jos interneto svetainėje, tiek per saitą Prekybos departamento interneto svetainėje; iii) organizacijos privatumo politika ir toliau atitinka sertifikavimo reikalavimus, taip pat iv) organizacijų pasirinktas nepriklausomas ginčų sprendimo mechanizmas gali būti naudojamas skundams nagrinėti ([80]).

(54) Jeigu yra patikimų įrodymų, kad organizacija nesilaiko savo įsipareigojimų pagal ES ir JAV DPS (be kita ko, jeigu Prekybos departamentas gavo skundų arba organizacija nepateikia tenkinančio atsakymo į Prekybos departamento užklausas), Prekybos departamentas pareikalaus, kad organizacija užpildytų ir pateiktų išsamų klausimyną ([81]). Tinkamai ir laiku į klausimyną neatsakiusi organizacija bus perduota atitinkamai institucijai (FPK arba Transporto departamentui), kad ši imtųsi galimų vykdymo užtikrinimo veiksmų ([82]). Vykdydamas atitikties stebėsenos veiklą

([74]) III priedo 2 išnaša.
([75]) Žr. III priedo skirsnį „Tikrinti, kaip laikomasi savarankiško sertifikavimo reikalavimų“.
([76]) Informacija apie DPS sąrašo tvarkymą pateikiama III priede (žr. skirsnio „Prekybos departamento vykdomas Duomenų privatumo sistemos programos administravimas ir priežiūra“ įvadą) ir I priede (I skirsnio 3 dalyje, I skirsnio 4 dalyje, III skirsnio 6 dalies d punkte ir III skirsnio 11 dalies g punkte).
([77]) III priedas, žr. skirsnio „Prekybos departamento vykdomas Duomenų privatumo sistemos programos administravimas ir priežiūra“ įvadą.
([78]) Žr. III priedo skirsnį „Pritaikyti Duomenų privatumo sistemos interneto svetainę prie tikslinės auditorijos poreikių“.
([79]) Žr. III priedo skirsnį „Periodiškai *ex officio* atlikti Duomenų privatumo sistemos programos reikalavimų laikymosi peržiūras ir vertinimus“.
([80]) Vykdydamas stebėsenos veiklą, Prekybos departamentas gali naudoti įvairias priemones, be kita ko, tikrinti, ar nėra neveikiančių saitų į privatumo politiką, arba aktyviai stebėti naujienas rengiant ataskaitas, kuriose pateikiama patikimų neatitikties įrodymų.
([81]) Žr. III priedo skirsnį „Periodiškai *ex officio* atlikti Duomenų privatumo sistemos programos reikalavimų laikymosi peržiūras ir vertinimus“.
([82]) Žr. III priedo skirsnį „Periodiškai *ex officio* atlikti Duomenų privatumo sistemos programos reikalavimų laikymosi peržiūras ir vertinimus“.

pagal privatumo skydą, Prekybos departamentas reguliariai atlikdavo 53 konstatuojamojoje dalyje minimas patikras vietoje ir nuolat stebėjo viešas ataskaitas, todėl galėjo nustatyti, nagrinėti ir spręsti atitikties problemas ([83]). Nuolat Principų nesilaikančios organizacijos bus išbrauktos iš DPS sąrašo ir privalės grąžinti arba ištrinti pagal šią sistemą gautus asmens duomenis ([84]).

(55) Kitais išbraukimo iš sąrašo atvejais, pvz., savo noru nustojus dalyvauti sistemoje arba neatlikus pakartotinio sertifikavimo, organizacija privalo tokius duomenis ištrinti arba grąžinti, arba gali juos išsaugoti, jeigu kasmet Prekybos departamentui patvirtina savo įsipareigojimą toliau taikyti Principus arba kitomis leidžiamomis priemonėmis užtikrina tinkamą asmens duomenų apsaugą (pvz., sudarydama sutartį, kuri visiškai atitinka Komisijos patvirtintose standartinėse sutarčių sąlygose nustatytus reikalavimus) ([85]). Šiuo atveju organizacija taip pat turi nurodyti savo kontaktinį centrą, kuris bus atsakingas už visus su ES ir JAV DPS susijusius klausimus.

2.3.3. ***Neteisingų teiginių apie dalyvavimą nustatymas ir šalinimas***

(56) Prekybos departamentas stebės bet kokius neteisingus teiginius apie dalyvavimą ES ir JAV DPS arba netinkamą ES ir JAV DPS sertifikavimo ženklo naudojimą tiek *ex officio*, tiek reaguodamas į skundus (pvz., gautus iš DAI) ([86]). Visų pirma, Prekybos departamentas nuolat tikrins, ar organizacijos, kurios i) nustojo dalyvauti ES ir JAV DPS, ii) neatliko metinio pakartotinio sertifikavimo (t. y. pradėjo metinio pakartotinio sertifikavimo procesą, bet jo laiku neužbaigė arba to proceso net nepradėjo), iii) kaip dalyvės yra pašalintos iš sistemos visų pirma dėl „nuolatinio reikalavimų nesilaikymo“ arba iv) neatliko pirminio sertifikavimo (t. y. pradėjo pirminio sertifikavimo procesą, bet jo laiku neužbaigė), iš visų susijusių paskelbtų privatumo politikos priemonių pašalino ES ir JAV DPS nuorodas, iš kurių galima suprasti, kad organizacija aktyviai dalyvauja sistemoje ([87]). Prekybos departamentas taip pat vykdys paiešką internete siekdamas nustatyti ES ir JAV DPS nuorodas organizacijų privatumo politikos priemonėse, be kita ko, ES ir JAV DPS niekada nedalyvavusių organizacijų neteisingus teiginius ([88]).

(57) Nustatęs, kad ES ir JAV DPS nuorodos nebuvo pašalintos arba yra naudojamos netinkamai, Prekybos departamentas informuos organizaciją apie galimą klausimo perdavimą FPK ir (arba) Transporto departamentui ([89]). Organizacijai nepateikus tenkinančio atsakymo, Prekybos departamentas šį klausimą perduoda atitinkamai agentūrai, kad ši imtųsi galimų vykdymo užtikrinimo veiksmų ([90]). Kai organizacija klaidina visuomenę dėl savo įsipareigojimo laikytis Principų pateikdama neteisingus teiginius arba taikydama klaidinančią praktiką, vykdymo užtikrinimo veiksmų imasi FPK, Transporto departamentas arba kitos atitinkamos JAV vykdymo užtikrinimo institucijos. Už klaidingą faktų pateikimą Prekybos departamentui baudžiama pagal Melagingų parodymų aktą (JAV kodekso 18 antraštinės dalies 1001 straipsnį).

([83]) Per antrąją metinę privatumo skydo peržiūrą Prekybos departamentas informavo, kad atliko 100 organizacijų patikras vietoje ir 21 atveju išsiuntė atitikties klausimynus (po to nustatytos problemos buvo išspręstos); žr. Komisijos tarnybų darbinį dokumentą SWD(2018) 497 *final*, p. 9. Be to, per trečiąją metinę privatumo skydo peržiūrą Prekybos departamentas pranešė, kad stebėdamas viešas ataskaitas nustatė tris incidentus ir pradėjo kas mėnesį vykdyti 30 bendrovių patikras vietoje, dėl to 28 proc. atvejų buvo imtasi tolesnių veiksmų pagal atitikties klausimynus (po to nustatyti trūkumai buvo nedelsiant pašalinti, o trimis atvejais buvo išspręsti pateikus įspėjimo raštą); žr. Komisijos tarnybų darbinį dokumentą SWD(2019) 495 *final*, p. 8.

([84]) I priedo III skirsnio 11 dalies g punktas. Nuolatinis reikalavimų nesilaikymas visų pirma pasireiškia tuo, kad organizacija atsisako laikytis kurios nors privatumo savireguliavimo įstaigos, nepriklausomos ginčų sprendimo įstaigos arba vykdymo užtikrinimo institucijos priimto galutinio sprendimo.

([85]) I priedo III skirsnio 6 dalies f punktas.

([86]) Žr. III priedo skirsnį „Atlikti neteisingų teiginių apie dalyvavimą paiešką ir šalinti tokius teiginius“.

([87]) *Ten pat*.

([88]) *Ten pat*.

([89]) *Ten pat*.

([90]) Per trečiąją metinę sistemos peržiūrą Prekybos departamentas pranešė pagal privatumo skydą nustatęs 669 neteisingų teiginių apie dalyvavimą atvejus (nuo 2018 m. spalio mėn. iki 2019 m. spalio mėn.); dauguma jų buvo išspręsti Prekybos departamentui pateikus įspėjimo raštą, o 143 atvejai buvo perduoti FPK (žr. 62 konstatuojamąją dalį). Žr. Komisijos tarnybų darbinį dokumentą SWD(2019) 495 *final*, p. 10.

2.3.4. ***Vykdymo užtikrinimas***

(58) Siekiant užtikrinti, kad tinkamas duomenų apsaugos lygis būtų garantuojamas praktiškai, reikalinga nepriklausoma priežiūros institucija, kuriai suteikti įgaliojimai stebėti, kaip laikomasi duomenų apsaugos taisyklių, ir užtikrinti, kad jų būtų laikomasi.

(59) ES ir JAV DPS organizacijos turi priklausyti kompetentingų JAV valdžios institucijų – FPK ir Transporto departamento – jurisdikcijai, o šios institucijos turi būtinus tyrimo ir vykdymo užtikrinimo įgaliojimus, kad galėtų veiksmingai užtikrinti Principų laikymąsi ([91]).

(60) FPK – nepriklausoma institucija, kurią sudaro penki Komisijos nariai, kuriuos Senatui patarus ir pritarus skiria Prezidentas ([92]). Komisijos nariai skiriami septynerių metų kadencijai, o Prezidentas gali juos atleisti tik dėl neveiksmingumo, pareigų nevykdymo ar netinkamo vykdymo. Daugiau nei trys FPK nariai negali priklausyti tai pačiai partijai, be to, kol yra paskirti, Komisijos nariai negali vykdyti jokio kito verslo, užsiimti profesine veikla ar dirbti.

(61) FPK gali tirti, kaip laikomasi Principų, taip pat nagrinėti organizacijų, kurios jau nėra įtrauktos į DPS sąrašą arba niekada nebuvo sertifikuotos, neteisingus teiginius apie Principų laikymąsi arba dalyvavimą ES ir JAV DPS ([93]). FPK gali užtikrinti vykdymą prašydama priimti administracinių arba federalinių teismų nutartis (įskaitant susitarimu pasiektas vadinamąsias susitarimo nutartis) ([94]) dėl preliminarių ar nuolatinių draudimų ar kitų teisių gynimo priemonių, ir sistemingai stebės, kaip laikomasi tokių nutarčių ([95]). Jeigu organizacijos tokių nutarčių nesilaiko, FPK gali reikalauti taikyti pinigines nuobaudas ir kitas teisių gynimo priemones, be kita ko, už bet kokią neteisėtu elgesiu padarytą žalą. Kiekvienoje ES ir JAV DPS organizacijai skirtoje susitarimo nutartyje bus nustatyti savarankiško pranešimo reikalavimai ([96]), o organizacijos privalės viešai skelbti visas su ES ir JAV DPS susijusias FPK pateiktų atitikties arba vertinimo ataskaitų dalis. Galiausiai FPK tvarkys internetinį organizacijų, dėl kurių FPK arba teismas priėmė nutartį su ES ir JAV DPS susijusiose bylose, sąrašą ([97]).

(62) Dėl privatumo skydo FPK ėmėsi vykdymo užtikrinimo veiksmų maždaug 22 atvejais – tiek dėl konkrečių sistemos reikalavimų pažeidimų (pvz., Prekybos departamentui nebuvo patvirtinta, kad iš sistemos pasitraukusi organizacija toliau taikė privatumo skydo apsaugos priemones, taip pat nei įvykdžius įsivertinimą, nei atlikus išorinę reikalavimų laikymosi peržiūrą nebuvo patvirtinta, kad organizacija laikosi sistemos reikalavimų) ([98]), tiek dėl neteisingų teiginių apie dalyvavimą sistemoje (pvz., organizacijų, kurios neatliko būtinų veiksmų, kad būtų sertifikuotos, arba sertifikavimo galiojimui pasibaigus klaidingai nurodė, kad toliau dalyvauja sistemoje) ([99]). Šių vykdymo užtikrinimo veiksmų, inter alia, imtasi aktyviai pasinaudojus administraciniais potvarkiais siekiant gauti medžiagos iš tam tikrų privatumo skydo dalyvių, kad būtų galima patikrinti, ar nėra esminių privatumo skydo įsipareigojimų pažeidimų ([100]).

([91]) ES ir JAV DPS organizacija turi viešai pareikšti savo įsipareigojimą laikytis Principų, atskleisti savo privatumo politiką, kuri atitinka šiuos Principus, ir visapusiškai ją įgyvendinti. Nesilaikant Principų, vykdymas užtikrinamas pagal FPK akto 5 straipsnį, kuriuo draudžiama vykdyti nesąžiningus ir apgaulingus veiksmus prekyboje arba darančius jai poveikį (JAV kodekso 15 antraštinės dalies 45 straipsnis), ir JAV kodekso 49 antraštinės dalies 41712 straipsnį, pagal kurį vežėjui arba bilietų pardavėjui draudžiama vykdyti nesąžiningą ar apgaulingą veiklą oro transporto arba oro transporto paslaugų pardavimo srityse.

([92]) JAV kodekso 15 antraštinės dalies 41 straipsnis.

([93]) IV priedas.

([94]) Iš FPK pateiktos informacijos matyti, kad ji neturi įgaliojimų atlikti privatumo apsaugos srities patikrinimų vietoje. Tačiau ji turi įgaliojimus nurodyti organizacijoms pateikti dokumentus ir liudytojų parodymus (žr. FPK akto 20 straipsnį) ir gali pasinaudoti teismų sistema, kad užtikrintų tokių nutarčių vykdymą, jeigu jų nesilaikoma.

([95]) Žr. IV priedo skirsnį „Prašymas priimti nutartis ir jų stebėjimas“.

([96]) FPK arba teismo nutartyse gali būti reikalaujama, kad bendrovės įgyvendintų privatumo užtikrinimo programas ir reguliariai FPK teiktų atitikties ataskaitas arba trečiųjų šalių atlikto nepriklausomo tų programų vertinimo rezultatus.

([97]) IV priedo skirsnis „Prašymas priimti nutartis ir jų stebėjimas“.

([98]) Žr. Komisijos tarnybų darbinį dokumentą SWD(2019) 495 *final*, p. 11.

([99]) Žr. FPK interneto svetainėje nurodytas bylas, pateikiamas adresu https://www.ftc.gov/business-guidance/privacy-security/privacy-shield. Taip pat žr. Komisijos tarnybų darbinį dokumentą SWD(2017) 344 *final*, p. 17; Komisijos tarnybų darbinį dokumentą SWD(2018) 497 *final*, p. 12, ir Komisijos tarnybų darbinį dokumentą SWD(2019) 495 *final*, p. 11.

([100]) Žr., pvz., pirmininko Josepho Simonso parengtas pastabas antroje privatumo skydo metinėje apžvalgoje (ftc.gov).

(63) Apskritai pastaraisiais metais FPK ėmėsi vykdymo užtikrinimo veiksmų ne vienu atveju, susijusiu su konkrečių duomenų apsaugos reikalavimų, kurie taip pat numatyti pagal ES ir JAV DPS, pvz., tikslo apribojimo, duomenų saugojimo ([101]), duomenų kiekio mažinimo ([102]), duomenų saugumo ([103]) ir duomenų tikslumo ([104]) principų, laikymosi.

(64) Transporto departamentas turi išimtinius įgaliojimus reguliuoti oro vežėjų privatumo užtikrinimo praktiką, o dėl bilietų pardavėjų privatumo užtikrinimo praktikos parduodant oro vežėjų paslaugas jurisdikcija dalijasi su FPK. Transporto departamento pareigūnai pirmiausia siekia susitarimo, o jei tai neįmanoma, gali pradėti vykdymo užtikrinimo procesą, per kurį Transporto departamento administracinės teisės teisėjui, turinčiam įgaliojimus priimti nutartis nutraukti veiksmus ir skirti pinigines nuobaudas, pateikiami įrodymai ([105]). Siekiant užtikrinti administracinės teisės teisėjų nepriklausomumą ir nešališkumą, teisėjams taikomos kelios apsaugos priemonės pagal Administracinio proceso aktą (APA). Pavyzdžiui, jie gali būti atleisti tik dėl svarios priežasties; bylos jiems skiriamos rotacijos principu; jie negali vykdyti pareigų, nesuderinamų su jų, kaip administracinės teisės teisėjų, pareigomis ir atsakomybe; jie nėra prižiūrimi institucijos, kurioje dirba (šiuo atveju Transporto departamento), tyrimo grupės; savo teisminę ir (arba) vykdymo užtikrinimo funkciją jie privalo vykdyti nešališkai ([106]). Transporto departamentas įsipareigojo stebėti vykdomuosius dokumentus ir užtikrinti, kad su ES ir JAV DPS bylomis susiję dokumentai būtų skelbiami jo interneto svetainėje ([107]).

2.4. **Teisių gynimas**

(65) Siekiant užtikrinti tinkamą apsaugą ir visų pirma asmens teisių įgyvendinimą, duomenų subjektui turėtų būti suteikta veiksmingų administracinių ir teisminių teisių gynimo priemonių.

(66) Pagal ES ir JAV DPS *teisių gynimo, vykdymo užtikrinimo ir atsakomybės principą* reikalaujama, kad organizacijos suteiktų dėl reikalavimų nesilaikymo nukentėjusiems asmenims galimybę ginti savo teises, t. y. galimybę Sąjungos duomenų subjektams pateikti skundus, kad ES ir JAV DPS organizacijos nesilaiko reikalavimų, ir reikalauti, kad šie skundai būtų išnagrinėti, prireikus priimant sprendimą, kuriuo nustatoma veiksminga teisių gynimo priemonė ([108]). Kai vykdomas sertifikavimas, organizacijos privalo atitikti šio principo reikalavimus užtikrindamos veiksmingus ir lengvai prieinamus nepriklausomus teisių gynimo mechanizmus, kuriuos taikant būtų galima asmeniui nemokamai ištirti ir operatyviai išspręsti kiekvieno asmens skundus ir ginčus ([109]).

([101]) Žr., pvz., FPK nutartį byloje „Drizly, LLC“, kurioje, be kita ko, reikalaujama, kad bendrovė 1) sunaikintų visus surinktus asmens duomenis, kurie nėra jai būtini produktams tiekti ar paslaugoms vartotojams teikti, 2) nerinktų ir nesaugotų asmeninės informacijos, išskyrus atvejus, kai tai būtina konkrečiais saugojimo sąraše nurodytais tikslais.

([102]) Žr., pvz., FPK nutartį byloje „CafePress“ (2022 m. kovo 24 d.), kurioje, be kita ko, reikalaujama kuo labiau sumažinti renkamų duomenų kiekį.

([103]) Žr., pvz., FPK vykdymo užtikrinimo veiksmus bylose „Drizzly, LLC“ ir „CafePress“, kuriais reikalaujama, kad atitinkamos bendrovės nustatytų specialią saugumo programą arba konkrečias saugumo priemones. Be to, dėl duomenų saugumo pažeidimų taip pat žr. 2023 m. sausio 27 d. FPK nutartį byloje „Chegg“, 2019 m. susitarimą su „Equifax“ (https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach).

([104]) Žr., pvz., bylą „RealPage, Inc“ (2018 m. spalio 16 d.), kurioje FPK ėmėsi vykdymo užtikrinimo veiksmų pagal FCRA prieš nuomininkų tikrinimo bendrovę, kuri būsto savininkams ir būsto valdymo įmonėms teikė informaciją apie asmenis, pagrįstą nuomininkų nuomos istorijos duomenimis, viešų archyvų informacija (įskaitant informaciją apie teistumą ir iškeldinimą) ir kredito informacija, kuri buvo laikoma kriterijumi nustatant teisę gauti būstą. FPK nustatė, kad bendrovė nesiėmė pagrįstų priemonių, kad užtikrintų informacijos, kurią ji pateikė taikydama savo automatizuoto sprendimo priėmimo priemonę, tikslumą.

([105]) Žr. V priedo skirsnį „Vykdymo užtikrinimo praktika“.

([106]) Žr. JAV kodekso 5 antraštinės dalies 3105 straipsnį, 7521 straipsnio a dalį, 554 straipsnio d dalį ir 556 straipsnio b dalies 3 punktą.

([107]) Žr. V priedo skirsnį „Su ES ir JAV DPS reikalavimų pažeidimais susijusių vykdomųjų dokumentų stebėjimas ir skelbimas“.

([108]) I priedo II skirsnio 7 dalis.

([109]) I priedo III skirsnio 11 dalis.

(67) Organizacijos gali pasirinkti Sąjungoje arba Jungtinėse Amerikos Valstijose veikiančius nepriklausomus teisių gynimo mechanizmus. Kaip išsamiau paaiškinta 73 konstatuojamojoje dalyje, tai apima galimybę savanoriškai įsipareigoti bendradarbiauti su ES DAI. Kai organizacijos tvarko žmogiškųjų išteklių duomenis, toks įsipareigojimas bendradarbiauti su ES DAI yra privalomas. Kitos alternatyvos – be kita ko, nepriklausomas alternatyvus ginčų sprendimas arba privačiojo sektoriaus sukurtos privatumo užtikrinimo programos, į kurių taisykles įtraukti Principai. Tokiose programose turi būti nustatyti veiksmingi vykdymo užtikrinimo mechanizmai, atitinkantys *teisių gynimo, vykdymo užtikrinimo ir atsakomybės principo* reikalavimus.

(68) Taigi pagal ES ir JAV DPS duomenų subjektams suteikiama įvairių galimybių įgyvendinti savo teises, pateikti skundus dėl organizacijų ES ir JAV DPS reikalavimų nesilaikymo ir reikalauti, kad jų skundai būtų išspręsti, prireikus priimant sprendimą, kuriuo nustatoma veiksminga teisių gynimo priemonė. Asmenys skundą gali pateikti tiesiogiai organizacijai, organizacijos paskirtai nepriklausomai ginčų sprendimo įstaigai, nacionalinėms DAI, Prekybos departamentui arba FPK. Jeigu jų skundai neišnagrinėti nė pagal vieną iš šių teisių gynimo arba vykdymo užtikrinimo mechanizmų, asmenys taip pat turi teisę kreiptis dėl privalomo arbitražo (šio sprendimo I priedo I priedas). Išskyrus arbitražo komisiją, į kurią galima kreiptis tik išnaudojus tam tikras teisių gynimo priemones, asmenys gali savo nuožiūra naudotis bet kuriuo ar visais teisių gynimo mechanizmais ir neprivalo rinktis kažkurio vieno mechanizmo ar jais naudotis konkrečia seka.

(69) Pirma, Sąjungos duomenų subjektai gali iškelti bylą dėl Principų nesilaikymo tiesiogiai kreipdamiesi į ES ir JAV DPS organizacijas ([110]). Siekdama palengvinti ginčų sprendimą, organizacija privalo nustatyti veiksmingą teisių gynimo mechanizmą tokiems skundams nagrinėti. Todėl organizacijos privatumo politikoje asmenims turi būti pateikiama aiški informacija apie skundus nagrinėsiantį organizacijoje arba ne organizacijoje veikiantį kontaktinį centrą (įskaitant bet kokį susijusį padalinį Sąjungoje, kuris gali atsakyti į užklausas arba skundus), taip pat apie specialią nepriklausomą ginčų sprendimo įstaigą (žr. 70 konstatuojamąją dalį). Iš paties asmens arba per Prekybos departamentą, kuriam skundą perdavė DAI, gavusi asmens skundą, organizacija Sąjungos duomenų subjektui privalo atsakyti per 45 dienas ([111]). Be to, reikalaujama, kad organizacijos greitai atsakytų į Prekybos departamento arba DAI ([112]) (jeigu organizacija įsipareigojo bendradarbiauti su DAI) užklausas ir kitus prašymus pateikti informacijos, kaip organizacijos laikosi Principų.

(70) Antra, asmenys skundą taip pat gali tiesiogiai pateikti nepriklausomai ginčų sprendimo įstaigai (Jungtinėse Amerikos Valstijose arba Sąjungoje), organizacijos paskirtai tirti ir nagrinėti asmenų pateiktus skundus (išskyrus atvejus, kai jie akivaizdžiai nepagrįsti ar nerimti) ir suteikti asmeniui tinkamas nemokamas teisių gynimo priemones ([113]). Tokios institucijos nustatytos sankcijos ir teisių gynimo priemonės turi būti pakankamai griežtos, kad priverstų organizacijas laikytis Principų, be to, tomis sankcijomis ir teisių gynimo priemonėmis organizacijos turėtų būti įpareigojamos panaikinti ar ištaisyti reikalavimų nesilaikymo padarinius ir, priklausomai nuo aplinkybių, liautis toliau tvarkius asmens duomenis, kuriems kyla pavojus, ir (arba) juos ištrinti, taip pat viešai paskelbti su reikalavimų nesilaikymu susijusias išvadas ([114]). Organizacijos paskirtos nepriklausomos ginčų sprendimo įstaigos privalo savo viešose interneto svetainėse pateikti atitinkamą informaciją apie ES ir JAV DPS ir paslaugas, kurias teikia veikdamos šioje sistemoje ([115]). Kasmet jos privalo skelbti metinę ataskaitą, kurioje pateikiami apibendrinti statistiniai duomenys apie tokias paslaugas ([116]).

([110]) I priedo III skirsnio 11 dalies d punkto i papunktis.
([111]) I priedo III skirsnio 11 dalies d punkto i papunktis.
([112]) Tai yra DAI kolegijos paskirta ginčų nagrinėjimo institucija, kaip nustatyta pagal papildomą duomenų apsaugos institucijų vaidmens principą (I priedo III skirsnio 5 dalis).
([113]) I priedo III skirsnio 11 dalies d punktas.
([114]) I priedo II skirsnio 7 dalis ir III skirsnio 11 dalies e punktas.
([115]) I priedo III skirsnio 11 dalies d punkto ii papunktis.
([116]) Metinėje ataskaitoje būtina nurodyti: 1) bendrą per ataskaitinius metus gautų su ES ir JAV DPS susijusių skundų skaičių; 2) gautų skundų rūšis; 3) ginčų sprendimo kokybės užtikrinimo priemones, pvz., skundų nagrinėjimo trukmę; 4) gautų skundų nagrinėjimo rezultatus, visų pirma taikytų teisių gynimo priemonių ar sankcijų skaičių ir rūšis.

(71) Laikydamasis savo atitikties peržiūros procedūrų, Prekybos departamentas gali patikrinti, ar ES ir JAV DPS organizacijos iš tikrųjų yra registruotos nepriklausomų teisių gynimo mechanizmų narės, kaip skelbiasi ([117]). Organizacijos ir atsakingi nepriklausomų teisių gynimo mechanizmų atstovai privalo greitai atsakyti į Prekybos departamento užklausas ir prašymus pateikti su ES ir JAV DPS susijusios informacijos. Prekybos departamentas dirbs su nepriklausomais teisių gynimo mechanizmais siekdamas patikrinti, ar jų interneto svetainėse pateikiama informacijos apie Principus ir paslaugas, jų teikiamas pagal ES ir JAV DPS, ir ar skelbiamos jų metinės ataskaitos ([118]).

(72) Jeigu organizacija nesilaiko ginčų sprendimo arba savireguliavimo įstaigos sprendimo, pastaroji privalo apie tai informuoti Prekybos departamentą ir FPK (arba kitą JAV valdžios instituciją, turinčią jurisdikciją atlikti tyrimą, jei organizacija nesilaiko reikalavimų) arba kompetentingą teismą ([119]). Jeigu organizacija atsisako vykdyti galutinį bet kurios privatumo savireguliavimo įstaigos, nepriklausomos ginčų sprendimo įstaigos ar valdžios institucijos sprendimą, arba kai tokia įstaiga ar institucija nustato, kad organizacija dažnai nesilaiko Principų, tai gali būti laikoma nuolatiniu reikalavimų nesilaikymu, o dėl to Prekybos departamentas, pirmiausia prieš 30 dienų įteikęs pranešimą ir suteikęs galimybę reikalavimų nesilaikiusiai organizacijai pateikti atsakymą, išbrauks organizaciją iš DPS sąrašo ([120]). Jeigu iš sąrašo išbraukta organizacija toliau teigia, kad yra sertifikuota pagal ES ir JAV DPS, Prekybos departamentas ją perduos FPK arba kitai vykdymo užtikrinimo institucijai ([121]).

(73) Trečia, asmenys taip pat gali teikti skundus Sąjungos nacionalinei DAI, o ji gali pasinaudoti savo tyrimų ir vykdymo užtikrinimo įgaliojimais pagal Reglamentą (ES) 2016/679. Organizacijos privalo bendradarbiauti su skundą tiriančia ir sprendžiančia DAI, kai toks skundas susijęs su žmogiškųjų išteklių duomenų, surinktų darbo santykių aplinkybėmis, tvarkymu arba kai atitinkama organizacija savanoriškai sutiko, kad DAI prižiūrėtų jos veiklą ([122]). Visų pirma organizacijos turi atsakyti į užklausas, paisyti DAI teikiamų rekomendacijų, be kita ko, dėl teisių gynimo ar kompensacinių priemonių, ir pateikti DAI rašytinį patvirtinimą, kad tokių veiksmų imtasi ([123]). Atvejus, kai DAI rekomendacijų nesilaikoma, DAI perduoda Prekybos departamentui (jis gali išbraukti organizacijas iš ES ir JAV DPS sąrašo) arba, jei gali reikėti vykdymo užtikrinimo veiksmų, – FPK arba Transporto departamentui (pagal JAV teisę už įsipareigojimo bendradarbiauti su DAI arba Principų nesilaikymą gali būti taikomos sankcijos) ([124]).

(74) Siekdami palengvinti bendradarbiavimą, kad skundai būtų nagrinėjami veiksmingiau, tiek Prekybos departamentas, tiek FPK įsteigė specialų kontaktinį centrą, atsakingą už tiesioginius ryšius su DAI ([125]). Šie kontaktiniai centrai padeda tvarkyti DAI užklausas dėl organizacijos atitikties Principams.

(75) DAI pateiktos rekomendacijos paskelbiamos ([126]) po to, kai abiem ginčo šalims buvo suteikta pagrįsta galimybė pateikti pastabų ir visus pageidaujamus įrodymus. Kolegija gali pateikti rekomendacijas iškart, kai tik bus įvykdyti tinkamo proceso reikalavimai, paprastai per 60 dienų nuo skundo gavimo dienos ([127]). Jeigu organizacija per 25 dienas po rekomendacijų pateikimo rekomendacijų neįvykdo ir nepateikia patenkinamo paaiškinimo dėl vėlavimo,

([117]) I priedo skirsnis „Tikrinti, kaip laikomasi savarankiško sertifikavimo reikalavimų“.
([118]) Žr. III priedo skirsnį „Sudaryti palankesnes sąlygas bendradarbiauti su alternatyvaus ginčų sprendimo įstaigomis, teikiančiomis su Principais susijusias paslaugas“. Taip pat žr. I priedo III skirsnio 11 dalies d punkto ii–iii papunkčius.
([119]) Žr. I priedo III skirsnio 11 dalies e punktą.
([120]) Žr. I priedo III skirsnio 11 dalies g punktą, visų pirma ii ir iii papunkčius.
([121]) Žr. III priedo skirsnį „Atlikti neteisingų teiginių apie dalyvavimą paieška ir šalinti tokius teiginius“.
([122]) I priedo II skirsnio 7 dalies b punktas.
([123]) I priedo III skirsnio 5 dalis.
([124]) I priedo III skirsnio 5 dalies c punkto ii papunktis.
([125]) III priedas (žr. skirsnį „Sudaryti palankesnes sąlygas bendradarbiauti su DAI“) ir IV priedas (žr. skirsnius „Pirmumas perduodamiems klausimams ir tyrimai“ ir „Bendradarbiavimas su ES DAI vykdymo užtikrinimo srityje“).
([126]) Neformalios DAI kolegijos darbo tvarkos taisykles turėtų nustatyti DAI, remdamosi savo kompetencija organizuoti savo darbą ir bendradarbiauti tarpusavyje.
([127]) I priedo III skirsnio 5 dalies c punkto i papunktis.

kolegija gali pranešti apie savo ketinimus šį klausimą perduoti FPK (ar kitai kompetentingai JAV vykdymo užtikrinimo institucijai) arba nuspręsti, kad esama rimtų įsipareigojimo bendradarbiauti pažeidimų. Pirmuoju atveju pagal FPK akto 5 straipsnį (ar panašų įstatymą) gali būti imamasi vykdymo užtikrinimo veiksmų ([128]). Antruoju atveju kolegija informuos Prekybos departamentą, o šiam nusprendus, kad organizacijos atsisakymas laikytis DAI kolegijos rekomendacijų laikytinas nuolatiniu reikalavimų nesilaikymu, organizacija bus išbraukta iš DPS sąrašo.

(76) Jeigu DAI, kuriai skirtas skundas, nesiėmė veiksmų arba ėmėsi nepakankamų veiksmų skundui išnagrinėti, skundą pateikęs asmuo turi galimybę apskųsti tokį (ne)veikimą atitinkamos ES valstybės narės nacionaliniams teismams.

(77) Asmenys skundus DAI taip pat gali pateikti net jei DAI kolegija nebuvo paskirta organizacijos ginčų sprendimo įstaiga. Tokiais atvejais DAI gali tokius skundus perduoti Prekybos departamentui arba FPK. Siekdamas palengvinti ir sustiprinti bendradarbiavimą klausimais, susijusiais su asmenų skundais ir ES ir JAV DPS organizacijų reikalavimų nesilaikymu, Prekybos departamentas įsteigs specialų kontaktinį centrą, kuris veiks kaip ryšių palaikymo įstaiga ir padės DAI atsakyti į užklausas, kaip organizacija laikosi Principų ([129]). FPK taip pat įsipareigojo įsteigti specialų kontaktinį centrą ([130]).

(78) Ketvirta, Prekybos departamentas įsipareigojo priimti, peržiūrėti ir kuo labiau pasistengti išspręsti skundus dėl to, kad organizacija nesilaiko Principų ([131]). Šiuo tikslu Prekybos departamentas nustatė DAI skirtas konkrečias procedūras, taikomas perduodant skundus specialiam kontaktiniam centrui, stebint skundų nagrinėjimo eigą ir toliau dirbant su organizacijomis, kad ginčų sprendimas vyktų lengviau ([132]). Siekdamas pagreitinti asmenų skundų nagrinėjimą, kontaktinis centras ne vėliau kaip per 90 dienų nuo klausimo perdavimo jam dienos, tiesiogiai susisiekia su atitinkama DAI, kad aptartų atitikties klausimus ir visų pirma pateiktų DAI naujausią informaciją apie skundų statusą ([133]). Todėl duomenų subjektai skundus dėl to, kad ES ir JAV DPS organizacijos nesilaiko reikalavimų, gali tiesiogiai pateikti savo nacionalinei DAI ir ši juos perduos Prekybos departamentui, kuris veikia kaip ES ir JAV DPS administruojanti JAV valdžios institucija.

(79) Jeigu remdamasis savo *ex officio* patikrinimais, skundais ar bet kuria kita informacija, Prekybos departamentas padaro išvadą, kad organizacija nuolat nesilaiko Principų, jis gali tokią organizaciją išbraukti iš DPS sąrašo ([134]). Atsisakymas laikytis kurios nors privatumo savireguliavimo įstaigos, nepriklausomos ginčų sprendimo įstaigos arba valdžios institucijos, įskaitant DAI, galutinio sprendimo bus laikomas nuolatiniu reikalavimų nesilaikymu ([135]).

(80) Penkta, ES ir JAV DPS organizacija turi priklausyti JAV valdžios institucijų, visų pirma FPK, jurisdikcijai ([136]), o šios institucijos turi būtinus tyrimo ir vykdymo užtikrinimo įgaliojimus, kad galėtų veiksmingai užtikrinti Principų laikymąsi. Siekdama nustatyti, ar buvo pažeistas FPK akto 5 straipsnis, FPK pirmiausia nagrinės skundus dėl Principų nesilaikymo, kuriuos jai perdavė nepriklausomos ginčų sprendimo institucijos arba savireguliavimo įstaigos, Prekybos departamentas ir DAI (veikdami savo iniciatyva arba gavę skundą) ([137]). FPK įsipareigojo sukurti standartizuotą perdavimo procesą, agentūroje paskirti kontaktinį centrą, kuris priims DAI perduotus klausimus, ir keistis informacija apie perduotus klausimus. Be to, FPK gali priimti tiesiogiai asmenų pateiktus skundus ir savo iniciatyva imtis ES ir JAV DPS tyrimų, ypač plačiau nagrinėdama privatumo klausimus.

([128]) I priedo III skirsnio 5 dalies c punkto ii papunktis.
([129]) Žr. III priedo skirsnį „Sudaryti palankesnes sąlygas bendradarbiauti su DAI“.
([130]) Žr. IV priedo skirsnius „Pirmumas perduodamiems klausimams ir tyrimai“ ir „Bendradarbiavimas su ES DAI vykdymo užtikrinimo srityje“.
([131]) Žr., pvz., III priedo skirsnį „Sudaryti palankesnes sąlygas bendradarbiauti su DAI“.
([132]) I priedo II skirsnio 7 dalies e punktas ir III priedo skirsnis „Sudaryti palankesnes sąlygas bendradarbiauti su DAI“.
([133]) *Ten pat*.
([134]) I priedo III skirsnio 11 dalies g punktas.
([135]) I priedo III skirsnio 11 dalies g punktas.
([136]) ES ir JAV DPS organizacija turi viešai pareikšti savo įsipareigojimą laikytis Principų, viešai atskleisti savo privatumo politiką, kuri atitinka šiuos Principus, ir visapusiškai ją įgyvendinti. Nesilaikant Principų, vykdymas užtikrinamas pagal FPK akto 5 straipsnį, kuriuo draudžiama vykdyti nesąžiningus ir apgaulingus veiksmus prekyboje arba darančius jai poveikį.
([137]) Taip pat žr. panašius įsipareigojimus, kuriuos prisiėmė Transporto departamentas (V priedas).

(81) Šešta, kraštutiniu atveju, kai nė vienu iš kitų galimų teisių gynimo būdų asmens skundas nebuvo tinkamai išspręstas, Sąjungos duomenų subjektas gali remtis ES ir JAV duomenų privatumo sistemos kolegijos (toliau – ES ir JAV DPS kolegija) vykdomu privalomu arbitražu ([138]). Organizacijos privalo informuoti asmenis apie galimybę kreiptis dėl privalomo arbitražo ir privalo reaguoti asmeniui pasinaudojus šia galimybe, nusiųsdamos pranešimą atitinkamai organizacijai ([139]).

(82) Tą ES ir JAV DPS kolegiją sudaro bent dešimt arbitrų, kuriuos Prekybos departamentas ir Komisija paskiria atsižvelgdami į jų nepriklausomumą, sąžiningumą, taip pat patirtį JAV privatumo ir Sąjungos duomenų apsaugos teisės srityje. Šalys iš visų arbitrų pasirenka vieno arba trijų ([140]) arbitrų kolegiją, kuri nagrinės jų ginčą.

(83) Prekybos departamentas arbitražui administruoti pasirinko Amerikos arbitražo asociacijos (AAA) tarptautinį padalinį Tarptautinį ginčų sprendimo centrą (ICDR). ES ir JAV DPS kolegijoje vykstantys procesai bus reglamentuojami sutartomis arbitražo taisyklėmis ir paskirtų arbitrų elgesio kodeksu. ICDR-AAA interneto svetainėje asmenys aiškiai ir glaustai informuojami apie arbitražo mechanizmą ir kreipimosi dėl arbitražo procedūrą.

(84) Prekybos departamento ir Komisijos sutartomis arbitražo taisyklėmis papildoma ES ir JAV DPS, kuriai būdingos kelios ypatybės, didinančios šio mechanizmo prieinamumą Sąjungos duomenų subjektams: i) parengti kolegijai adresuotą reikalavimą duomenų subjektui gali padėti jo nacionalinė DAI; ii) nors arbitražas vyks Jungtinėse Amerikos Valstijose, Sąjungos duomenų subjektai gali nuspręsti dalyvauti naudodamiesi vaizdo arba telefoninės konferencijos paslaugomis, kurios asmeniui teikiamos nemokamai; iii) nors arbitražas paprastai vyksta anglų kalba, duomenų subjektas, pateikęs pagrįstą prašymą, gali gauti nemokamas vertimo žodžiu arbitražo posėdyje ir vertimo raštu paslaugas; iv) galiausiai nors kiekviena šalis turi sumokėti savo advokato mokesčius, jeigu šaliai kolegijoje atstovauja advokatas, Prekybos departamentas įsteigs fondą, į kurį ES ir JAV DPS organizacijos mokės metines įmokas, ir iš šio fondo bus padengiamos arbitražo proceso išlaidos, kurių maksimalų dydį nustatys JAV valdžios institucijos pasikonsultavusios su Komisija ([141]).

(85) ES ir JAV DPS kolegija turi įgaliojimus nustatyti konkrečiam asmeniui skirtą nepiniginę lygiavertę teisių gynimo priemonę ([142]), kuri yra būtina dėl Principų nesilaikymo susidariusiai padėčiai ištaisyti. Nors priimdama sprendimą kolegija atsižvelgia į kitas teisių gynimo priemones, kurios jau buvo taikomos pagal kitus ES ir JAV DPS mechanizmus, asmenys vis vien gali kreiptis dėl arbitražo, jeigu mano, kad minėtosios kitos teisių gynimo priemonės nepakankamos. Todėl Sąjungos duomenų subjektai gali kreiptis dėl arbitražo visais atvejais, kai dėl ES ir JAV DPS organizacijų, nepriklausomų teisių gynimo mechanizmų arba 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 ES ir JAV DPS organizacija, t. y. tais atvejais, kai organizacija įpareigojama bendradarbiauti su DAI ir paisyti jos rekomendacijų dėl žmogiškųjų išteklių duomenų, surinktų su darbu susijusiomis aplinkybėmis, tvarkymo arba savanoriškai įsipareigojo tai daryti. Asmenys gali užtikrinti arbitražo sprendimo vykdymą JAV teismuose pagal Federalinį arbitražo aktą – taip užtikrinamas teisių gynimas, jeigu organizacija nesilaiko sprendimo.

([138]) Žr. I priedo I priedą „Arbitražo pavyzdys“.
([139]) Žr. I priedo II skirsnio 1 dalies a punkto xi papunktį ir II skirsnio 7 dalies c punktą.
([140]) Dėl kolegijos arbitrų skaičiaus šalys turi susitarti.
([141]) I priedo I priedo G skirsnio 6 dalis.
([142]) Asmenys per arbitražą negali reikalauti atlyginti žalos, tačiau kreipimasis dėl arbitražo nereiškia, kad tokie asmenys netenka galimybės prisiteisti žalos atlyginimą JAV bendrosios kompetencijos teismuose.

(86) Septinta, kai organizacija nesilaiko savo įsipareigojimo laikytis Principų ir paskelbtos privatumo politikos, pagal JAV teisę galima pasinaudoti papildomomis teisminėmis teisių gynimo priemonėmis, įskaitant žalos atlyginimą. Pavyzdžiui, asmenys gali tam tikromis sąlygomis pasinaudoti teisminėmis teisių gynimo priemonėmis (įskaitant žalos atlyginimą) pagal valstijos vartotojų teisės aktus (klaidingai pateikus faktus, vykdant nesąžiningus ar apgaulingus veiksmus ar praktiką ([143])) ir pagal deliktų teisę (visų pirma dėl deliktų, susijusių su kišimusi į asmeninius reikalus ([144]), pavardės ar atvaizdo nusavinimu ([145]) ir viešu privačių faktų atskleidimu ([146])).

(87) Kartu įvairiomis pirmiau aprašytomis teisių gynimo priemonėmis užtikrinama, kad kiekvienas skundas dėl sertifikuotų organizacijų ES ir JAV DPS reikalavimų nesilaikymo būtų veiksmingai išnagrinėtas ir ištaisytas.

3. JUNGTINIŲ AMERIKOS VALSTIJŲ VALDŽIOS INSTITUCIJŲ SUSIPAŽINIMAS SU ASMENS DUOMENIMIS, PERDUOTAIS IŠ EUROPOS SĄJUNGOS, IR JŲ NAUDOJIMAS

(88) Komisija taip pat įvertino apribojimus ir apsaugos priemones, įskaitant pagal Jungtinių Amerikos Valstijų teisės aktus galimus priežiūros ir asmens teisių gynimo mechanizmus, JAV valdžios institucijoms dėl viešojo intereso, visų pirma, baudžiamosios teisėsaugos ir nacionalinio saugumo tikslais, renkant ir vėliau naudojant asmens duomenis, perduotus duomenų valdytojams ir duomenų tvarkytojams JAV (valdžios sektoriaus susipažinimą su informacija) ([147]). Vertindama, ar sąlygos, kuriomis valdžios sektorius gali susipažinti su duomenimis, perduotais Jungtinėms Amerikos Valstijoms pagal šį sprendimą, atitinka „esminio lygiavertiškumo“ kriterijų pagal Reglamento (ES) 2016/679 45 straipsnio 1 dalį, kaip jį išaiškino Teisingumo Teismas, atsižvelgdamas į Pagrindinių teisių chartiją, Komisija atsižvelgė į kelis kriterijus.

(89) Visų pirma, bet koks teisės į asmens duomenų apsaugą apribojimas turi būti numatytas įstatyme, o pačiame teisiniame pagrinde, kuriuo remiantis leidžiama apriboti tokią teisę, turi būti apibrėžta atitinkamos teisės įgyvendinimo apribojimo apimtis ([148]). Be to, siekiant įvykdyti proporcingumo reikalavimą, pagal kurį nuo asmens duomenų apsaugos nukrypti leidžiančios nuostatos ir asmens duomenų apsaugos apribojimai neviršytų to, kas griežtai būtina demokratinėje visuomenėje siekiant konkrečių bendrojo intereso tikslų, kurie yra lygiaverčiai Sąjungos pripažįstamiems tikslams, pagal tokį teisinį pagrindą turi būti nustatytos aiškios ir tikslios taisyklės, kuriomis reglamentuojamas atitinkamų priemonių apimtis ir taikymas, ir nustatytos minimalios apsaugos priemonės, kad asmenys, kurių duomenys buvo perduoti, turėtų pakankamai garantijų ir galėtų veiksmingai apsaugoti savo asmens duomenis nuo piktnaudžiavimo pavojų ([149]). Be to, šios taisyklės ir apsaugos priemonės turi

([143]) Žr., pvz., valstijos vartotojų teisių apsaugos teisės aktus Kalifornijoje (Kalifornijos civilinio kodekso 1750–1785 straipsniai – (Vakarų) Vartotojų teisių gynimo priemonių aktas); Kolumbijos apygardoje (Kolumbijos apygardos kodekso 28–3901 straipsniai); Floridoje (Floridos statutų 501.201–501.213 straipsniai – Apgaulingos ir nesąžiningos prekybos praktikos aktas); Ilinojuje (815 Ilinojaus jungtinio statuto 505/1–505/12 straipsniai – Vartotojų apgaudinėjimo ir apgaulingos verslo praktikos aktas); Pensilvanijoje (73 Pensilvanijos statutų rinkinio 201-1–201-9.3 straipsniai – (Vakarai) Nesąžiningos prekybos praktikos ir vartotojų apsaugos įstatymas).

([144]) T. y. kai tyčia kišamasi į asmens privačius reikalus ar rūpesčius racionalų asmenį labai įžeidžiančiu būdu ((Antrojo) Deliktų teisės normų sąvado 652 straipsnio b dalis).

([145]) Šis deliktas paprastai taikomas pasisavinus asmens vardą ir pavardę ar atvaizdą ir juos naudojant verslo ar produkto reklamai arba panašiems komerciniams tikslams (žr. (Antrojo) Deliktų teisės normų sąvado 652 straipsnio c dalį).

([146]) T. y. kai viešai skelbiama informacija apie asmens privatų gyvenimą, jei tai labai įžeidžia racionalų asmenį ir informacija neturi teisėtai rūpėti visuomenei ((Antrojo) Deliktų teisės normų sąvado 652 straipsnio d dalis).

([147]) Tai taip pat svarbu atsižvelgiant į I priedo I skirsnio 5 dalį. Pagal šį skirsnį ir panašiai, kaip nustatyta BDAR, duomenų apsaugos reikalavimų laikymuisi ir teisėms, kurios yra privatumo principų dalis, gali būti taikomi apribojimai. Tačiau tokie apribojimai nėra absoliutiniai ir jais galima remtis tik esant kelioms sąlygoms, pavyzdžiui, tiek, kiek būtina, kad būtų laikomasi teismo nutarties arba viešojo intereso, teisėsaugos ar nacionalinio saugumo reikalavimų. Šiomis aplinkybėmis ir dėl aiškumo šiame skirsnyje taip pat daroma nuoroda į VP 14086 nustatytas sąlygas, kurios vertinamos, be kita ko, 127–141 konstatuojamosiose dalyse.

([148]) Žr. Sprendimo *Schrems II* 174–175 punktus ir juose minimą teismo praktiką. Dėl valstybių narių valdžios institucijų galimybės susipažinti su duomenimis taip pat žr. Sprendimo *Privacy International*, C-623/17, ECLI:EU:C:2020:790, 65 punktą ir Sprendimo sujungtose bylose *La Quadrature du Net ir kt.*, C-511/18, C-512/18 ir C-520/18, ECLI:EU:C:2020:791, 175 punktą.

([149]) Žr. Sprendimo *Schrems II* 176 ir 181 punktus, taip pat juose minimą teismo praktiką. Dėl valstybių narių valdžios institucijų galimybės susipažinti su duomenimis taip pat žr. Sprendimo *Privacy International* 68 punktą ir Sprendimo *La Quadrature du Net ir kt.* 132 punktą.

būti teisiškai privalomos ir asmenys turi turėti galimybę užtikrinti jų vykdymą ([150]). Visų pirma, duomenų subjektai turi turėti galimybę imtis teisinių veiksmų nepriklausomame ir nešališkame teisme, kad galėtų susipažinti su savo asmens duomenimis arba reikalauti ištaisyti arba ištrinti tokius duomenis ([151]).

3.1. **JAV valdžios institucijų susipažinimas su duomenimis ir jų naudojimas baudžiamosios teisėsaugos tikslais**

(90) Dėl asmens duomenų, perduodamų pagal ES ir JAV DPS, apribojimų baudžiamosios teisėsaugos tikslais, Jungtinių Amerikos Valstijų teisėje nustatyti keli galimybės susipažinti su asmens duomenimis ir jų naudojimo apribojimai, taip pat numatyti priežiūros ir teisių gynimo mechanizmai, atitinkantys šio sprendimo 89 konstatuojamojoje dalyje nurodytus reikalavimus. Paskesniuose skirsniuose išsamiai įvertinamos sąlygos, kuriomis tokia galimybė susipažinti su duomenimis gali būti suteikta, ir naudojantis tokiais įgaliojimais taikomos apsaugos priemonės. Šiuo atžvilgiu JAV vyriausybė (per Teisingumo departamentą) taip pat pateikė patikinimą dėl taikomų apribojimų ir apsaugos priemonių (šio sprendimo VI priedas).

3.1.1. ***Teisiniai pagrindai, apribojimai ir apsaugos priemonės***

3.1.1.1. *Apribojimai ir apsaugos priemonės, susiję su asmens duomenų rinkimu baudžiamosios teisėsaugos tikslais*

(91) Su sertifikuotų JAV organizacijų tvarkomais asmens duomenimis, kurie būtų perduodami iš Sąjungos remiantis ES ir JAV DPS, baudžiamosios teisėsaugos tikslais gali susipažinti JAV federaliniai prokurorai ir federaliniai tyrėjai, laikydamiesi skirtingų procedūrų, kaip išsamiau paaiškinta 92–99 konstatuojamosiose dalyse. Šios procedūros taikomos taip pat, kaip ir gaunant informaciją iš bet kurios JAV organizacijos, neatsižvelgiant į atitinkamų duomenų subjektų pilietybę ar gyvenamąją vietą ([152]).

(92) Pirma, federalinio teisėsaugos pareigūno arba vyriausybės advokato prašymu teisėjas gali išduoti kratos arba konfiskavimo orderį (be kita ko, elektroniškai saugomos informacijos) ([153]). Toks orderis gali būti išduotas tik jei yra „tikėtina priežastis“ ([154]) manyti, kad orderyje nurodytoje vietoje veikiausiai bus rasta „konfiskuotinų objektų“ (nusikalstamos veikos įrodymų, neteisėtai laikomų daiktų arba nusikalstamai veikai vykdyti sukurto, numatyto naudoti arba panaudoto turto). Orderyje turi būti nurodytas konfiskuotinas turtas ar daiktas, taip pat nurodytas

([150]) Žr. Sprendimo *Schrems II* 181–182 punktus.

([151]) Žr. Sprendimo *Schrems I* 95 punktą ir Sprendimo *Schrems II* 194 punktą. Šiuo atžvilgiu ESTT visų pirma pabrėžė, kad Pagrindinių teisių chartijos 47 straipsnio, kuriame garantuojama teisė į veiksmingą teisinę gynybą nepriklausomame ir nešališkame teisme, laikymasis yra „svarbus užtikrinant Sąjungos teisėje reikalaujamą apsaugos lygį“ ir jo „laikymąsi Komisija turi konstatuoti prieš priimdama sprendimą dėl tinkamumo pagal Reglamento (ES) 2016/679 45 straipsnio 1 dalį“ (Sprendimo *Schrems II* 186 punktas).

([152]) Žr. VI priedą. Žr., pvz., susijusias su Pokalbių pasiklausymo aktu, Saugomų ryšių duomenų aktu ir Renkamų numerių registro aktu (išsamiau nurodytais 95–98 konstatuojamosiose dalyse), *Suzlon Energy Ltd / Microsoft Corp., 671 F.3d 726, 729* (9 Cir. 2011).

([153]) Federalinės baudžiamojo proceso taisyklės, 41. 2018 m. sprendime Aukščiausiasis Teismas patvirtino, kad kratos orderis arba sutikimas netaikyti orderio taip pat reikalingi tam, kad teisėsaugos institucijos galėtų susipažinti su istoriniais mobiliojo ryšio vietos nustatymo įrašais, kuriuose pateikiama išsami naudotojo judėjimo apžvalga, ir kad naudotojas gali pagrįstai tikėtis su tokia informacija susijusio privatumo apsaugos (*Timothy Ivory Carpenter / Jungtinės Amerikos Valstijos*, Nr. 16–402, 585 U.S. (2018)). Todėl tokių duomenų iš mobiliojo ryšio bendrovės paprastai negalima gauti pagal teismo nutartį, remiantis pagrįstomis priežastimis manyti, kad informacija yra svarbi ir reikšminga vykstančiam baudžiamajam tyrimui, tačiau naudojant orderį reikalaujama įrodyti, kad yra tikėtina priežastis.

([154]) Anot Aukščiausiojo Teismo, „tikėtina priežastis“ yra „praktinis, netechninis“ standartas, grindžiamas „faktiniais ir praktiniais kasdienio gyvenimo sumetimais, kuriais remdamiesi veikia racionalūs ir apdairūs žmonės“ (*Ilinojus / Gates*, 462 U.S. 213, 232 (1983)). Kalbant apie kratos orderius, tikėtina priežastis yra tada, kai esama nemažos tikimybės, kad per kratą bus rasta nusikalstamos veikos įrodymų (ten pat).

teisėjas, kuriam turi būti grąžintas orderis. Asmuo, kurio paties arba kurio turto krata atliekama, gali imtis veiksmų, kad panaikintų įrodymus, gautus arba įgytus neteisėtai atlikus kratą, jeigu tie įrodymai pateikiami prieš tą asmenį baudžiamajame procese ([155]). Kai reikalaujama, kad duomenų turėtojas (pvz., bendrovė) atskleistų duomenis pagal orderį, jis reikalavimą atskleisti duomenis visų pirma gali ginčyti dėl pernelyg didelės naštos ([156]).

(93) Antra, tiriant tam tikrus sunkius nusikaltimus, paprastai federalinio prokuroro prašymu, didžioji žiuri (teismo tyrimo skyrius, kurį sudaro teisėjas arba magistratas) gali išduoti potvarkį ([157]), kuriame reikalaujama, kad asmuo pateiktų veiklos įrašus, elektroniškai saugomą informaciją ar kitus materialius daiktus arba leistų su jais susipažinti. Be to, vykdant tyrimus, susijusius su sukčiavimu sveikatos priežiūros srityje, smurtu prieš vaikus, slaptosios tarnybos apsauga, kontroliuojamų medžiagų bylomis ir generalinių inspektorių tyrimais, pagal įvairius įstatymus leidžiama naudoti administracinius potvarkius reikalaujant pateikti veiklos įrašus, elektroniškai saugomą informaciją ar kitus materialius daiktus arba leisti su jais supažinti ([158]). Abiem atvejais informacija turi būti susijusi su tyrimu, o potvarkis negali būti nepagrįstas, t. y. pernelyg platus, sunkiai įvykdomas ar sukeliantis per didelę naštą (ir potvarkio gavėjas gali jį užginčyti dėl šių priežasčių) ([159]).

(94) Labai panašios sąlygos taikomos administraciniams potvarkiams, išduotiems norint susipažinti su JAV bendrovių turimais duomenimis civiliniais ar reguliavimo (viešojo intereso) tikslais. Civilinės ir reguliavimo sričių pareigų turinčių agentūrų įgaliojimai priimti administracinius potvarkius turi būti nustatyti įstatyme. Administracinis potvarkis turi būti naudojamas atlikus „pagrįstumo patikrinimą“, pagal kurį reikalaujama, kad tyrimas būtų atliekamas siekiant teisėto tikslo, pagal potvarkį prašoma informacija būtų susijusi su tuo tikslu, agentūra dar neturėtų informacijos, kurios ji prašo potvarkyje, ir išduodant potvarkį būtų atlikti visi būtini administraciniai veiksmai ([160]). Aukščiausiojo Teismo praktikoje taip pat išaiškintas poreikis pasiekti pusiausvyrą tarp viešojo intereso, susijusio su prašoma informacija, ir asmenų bei organizacijų privatumo interesų svarbos ([161]). Nors administraciniam potvarkiui nereikia išankstinio teismo leidimo, jam taikoma teisminė peržiūra tuo atveju, kai potvarkio gavėjas užginčija pirmiau nurodytus pagrindus arba jeigu išduodančioji agentūra siekia užtikrinti potvarkio vykdymą teisme ([162]). Be šių bendrų apribojimų atskiruose įstatymuose gali būti nustatyti konkretūs (griežtesni) reikalavimai ([163]).

([155]) Žr. *Mapp / Ohajas*, 367 U.S. 643 (1961).

([156]) Žr. *In Re Application of United States*, 610 F.2d 1148, 1157 (3 Cir. 1979) (laikant, jog „dėl tinkamo proceso reikalaujama, kad naštos klausimas būtų išnagrinėtas prieš įpareigojant telefono bendrovę teikti“ pagalbą pagal kratos orderį) ir *In re Application of United States*, 616 F.2d 1122 (9 Cir 1980).

([157]) Pagal JAV Konstitucijos penktąją pataisą reikalaujama, kad didžioji žiuri pateiktų kaltinimą dėl bet kurio „mirties bausme baudžiamo ar kitokio itin sunkaus nusikaltimo“. Iš 16–23 narių sudaryta didžioji žiuri nustato, ar yra tikėtina priežastis manyti, kad padaryta nusikalstama veika. Kad būtų galima padaryti šią išvadą, didžiosioms žiuri suteikti tyrimo įgaliojimai, kad jos galėtų išduoti potvarkius.

([158]) Žr. VI priedą.

([159]) Federalinės baudžiamojo proceso taisyklės, 17.

([160]) *Jungtinės Amerikos Valstijos / Powell*, 379 U.S. 48 (1964).

([161]) *Oklahoma Press Publishing Co. / Walling*, 327 U.S. 186 (1946).

([162]) Aukščiausiasis Teismas išaiškino, kad užginčijus administracinį potvarkį teismas turi išnagrinėti, ar 1) tyrimas atliekamas siekiant teisėto tikslo, 2) atitinkamą potvarkį priimti įgaliota įstaiga priklauso Kongreso kompetencijai ir 3) „prašomi pateikti dokumentai yra svarbūs tyrimui“. Teismas taip pat pažymėjo, kad prašymas priimti administracinį potvarkį turi būti „pagrįstas“, t. y., kad „pateiktinų dokumentų aprašas tūri būti tinkamas atitinkamo tyrimo tikslais, bet ne per platus“ ir „turi būti konkrečiai aprašoma vieta, kurioje ketinama daryti kratą, ir nurodomi areštuotini asmenys ar daiktai.“

([163]) Pavyzdžiui, Teisės į finansinį privatumą aktu valdžios institucijai suteikiami įgaliojimai pagal administracinį potvarkį gauti finansų įstaigos turimus finansinius duomenis tik tuo atveju, jei 1) yra pagrindo manyti, kad prašomi įrašai yra svarbūs teisėtam teisėsaugos tyrimui ir 2) klientui buvo pateikta potvarkio arba šaukimo kopija kartu su pranešimu, kuriame pagrįstai konkrečiai nurodomas tyrimo pobūdis (JAV kodekso 12 antraštinės dalies 3405 straipsnis). Kitas pavyzdys – Sąžiningo kredito informacijos teikimo aktas, kuriuo vartotojų informaciją teikiančioms agentūroms draudžiama atskleisti vartotojų ataskaitas pagal administracinius potvarkius (jos gali reaguoti tik į didžiosios žiuri potvarkius arba teismo nutartis, JAV kodekso 15 antraštinės dalies 1681 ir paskesni straipsniai). Prieigai prie ryšių informacijos taikomi konkretūs Saugomų ryšių duomenų akto reikalavimai, be kita ko, susiję su galimybe naudoti administracinius potvarkius (išsami apžvalga pateikta 96 ir 97 konstatuojamosiose dalyse).

(95) Trečia, baudžiamosios teisėsaugos institucijos susipažinti su ryšių duomenimis gali remdamosi keliais teisiniais pagrindais. Teismas gali priimti nutartį, kuria leidžiama tikruoju laiku rinkti su turiniu nesusijusią skambinimo, nukreipimo, adresavimo ar signalizavimo informaciją apie telefono numerį arba el. pašto adresą (naudojant renkamų numerių registratorių arba gaunamų skambučių sekiklį), jeigu nustato, kad institucija patvirtino, jog informacija, kuri veikiausiai bus gauta, yra svarbi vykstančiam baudžiamajam tyrimui ([164]). Nutartyje turi būti nurodyta, *inter alia*, įtariamojo tapatybė, jei žinoma; ryšių, kuriems ji taikoma, požymiai ir nusikalstama veika, su kuria susijusi rinktina informacija. Naudoti renkamų numerių registratorių arba gaunamų skambučių sekiklį gali būti leidžiama ne ilgiau kaip šešiasdešimt dienų, o šis laikotarpis gali būti pratęstas tik nauja teismo nutartimi.

(96) Be to, galimybę baudžiamosios teisėsaugos tikslais susipažinti su informacija apie abonentą, srauto duomenimis ir saugomu ryšių turiniu, kuriuos turi interneto paslaugų teikėjai, telefono bendrovės ir kiti trečiųjų šalių paslaugų teikėjai, galima gauti pagal Saugomų ryšių duomenų aktą ([165]). Kad gautų saugomą elektroninių ryšių turinį, baudžiamosios teisėsaugos institucijos iš esmės iš teisėjo turi gauti orderį, remdamosi tikėtina priežastimi manyti, kad atitinkamoje paskyroje yra nusikalstamos veikos įrodymų ([166]). Norėdamos gauti abonento registracijos informaciją, IP adresus ir susijusias laiko žymas, taip pat sąskaitų informaciją, baudžiamosios teisėsaugos institucijos gali naudotis potvarkiu. Dėl didžiosios dalies kitos saugomos su turiniu nesusijusios informacijos, pvz., el. laiškų antraščių be temos eilutės, baudžiamosios teisėsaugos institucija turi gauti teismo nutartį, o ši bus išduota teisėjui įsitikinus, kad yra pagrįstų priežasčių manyti, jog prašoma informacija yra svarbi ir reikšminga vykstančiam baudžiamajam tyrimui.

(97) Pagal Saugomų ryšių duomenų aktą prašymus gavę paslaugų teikėjai gali savanoriškai apie tai pranešti klientui ar abonentui, kurio informacijos prašoma, išskyrus atvejus, kai atitinkama baudžiamosios teisėsaugos institucija gauna apsaugos orderį, kuriuo toks pranešimas draudžiamas ([167]). Toks apsaugos orderis yra teismo nutartis, kuria reikalaujama, kad elektroninių ryšių paslaugų arba nuotolinių kompiuterinių paslaugų teikėjas, kuriam skirtas orderis, potvarkis ar teismo nutartis, apie tą orderį, potvarkį ar teismo nutartį nepraneštų jokiam kitam asmeniui tol, kol, teismo manymu, tai reikalinga. Apsaugos orderiai išduodami teismui nustačius, kad yra priežasčių manyti, jog pranešimas gerokai pakenktų tyrimui arba nepagrįstai užvilkintų bylos nagrinėjimą, pvz., dėl to, kad kiltų pavojus asmens gyvybei ar fiziniam saugumui, būtų vengiama baudžiamojo persekiojimo, būtų bauginami galimi liudytojai ir kt. Generalinio prokuroro pavaduotojo memorandumu (kuris yra privalomas visiems Teisingumo departamento advokatams ir atstovams) reikalaujama, kad prokurorai išsamiai išnagrinėtų, ar reikia apsaugos orderio, ir pateiktų teismui pagrindimą, kaip konkrečiu atveju tenkinami įstatyme nustatyti apsaugos orderio išdavimo kriterijai ([168]). Memorandume taip pat reikalaujama, kad prašymuose išduoti apsaugos orderius įprastai nebūtų siekiama pranešimą atidėti ilgiau kaip vieniems metams. Jeigu išskirtinėmis aplinkybėmis gali prireikti ilgesnės trukmės orderių, tokių orderių galima prašyti tik gavus raštišką JAV prokuroro arba atitinkamo generalinio prokuroro pavaduotojo paskirto priežiūros pareigūno sutikimą. Be to, baigdamas tyrimą prokuroras turi nedelsdamas įvertinti, ar yra pagrindo toliau vykdyti galiojančius apsaugos orderius, o jei nėra, nutraukti apsaugos orderio galiojimą ir užtikrinti, kad apie tai būtų pranešta paslaugų teikėjui ([169]).

([164]) JAV kodekso 18 antraštinės dalies 3123 straipsnis.

([165]) JAV kodekso 18 antraštinės dalies 2701–2713 straipsniai.

([166]) JAV kodekso 18 antraštinės dalies 2701 straipsnio a dalis ir b dalies 1 punkto A papunktis. Jeigu atitinkamam abonentui arba klientui yra pranešama (iš anksto arba, tam tikromis aplinkybėmis, pranešimą pateikus vėliau), ilgiau nei 180 dienų saugomą turinio informaciją taip pat galima gauti remiantis administraciniu potvarkiu arba didžiosios žiuri potvarkiu (JAV kodekso 18 antraštinės dalies 2701 straipsnio b dalies 1 punkto B papunktis), arba teismo nutartimi (jeigu yra pagrįstų priežasčių manyti, kad informacija yra svarbi ir reikšminga vykstančiam baudžiamajam tyrimui (JAV kodekso 18 antraštinės dalies 2701 straipsnio d dalis)). Tačiau pagal federalinio apeliacinio teismo sprendimą, kad iš komercinių ryšių paslaugų teikėjo gautų privačių ryšių turinį arba saugomus duomenis, vyriausybės tyrėjai paprastai iš teisėjų gauna kratos orderius. *Jungtinės Amerikos Valstijos / Warshak*, 631 F.3d 266 (6 Cir. 2010).

([167]) JAV kodekso 18 antraštinės dalies 2705 straipsnio b dalis.

([168]) Žr. 2017 m. spalio 19 d. generalinio prokuroro pavaduotojo Rodo Rosensteino paskelbtą memorandumą dėl griežtesnės politikos, susijusios su prašymais išduoti apsaugos (arba neatskleidimo) orderius, pateikiamą adresu https://www.justice.gov/criminal-ccips/page/file/1005791/download.

([169]) 2022 m. gegužės 27 d. generalinio prokuroro pavaduotojos Lisos Moncao paskelbtas memorandumas dėl papildomos politikos, susijusios su prašymais išduoti apsaugos orderius pagal JAV kodekso 18 antraštinės dalies 2705 straipsnio b dalį.

(98) Baudžiamosios teisėsaugos institucijos taip pat gali tikruoju laiku perimti laidinių, žodinių ar elektroninių ryšių duomenis, remdamosi teismo nutartimi, kurioje teisėjas, *inter alia*, nustato, kad yra tikėtina priežastis manyti, jog slapta pasiklausant pokalbių arba perimant elektroninius duomenis bus gauta federalinės nusikalstamos veikos įrodymų arba bus nustatyta nuo baudžiamojo persekiojimo besislapstančio asmens buvimo vieta ([170]).

(99) Papildomos apsaugos priemonės užtikrinamos įvairiomis Teisingumo departamento politikos priemonėmis ir gairėmis, tarp jų Generalinio prokuroro gairėmis dėl Federalinio tyrimų biuro (FTB) vidaus operacijų (AGG-DOM), kuriose, *inter alia*, reikalaujama, kad FTB naudotų kuo mažiau intervencinius tyrimo metodus, atsižvelgdamas į poveikį privatumui ir piliečių laisvėms ([171]).

(100) Pagal JAV vyriausybės pateiktus pareiškimus, valstijų lygmens teisėsaugos tyrimams (pagal valstijų įstatymus vykdomiems tyrimams) taikomos pirmiau aprašytos tokios pačios arba dar griežtesnės apsaugos priemonės ([172]). Visų pirma konstitucinėmis nuostatomis, taip pat valstijų įstatymais ir teismų praktika pakartotinai patvirtinamos pirmiau minėtos apsaugos nuo nepagrįstų kratų ir arešto priemonės, nustatant reikalavimą išduoti kratos orderį ([173]). Panašiai, kaip ir taikant federaliniu lygmeniu užtikrinamas apsaugos priemones, kratos orderiai gali būti išduodami tik įrodžius tikėtiną priežastį, o juose turi būti aprašyta vieta, kurioje ketinama daryti kratą, ir nurodytas areštuotinas asmuo arba daiktas ([174]).

([170]) JAV kodekso 18 antraštinės dalies 2510–2522 straipsniai.

([171]) Generalinio prokuroro gairės dėl Federalinio tyrimų biuro (FTB) vidaus operacijų (2008 m. rugsėjo mėn.), pateikiamos adresu http://www.justice.gov/archive/opa/docs/guidelines.pdf. Papildomų taisyklių ir politikos priemonių, kuriomis nustatomi federalinių prokurorų tyrimo veiklos apribojimai, išdėstyta Jungtinių Amerikos Valstijų teisininkų vadove, pateikiamame adresu http://www.justice.gov/usam/united-states-attorneys-manual. Norint nukrypti nuo šių gairių, reikia gauti išankstinį FTB direktoriaus, direktoriaus pavaduotojo ar direktoriaus paskirto vykdomojo direktoriaus pavaduotojo sutikimą, nebent tokio sutikimo neįmanoma gauti dėl tiesioginės arba didelės grėsmės asmenų ar turto saugumui arba nacionaliniam saugumui (tokiu atveju apie tai reikia kuo greičiau pranešti direktoriui ar kitam įgaliojimus suteikiančiam asmeniui). Jeigu gairių nesilaikoma, FTB apie tai turi pranešti Teisingumo departamentui, o šis apie tai informuos generalinį prokurorą ir generalinio prokuroro pavaduotoją.

([172]) VI priedo 2 išnaša. Taip pat žr., pvz., Sprendimą *Arnold / Klyvlendo miestas*, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) („Asmens teisių ir piliečių laisvių srityse Jungtinių Amerikos Valstijų Konstitucijoje, kai taikoma valstijoms, nustatyta apatinė riba, ir valstijų teismai turi jos laikytis“). *Cooper / Kalifornija*, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) („Mūsų sprendimas, žinoma, nedaro poveikio valstijos teisei nustatyti aukštesnius kratų ir arešto standartus, nei reikalaujama Federalinėje Konstitucijoje, jei ji nusprendžia tai daryti“); *Petersen / Mesos miestas*, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) („Nors Arizonos Konstitucijoje gali būti nustatyti griežtesni kratų ir arešto standartai nei Federalinėje Konstitucijoje, Arizonos teismai negali suteikti mažiau griežtos apsaugos nei pagal Ketvirtąją pataisą“).

([173]) Dauguma valstijų savo konstitucijose atkartojo Ketvirtojoje pataisoje nustatytas apsaugos priemones. Žr. Alabamos Konstitucijos I antraštinės dalies 5 straipsnį; Aliaskos Konstitucijos I antraštinės dalies 14 straipsnį; 1; Arkanzaso Konstitucijos II antraštinės dalies 15 straipsnį; Kalifornijos Konstitucijos I antraštinės dalies 13 straipsnį; Kolorado Konstitucijos II antraštinės dalies 7 straipsnį; Konektikuto Konstitucijos I antraštinės dalies 7 straipsnį; Delavero Konstitucijos I antraštinės dalies 6 straipsnį; Floridos Konstitucijos I antraštinės dalies 12 straipsnį; Džordžijos Konstitucijos I antraštinės dalies I straipsnio XIII dalį; Havajų Konstitucijos I antraštinės dalies 7 straipsnį; Aidaho Konstitucijos I antraštinės dalies 17 straipsnį; Ilinojaus Konstitucijos I antraštinės dalies 6 straipsnį; Indianos Konstitucijos I antraštinės dalies 11 straipsnį; Ajovos Konstitucijos I antraštinės dalies 8 straipsnį; Kanzaso Konstitucijos Teisių akto 15 straipsnį; Kentukio Konstitucijos 10 straipsnį; Luizianos Konstitucijos I antraštinės dalies 5 straipsnį; Meino Konstitucijos I antraštinės dalies 5 straipsnį; Masačiusetso Konstitucijos Teisių deklaracijos 14 straipsnį; Mičigano Konstitucijos I antraštinės dalies 11 straipsnį; Minesotos Konstitucijos I antraštinės dalies 10 straipsnį; Misisipės Konstitucijos III antraštinės dalies 23 straipsnį; Misūrio Konstitucijos I antraštinės dalies 15 straipsnį; Montanos Konstitucijos II antraštinės dalies 11 straipsnį; Nebraskos Konstitucijos I antraštinės dalies 7 straipsnį; Nevados Konstitucijos I antraštinės dalies 18 straipsnį; Naujojo Hampšyro Konstitucijos 1 dalies 19 straipsnį; Naujojo Džersio Konstitucijos II antraštinės dalies 7 straipsnį; Naujosios Meksikos Konstitucijos II antraštinės dalies 10 straipsnį; Niujorko Konstitucijos I antraštinės dalies 12 straipsnį; Šiaurės Dakotos Konstitucijos I antraštinės dalies 8 straipsnį; Ohajo Konstitucijos I antraštinės dalies 14 straipsnį; Oklahomos Konstitucijos II antraštinės dalies 30 straipsnį; Oregono Konstitucijos I antraštinės dalies 9 straipsnį; Pensilvanijos Konstitucijos I antraštinės dalies 8 straipsnį; Rod Ailando Konstitucijos I antraštinės dalies 6 straipsnį; Pietų Karolinos Konstitucijos I antraštinės dalies 10 straipsnį; Pietų Dakotos Konstitucijos VI antraštinės dalies 11 straipsnį; Tenesio Konstitucijos I antraštinės dalies 7 straipsnį; Teksaso Konstitucijos I antraštinės dalies 9 straipsnį; Jutos Konstitucijos I antraštinės dalies 14 straipsnį; Vermonto Konstitucijos I skyriaus 11 straipsnį; Vakarų Virdžinijos Konstitucijos III antraštinės dalies 6 straipsnį; Viskonsino Konstitucijos I antraštinės dalies 11 straipsnį; Vajomingo Konstitucijos I antraštinės dalies 4 straipsnį. Kitos valstijos (pvz., Merilandas, Šiaurės Karolina ir Virdžinija) savo konstitucijose įtvirtino konkrečią formuluotę, susijusią su orderiais, kurie buvo aiškinami teismine tvarka siekiant suteikti panašią į Ketvirtojoje pataisoje numatytąją arba didesnę apsaugą (žr. Merilando Teisių deklaracijos 26 straipsnį; Šiaurės Karolinos Konstitucijos I antraštinės dalies 20 straipsnį; Virdžinijos Konstitucijos I antraštinės dalies 10 straipsnį ir atitinkamą teismų praktiką, pvz., *Hamel / Valstija*, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008; *Valstija / Johnson*, 861 S.E.2d 474, 483 (N.C. 2021) ir *Lowe / Tautų Sandrauga*, 337 S.E.2d 273, 274 (Va. 1985)). Galiausiai, Arizona ir Vašingtonas turi konstitucines nuostatas, kuriomis privatumas apsaugomas bendriau (Arizonos Konstitucijos 2 antraštinės dalies 8 straipsnis; Vašingtono Konstitucijos I antraštinės dalies 7 straipsnis), kurias teismai išaiškino kaip suteikiančias didesnę apsaugą nei Ketvirtoji pataisa (žr., pvz., *Valstija / Bolt*, 689 P.2d 519, 523 (Ariz. 1984), *Valstija / Ault*, 759 P.2d 1320, 1324 (Ariz. 1988), *Valstija / Myrick*, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984) , *Valstija / Young*, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)).

([174]) Žr., pvz., Kalifornijos baudžiamojo kodekso 1524,3 straipsnio b punktą; Alabamos baudžiamojo proceso taisyklių 3.6–3.13 taisykles; Patikslinto Vašingtono kodekso 10.79.035 skirsnį; Virdžinijos Kodekso 19.2 antraštinės dalies „Baudžiamasis procesas“ 5 skyriaus 19.2–59 straipsnį.

3.1.1.2. *Tolesnis surinktos informacijos naudojimas*

(101) Su tolesniu federalinių baudžiamosios teisėsaugos institucijų surinktų duomenų naudojimu susijusios specialios apsaugos priemonės nustatomos įvairiuose įstatymuose, gairėse ir standartuose. Išskyrus konkrečias priemones, taikomas FTB veiklai (AGG-DOM ir FTB vidaus tyrimų ir operacijų vadovą), šiame skirsnyje aprašyti reikalavimai bendrai taikomi, kai bet kuri federalinė institucija toliau naudoja duomenis, įskaitant tuos, su kuriais galima susipažinti civiliniais ar reguliavimo tikslais. Tarp jų – reikalavimai, nustatyti Valdymo ir biudžeto tarnybos pranešimuose ir (arba) taisyklėse, Federaliniame informacijos saugumo valdymo modernizavimo akte, E. valdžios akte ir Federalinių registrų akte.

(102) Vadovaudamasi Clingerio ir Coheno aktu (Viešosios teisės rink. 104–106, E skyrius) ir 1987 m. Kompiuterių saugumo aktu (Viešosios teisės rink. 100–235) suteiktais įgaliojimais, Valdymo ir biudžeto tarnyba (VBT) paskelbė aplinkraštį Nr. A-130, kuriame nustatė bendras privalomas gaires, taikomas visoms federalinėms agentūroms (įskaitant teisėsaugos institucijas) tvarkant asmens tapatybės informaciją ([175]). Visų pirma aplinkraštyje reikalaujama, kad visos federalinės agentūros „apribotų asmens tapatybės informacijos kūrimą, rinkimą, naudojimą, tvarkymą, saugojimą, priežiūrą, platinimą ir atskleidimą tiek, kiek tai teisiškai leidžiama, yra aktualu ir pagrįstai laikoma būtina įgaliotosios agentūros funkcijoms tinkamai vykdyti“ ([176]). Be to, federalinės agentūros privalo, kiek tai pagrįstai įmanoma, užtikrinti, kad asmens tapatybės informacija būtų tiksli, aktuali, laiku atnaujinama ir išsami ir kad jos kiekis būtų sumažintas iki agentūros funkcijoms tinkamai vykdyti būtino minimumo. Apskritai federalinės agentūros turi įdiegti išsamią privatumo užtikrinimo programą, kad užtikrintų atitiktį taikomiems privatumo reikalavimams, parengti ir įvertinti privatumo politiką ir valdyti riziką privatumui; prižiūrėti su privatumo reikalavimų laikymusi susijusių incidentų nustatymo, dokumentavimo ir pranešimo apie juos procedūras; rengti darbuotojų ir rangovų informuotumo apie privatumą ir mokymo programas; įdiegti politikos priemones ir procedūras, kuriomis būtų užtikrinama, kad darbuotojai būtų laikomi atsakingais už privatumo reikalavimų ir politikos laikymąsi ([177]).

(103) Be to, E. valdžios akte ([178]) reikalaujama, kad visos federalinės agentūros (įskaitant baudžiamosios teisėsaugos institucijas) įdiegtų informacijos saugumo užtikrinimo priemones, atitinkančias žalos, kuri būtų padaryta dėl neteisėto susipažinimo su informacija, jos naudojimo, atskleidimo, sutrikdymo, pakeitimo ar sunaikinimo, riziką ir dydį, paskirtų vyriausiąjį informacijos pareigūną, kuris užtikrintų, kad būtų laikomasi informacijos saugumo reikalavimų, ir atliktų savo informacijos saugumo programos ir praktikos metinį nepriklausomą vertinimą (pvz., tai galėtų atlikti generalinis inspektorius, žr. 109 konstatuojamąją dalį) ([179]). Be to, pagal Federalinių registrų aktą (FRA) ([180]) ir papildomus reglamentus ([181]) reikalaujama, kad federalinių agentūrų turimai informacijai būtų taikomos apsaugos priemonės, kuriomis užtikrinamas informacijos fizinis vientisumas ir ji apsaugoma nuo neteisėtos prieigos.

(104) Remdamiesi federaliniais teisės aktais, įskaitant 2014 m. Federalinį informacijos saugumo modernizavimo aktą, suteiktais įgaliojimais, VBT ir Nacionalinis standartų ir technologijų institutas (NIST) parengė standartus, kurie yra privalomi federalinėms agentūroms (įskaitant baudžiamosios teisėsaugos institucijas) ir kuriuose papildomai patikslinami nustatytini minimalūs informacijos saugumo reikalavimai, įskaitant galimybės susipažinti su informacija kontrolę, informuotumo užtikrinimą ir mokymą, nenumatytų atvejų planavimą, reagavimą į incidentus, audito ir atskaitomybės priemones, sistemų ir informacijos vientisumo užtikrinimą, privatumo ir saugumo rizikos vertinimus ir kt. ([182]) Be to,

([175]) T. y. „informacija, kuri gali būti naudojama asmens tapatybei atpažinti arba atsekti, atskirai arba kartu su kita informacija, kuri yra susijusi arba gali būti susieta su konkrečiu asmeniu“, žr. VBT aplinkraštį Nr. A-130, p. 33 (asmens tapatybės informacijos apibrėžtis).

([176]) VBT aplinkraštis Nr. A-130 „Informacijos valdymas kaip strateginis išteklius“ (*Managing Information as a Strategic Resource*), II priedas „Atsakomybė už asmens tapatybės informacijos valdymą“ (*Responsibilities for Managing Personally Identifiable Information*), 81 Fed. Reg. 49,689 (2016 m. liepos 28 d.), p. 17.

([177]) II priedėlio 5 straipsnio a–h dalys.

([178]) JAV kodekso 44 antraštinės dalies 36 skyrius.

([179]) JAV kodekso 44 antraštinės dalies 3544–3545 straipsniai.

([180]) FAC, JAV kodekso 44 antraštinės dalies 3105 straipsnis.

([181]) Federalinių reglamentų kodekso 36 antraštinės dalies 1228,150 ir paskesni straipsniai, 1228,228 straipsnis ir A priedėlis.

([182]) Žr., pvz., VBT aplinkraštį Nr. A-130, NIST SP 800–53, red. 5 „Informacinių sistemų ir organizacijų saugumo ir privatumo kontrolės priemonės“ (*Security and Privacy Controls for Information Systems and Organizations*) (2020 m. gruodžio 10 d.) ir NIST federalinius informacijos tvarkymo standartus 200 dėl minimalių federalinių informacijos ir informacinių sistemų saugumo reikalavimų.

visos federalinės agentūros (įskaitant baudžiamosios teisėsaugos institucijas), vadovaudamosi VBT gairėmis, privalo turėti ir įgyvendinti duomenų saugumo pažeidimų nagrinėjimo planą, be kita ko, apimantį su reagavimu į tokius pažeidimus ir žalos rizikos vertinimu susijusius aspektus ([183]).

(105) Dėl duomenų saugojimo FRA ([184]) reikalaujama, kad JAV federalinės agentūros (įskaitant baudžiamosios teisėsaugos institucijas) nustatytų savo įrašų saugojimo laikotarpius (kuriems pasibaigus tokie įrašai turi būti sunaikinami), o juos turi patvirtinti Nacionalinė archyvų ir įrašų administracija ([185]). Tokio saugojimo laikotarpio trukmė nustatoma atsižvelgiant į įvairius veiksnius, pvz., tyrimo rūšį, tai, ar įrodymai vis dar svarbūs tyrimui, ir kt. Dėl FTB AGG-DOM nustatyta, kad FTB turi būti parengęs tokį įrašų saugojimo planą ir turėti sistemą, kuri leistų greitai sužinoti tyrimų statusą ir pagrindą.

(106) Galiausiai VBT aplinkraštyje Nr. A-130 taip pat nustatyti tam tikri asmens tapatybės informacijos platinimo reikalavimai. Iš esmės, asmens tapatybės informacija turi būti platinama ir atskleidžiama tiek tiek, kiek tai teisiškai leidžiama, yra aktualu ir pagrįstai laikoma būtina įgaliotosios agentūros funkcijoms tinkamai vykdyti ([186]). JAV federalinės agentūros, dalydamosi asmens tapatybės informacija su kitais vyriausybės subjektais, prireikus privalo nustatyti sąlygas (įskaitant konkrečių saugumo ir privatumo kontrolės priemonių įgyvendinimą), kuriomis tokios informacijos tvarkymas reglamentuojamas rašytiniais susitarimais (be kita ko, sutartimis, duomenų naudojimo susitarimais, keitimosi informacija susitarimais ir susitarimo memorandumais) ([187]). Dėl galimų informacijos platinimo pagrindų AGG-DOM ir FTB vidaus tyrimų ir operacijų vadove ([188]), pavyzdžiui, numatoma, kad FTB gali būti taikomas teisinis reikalavimas platinti informaciją (pvz., pagal tarptautinį susitarimą) arba jam gali būti leidžiama ją platinti (pvz., kitoms JAV agentūroms) tam tikromis aplinkybėmis, pvz., jei atskleidimas yra suderinamas su tikslu, kuriuo informacija buvo surinkta, ir yra susijęs su jo atsakomybės sritimis; Kongreso komitetams; užsienio agentūroms, jeigu informacija yra susijusi su jų atsakomybės sritimis, o jos platinimas atitinka Jungtinių Amerikos Valstijų interesus; ją platinti visų pirma būtina siekiant užtikrinti asmenų ar turto saugą ar saugumą arba apsaugoti nuo nusikalstamos veikos ar grėsmės nacionaliniam saugumui arba užkirsti tam kelią, o atskleidimas yra suderinamas su tikslu, kuriuo informacija buvo surinkta ([189]).

3.1.2. ***Priežiūra***

(107) Federalinių baudžiamosios teisėsaugos agentūrų veiklą prižiūri įvairios įstaigos ([190]). Kaip paaiškinta 92–99 konstatuojamosiose dalyse, daugeliu atvejų tai yra išankstinė priežiūra, vykdoma teisminių institucijų, kurios, prieš pradedant taikyti individualias rinkimo priemones, turi suteikti tam leidimą. Įvairius baudžiamosios teisėsaugos institucijų veiklos etapus, įskaitant asmens duomenų rinkimą ir tvarkymą, prižiūri kitos įstaigos. Šios teisminės ir neteisminės institucijos kartu užtikrina, kad teisėsaugos institucijų veikla būtų nepriklausomai prižiūrima.

([183]) Memorandumas 17–12 „Pasirengimas asmens tapatybės informacijos saugumo pažeidimams ir reagavimas į juos“ (*Preparing for and Responding to a Breach of Personally Identifiable Information*), paskelbtas adresu https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf, ir VBT aplinkraštis Nr. A-130. Pavyzdžiui, Teisingumo departamento reagavimo į duomenų saugumo pažeidimus procedūros, žr. https://www.justice.gov/file/4336/download.

([184]) FRA, JAV kodekso 44 antraštinės dalies 3101 ir paskesni straipsniai.

([185]) Nacionalinė archyvų ir įrašų administracija turi įgaliojimus vertinti agentūros įrašų tvarkymo praktiką ir gali nustatyti, ar pagrįsta toliau saugoti tam tikrus įrašus (JAV kodekso 44 antraštinės dalies 2904 straipsnio c dalis ir 2906 straipsnis).

([186]) VBT aplinkraštis Nr. A-130, 5 skirsnio f punkto 1 papunkčio d dalis.

([187]) VBT aplinkraštis Nr. A-130, I priedėlio 3 straipsnio d dalis.

([188]) Taip pat žr. FTB vidaus tyrimų ir operacijų vadovo 14 skirsnį.

([189]) AGG-DOM VI skirsnio B ir C dalys; FTB vidaus tyrimų ir operacijų vadovo 14 skirsnis.

([190]) Šiame skirsnyje nurodyti mechanizmai taikomi ir tada, kai federalinės institucijos renka ir naudoja duomenis civiliniais ir reguliavimo tikslais. Federalines civilines ir reguliavimo agentūras tikrina jų atitinkami generaliniai inspektoriai ir prižiūri Kongresas, įskaitant Vyriausybės apskaitos tarnybą – Kongreso audito ir tyrimo agentūrą. Jeigu agentūra neturi paskirto privatumo ir piliečių laisvių pareigūno (tai pareigybė, kuri dėl atsakomybės už teisėsaugą ir nacionalinį saugumą paprastai yra tokiose agentūrose kaip Teisingumo departamentas ir Vidaus saugumo departamentas (VSD)), šios pareigos tenka vyresniajam agentūros privatumo apsaugos pareigūnui (angl. *Senior Agency Official for Privacy*, SAOP). Visos federalinės agentūros yra teisiškai įpareigotos paskirti SAOP, atsakingą už tai, kad agentūra laikytųsi teisės aktų dėl privatumo ir prižiūrėtų susijusius klausimus. Žr., pvz., VBT M-16–24 „Vyresniųjų agentūros privatumo apsaugos pareigūnų vaidmuo ir skyrimas“ (2016 m.).

(108) Pirma, įvairiuose baudžiamosios teisėsaugos įgaliojimų turinčiuose departamentuose dirba privatumo ir piliečių laisvių apsaugos pareigūnai ([191]). Nors konkretūs šių pareigūnų įgaliojimai gali šiek tiek skirtis priklausomai nuo įstatymo, kuriuo nustatomi įgaliojimai, paprastai šie įgaliojimai apima procedūrų priežiūrą siekiant užtikrinti, kad atitinkamas departamentas ar agentūra tinkamai atsižvelgtų į privatumo ir piliečių laisvių aspektus ir nustatytų tinkamas procedūras asmenų, manančių, kad jų privatumas arba piliečių laisvės buvo pažeistos, pateiktiems skundams nagrinėti. Kiekvieno departamento ar agentūros vadovai turi užtikrinti, kad privatumo ir piliečių laisvių apsaugos pareigūnai turėtų medžiagos ir išteklių savo įgaliojimams vykdyti, galėtų naudotis visa medžiaga ir darbuotojų paslaugomis, reikalingais jų funkcijoms vykdyti, ir būtų informuojami apie siūlomus politikos pakeitimus ir dėl tokių pakeitimų su jais būtų konsultuojamasi ([192]). Privatumo ir piliečių laisvių apsaugos pareigūnai periodiškai teikia ataskaitas Kongresui, be kita ko, nurodydami departamento ar agentūros gautų skundų skaičių ir pobūdį, taip pat tokių skundų nagrinėjimo, atliktų peržiūrų bei tyrimų ir pareigūno vykdytos veiklos poveikio santrauką ([193]).

(109) Antra, Teisingumo departamento, įskaitant FTB, veiklą prižiūri nepriklausomas generalinis inspektorius ([194]). Generaliniai inspektoriai yra teisiškai nepriklausomi ([195]) ir atsakingi už departamento programų ir operacijų nepriklausomus tyrimus, auditą ir patikrinimus. Jie turi galimybę susipažinti su visais įrašais, ataskaitomis, audito medžiaga, peržiūrų medžiaga, dokumentais, užrašais, rekomendacijomis ar kita susijusia medžiaga, prireikus remdamiesi potvarkiu, be to, gali priimti parodymus ([196]). Nors generaliniai inspektoriai teikia neprivalomas rekomendacijas dėl taisomųjų veiksmų, jų ataskaitos, be kita ko, dėl tolesnių veiksmų (arba neveikimo) ([197]), paprastai skelbiamos viešai ir siunčiamos Kongresui, o šis tuo pagrindu gali vykdyti savo priežiūros funkciją (žr. 111 konstatuojamąją dalį) ([198]).

([191]) Žr. JAV kodekso 42 antraštinės dalies 2000ee-1 straipsnį. Tai yra, pvz., Teisingumo departamentas, Vidaus saugumo departamentas ir FTB. Be to, VSD vyriausiasis privatumo apsaugos pareigūnas yra atsakingas už privatumo apsaugos priemonių palaikymą ir griežtinimą, taip pat skaidrumo skatinimą departamente (JAV kodekso 6 antraštinės dalies 142 straipsnis, 222 skirsnis). Visas VSD sistemas, technologijas, formas ir programas, kuriomis renkami asmens duomenys arba kurios turi poveikį privatumui, prižiūri vyriausiasis privatumo apsaugos pareigūnas, kuris gali susipažinti su visais departamentui prieinamais įrašais, ataskaitomis, audito medžiaga, peržiūrų medžiaga, dokumentais, užrašais, rekomendacijomis ir kita medžiaga, prireikus remdamasis potvarkiu. Privatumo apsaugos pareigūnas turi kasmet teikti Kongresui ataskaitas dėl departamento veiklos, kuri turi poveikį privatumui, įskaitant skundus dėl privatumo pažeidimų.

([192]) JAV kodekso 42 antraštinės dalies 2000ee-1 straipsnio d dalis.

([193]) Žr. JAV kodekso 42 antraštinės dalies 2000ee-1 straipsnio f dalies 1–2 punktus. Pavyzdžiui, iš Teisingumo departamento vyriausiojo privatumo ir piliečių laisvių apsaugos pareigūno ir Privatumo ir piliečių laisvių tarnybos ataskaitos už laikotarpį nuo 2020 m. spalio mėn. iki 2021 m. kovo mėn. matyti, kad buvo atliktos 389 privatumo aspektų peržiūros, be kita ko, informacinių sistemų ir kitų programų (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf.

([194]) Panašiai 2002 m. Vidaus saugumo aktu įsteigta generalinio inspektoriaus tarnyba Vidaus saugumo departamente.

([195]) Generalinių inspektorių postas yra užtikrintas ir juos gali atleisti tik Prezidentas, kuris privalo Kongresui raštu nurodyti tokio atleidimo priežastis.

([196]) Žr. 1978 m. Generalinių inspektorių akto 6 straipsnį.

([197]) Šiuo klausimu žr., pvz., Teisingumo departamento generalinio inspektoriaus tarnybos parengtą apžvalgą, kurioje apžvelgiamos jo pateiktos rekomendacijos ir jų įgyvendinimo mastas departamentams ir agentūroms vykdant tolesnius veiksmus (https://oig.justice.gov/sites/default/files/reports/22-043.pdf).

([198]) Žr. 1978 m. Generalinių inspektorių akto 4 straipsnio 5 dalį ir 5 straipsnį. Pavyzdžiui, Teisingumo departamento generalinio inspektoriaus tarnyba neseniai paskelbė savo pusmečio ataskaitą Kongresui (2021 m. spalio 1 d.–2022 m. kovo 31 d., https://oig.justice.gov/node/23596), kurioje apžvelgiami jos atlikto Teisingumo departamento programų ir operacijų audito, vertinimų, patikrinimų, specialių peržiūrų ir tyrimų rezultatai. Ši veikla apėmė buvusio rangovo tyrimą dėl neteisėto elektroninio stebėjimo (slapto asmens pokalbių pasiklausymo) atskleidimo vykstant tyrimui, o po šio tyrimo rangovui skirta bausmė. Generalinio inspektoriaus tarnyba taip pat atliko Teisingumo departamento agentūrų informacijos saugumo programų ir praktikos tyrimą, kuris apima reprezentatyvios agentūrų sistemų dalies informacijos saugumo politikos, procedūrų ir praktikos veiksmingumo patikrinimą.

(110) Trečia, baudžiamosios teisėsaugos įgaliojimų turinčius departamentus, vykdančius kovos su terorizmu veiklą, prižiūri Privatumo ir piliečių laisvių priežiūros valdyba (PCLOB), nepriklausoma vykdomosios valdžios agentūra, kurią sudaro dvipartinė penkių narių valdyba, Senatui pritarus Prezidento skiriama nustatytai šešerių metų kadencijai ([199]). Pagal PCLOB steigimo sutartį jai patikėta atsakomybė kovos su terorizmu politikos ir jos įgyvendinimo srityje, siekiant apsaugoti privatumą ir piliečių laisves. Atlikdama peržiūrą, ji gali susipažinti su visais aktualiais agentūros įrašais, ataskaitomis, audito medžiaga, peržiūrų medžiaga, dokumentais, užrašais ir rekomendacijomis, įskaitant įslaptintą informaciją, rengti pokalbius ir išklausyti parodymus ([200]). Ji gauna ataskaitas iš kelių federalinių departamentų ar agentūrų piliečių laisvių ir privatumo apsaugos pareigūnų ([201]), gali teikti rekomendacijas vyriausybei ir teisėsaugos institucijoms ir reguliariai teikia ataskaitas Kongreso komitetams bei Prezidentui ([202]). Valdybos ataskaitos, įskaitant ataskaitas Kongresui, turi būti kuo plačiau skelbiamos viešai ([203]).

(111) Galiausiai baudžiamosios teisėsaugos veiklą prižiūri specialūs JAV Kongreso komitetai (Atstovų Rūmų ir Senato teismų komitetai). Teismų komitetai vykdo reguliarią priežiūrą įvairiais būdais, visų pirma rengdami posėdžius, vykdydami tyrimus, peržiūras ir teikdami ataskaitas ([204]).

3.1.3. ***Teisių gynimas***

(112) Kaip nurodyta, baudžiamosios teisėsaugos institucijos daugeliu atvejų privalo gauti išankstinį teismo leidimą rinkti asmens duomenis. Nors administraciniams potvarkiams tai nebūtina, jie išduodami tik konkrečiais atvejais ir bus atliekama jų nepriklausoma teisminė peržiūra bent tais atvejais, kai valdžios institucijos siekia vykdymo užtikrinimo teisme. Visų pirma administracinių potvarkių gavėjai gali juos užginčyti teisme, motyvuodami tuo, kad jie yra nepagrįsti, t. y. pernelyg platūs, sunkiai įvykdomi ar sukeliantys per didelę naštą ([205]).

(113) Asmenys pirmiausia gali teikti prašymus ar skundus baudžiamosios teisėsaugos institucijoms dėl jų asmens duomenų tvarkymo. Jie taip pat gali prašyti prieigos prie asmens duomenų ir prašyti leisti juos ištaisyti ([206]). Dėl veiklos, susijusios su kova su terorizmu, asmenys taip pat gali pateikti skundą teisėsaugos institucijų privatumo ir piliečių laisvių apsaugos pareigūnams (arba kitiems privatumo apsaugos pareigūnams) ([207]).

(114) Be to, JAV teisėje numatyta įvairių asmenims prieinamų teisminių teisių gynimo būdų prieš valdžios instituciją arba jos pareigūną šiems tvarkant asmens duomenis ([208]). Tokiais būdais, visų pirma nustatytais Administracinio proceso akte (APA), Informacijos laisvės akte (FOIA) ir Elektroninių ryšių privatumo akte (ECPA), gali pasinaudoti visi asmenys, nepaisant jų pilietybės, laikydamiesi taikomų sąlygų.

([199]) Valdybos nariai turi būti atrenkami tik dėl jų profesinės kvalifikacijos, pasiekimų, reikšmės visuomenėje, kompetencijos piliečių laisvių ir privatumo srityje, taip pat dėl susijusios patirties, bet neatsižvelgiant į politinę priklausomybę. Jokiu būdu negali būti daugiau kaip trijų tai pačiai politinei partijai priklausančių valdybos narių. Į valdybą paskirtas asmuo, eidamas pareigas valdyboje, negali būti išrinktas federalinės vyriausybės tarnautojas, pareigūnas ar darbuotojas, išskyrus valdybos nario pareigas. Žr. JAV kodekso 42 antraštinės dalies 2000ee straipsnio h dalį.

([200]) JAV kodekso 42 antraštinės dalies 2000ee straipsnio g dalis.

([201]) Žr. JAV kodekso 42 antraštinės dalies 2000ee-1 straipsnio f dalies 1 punkto A papunkčio iii dalį. Be kita ko, bent iš Teisingumo departamento, Gynybos departamento, Vidaus saugumo departamento, taip pat bet kurio kito departamento, agentūros arba vykdomosios valdžios subjekto, kurį PCLOB paskyrė kaip tinkamą veikti tam tikroje srityje.

([202]) JAV kodekso 42 antraštinės dalies 2000ee straipsnio e dalis.

([203]) JAV kodekso 42 antraštinės dalies 2000ee straipsnio f dalis.

([204]) Pavyzdžiui, komitetai rengia teminius posėdžius (žr., pvz., neseniai surengtą Atstovų Rūmų teismų komiteto posėdį dėl nusikaltėlių skaitmeninių paieškos sistemų, https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983), taip pat reguliarius, pvz., FTB ir Teisingumo departamento, priežiūros posėdžius (žr. https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 ir https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899).

([205]) Žr. VI priedą.

([206]) VBT aplinkraščio Nr. A-130 II priedėlio 3 skirsnio a ir f punktai, pagal kuriuos reikalaujama, kad federalinės agentūros, gavusios asmenų prašymą, užtikrintų tinkamą prieigą prie duomenų, leistų juos ištaisyti ir nustatytų su privatumu susijusių skundų ir prašymų priėmimo ir nagrinėjimo procedūras.

([207]) Dėl, pavyzdžiui, Teisingumo departamento ir Vidaus saugumo departamento žr. JAV kodekso 42 antraštinės dalies 2000ee-1 straipsnį. Taip pat žr. VBT memorandumą M-16–24 „Vyresniųjų agentūros privatumo apsaugos pareigūnų vaidmuo ir skyrimas“.

([208]) Šiame skirsnyje nurodyti teisių gynimo mechanizmai taikomi ir tada, kai federalinės institucijos renka ir naudoja duomenis civiliniais ir reguliavimo tikslais.

(115) Paprastai pagal APA teisminės peržiūros nuostatas ([209]) „asmuo, kuris dėl agentūros veiksmų patyrė neigiamų teisinių padarinių, nukentėjo arba jo padėtis pablogėjo“, turi teisę kreiptis dėl teisminės peržiūros ([210]). Tai apima galimybę prašyti, kad teismas „agentūros veiksmus, sprendimus ir išvadas, kurie, kaip nustatyta <...> yra šališki, savavališki, kilę iš piktnaudžiavimo įgaliojimais ar kitaip neatitinka įstatymų, pripažintų neteisėtais ir panaikintų“ ([211]).

(116) Konkrečiau, ECPA ([212]) II antraštinėje dalyje įtvirtinta įstatymu nustatytų teisių į privatumą sistema, pagal kurią iš esmės reglamentuojama teisėsaugos institucijų galimybė susipažinti su laidinių, žodinių ar elektroninių ryšių turiniu, kurį saugo trečiosios šalys paslaugų teikėjai ([213]). Šiuo aktu kriminalizuojamas neteisėtas (t. y. teismo nesankcionuotas arba kitaip neleistinas) susipažinimas su tokių ryšių duomenimis, o nukentėjusiam asmeniui suteikiama galimybė pareikšti civilinį ieškinį JAV federaliniame teisme dėl faktinės ir baudinės žalos, taip pat lygiavertės arba deklaratyviosios teisių gynimo priemonės taikymo valdžios pareigūno, kuris sąmoningai įvykdė tokius neteisėtus veiksmus, arba Jungtinių Amerikos Valstijų atžvilgiu.

(117) Be to, keliais kitais įstatymais, kaip antai Pokalbių pasiklausymo aktu ([214]), Kompiuterinio sukčiavimo ir piktnaudžiavimo aktu ([215]), Federaliniu deliktinių reikalavimų aktu ([216]), Teisės į finansinį privatumą aktu ([217]) ir Sąžiningo kredito informacijos teikimo aktu ([218]), asmenims suteikiama teisė pareikšti ieškinį JAV valdžios institucijai arba pareigūnui dėl jų asmens duomenų tvarkymo.

([209]) JAV kodekso 5 antraštinės dalies 702 straipsnis.

([210]) Paprastai atliekama tik „galutinio“ (o ne „išankstinio, procesinio ar tarpinio“) agentūros veiksmo teisminė peržiūra. Žr. JAV kodekso 5 antraštinės dalies 704 straipsnį.

([211]) JAV kodekso 5 antraštinės dalies 706 straipsnio 2 dalies A punktas.

([212]) JAV kodekso 18 antraštinės dalies 2701–2712 straipsniai.

([213]) ECPA užtikrinama apsauga taikoma ryšių duomenims, saugomiems dviejų nurodytų klasių tinklo paslaugų teikėjų, t. y.: i) elektroninių ryšių paslaugų, pvz., telefonijos ar el. pašto; ii) nuotolinės kompiuterijos paslaugų, pvz., kompiuterinių saugojimo ar apdorojimo paslaugų.

([214]) JAV kodekso 18 antraštinės dalies 2510 ir paskesni straipsniai. Pagal Pokalbių pasiklausymo aktą (JAV kodekso 18 antraštinės dalies 2520 straipsnį) asmuo, kurio laidinių, žodinių arba elektroninių ryšių duomenys perimami, atskleidžiami arba sąmoningai naudojami, gali pareikšti civilinį ieškinį dėl Pokalbių pasiklausymo akto pažeidimo, be kita ko, tam tikromis aplinkybėmis – ieškinį atskiram valdžios pareigūnui arba Jungtinėms Amerikos Valstijoms. Dėl su turiniu nesusijusios informacijos (pvz., IP adreso, siunčiamų ir gaunamų el. laiškų adresų) rinkimo taip pat žr. 18 antraštinės dalies skyrių dėl renkamų numerių registratorių arba gaunamų skambučių sekiklių (JAV kodekso 18 antraštinės dalies 3121–3127 straipsniai ir dėl civilinių ieškinių – 2707 straipsnis).

([215]) JAV kodekso 18 antraštinės dalies 1030 straipsnis. Pagal Kompiuterinio sukčiavimo ir piktnaudžiavimo aktą asmuo gali pareikšti ieškinį bet kuriam asmeniui dėl tyčinės neleidžiamos prieigos (arba perteklinės leidžiamos prieigos), siekiant gauti informacijos iš finansų įstaigos, JAV valdžios sektoriaus kompiuterių sistemos arba kito konkretaus kompiuterio, be kita ko, tam tikromis aplinkybėmis – ieškinį atskiram valdžios pareigūnui.

([216]) JAV kodekso 28 antraštinės dalies 2671 ir paskesni straipsniai. Pagal Federalinį deliktinių reikalavimų aktą asmuo tam tikromis aplinkybėmis gali pareikšti ieškinį Jungtinėms Amerikos Valstijoms dėl „bet kurio Vyriausybės pareigūno aplaidaus arba neteisėto veiksmo arba neveikimo einant savo pareigas arba dirbant savo darbą“.

([217]) JAV kodekso 12 antraštinės dalies 3401 ir paskesni 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. Valdžios sektoriui susipažinti su saugomais finansiniais įrašais paprastai draudžiama, išskyrus atvejus, kai valdžios institucijos, remdamosi teisėtu potvarkiu arba kratos orderiu, pateikia prašymą arba, laikydamosi tam tikrų apribojimų, pateikia oficialų rašytinį prašymą, o asmeniui, kurio informacijos prašoma, pranešama apie tokį prašymą.

([218]) JAV kodekso 15 antraštinės dalies 1681–1681x straipsniai. Pagal Sąžiningo kredito informacijos teikimo aktą asmuo gali pareikšti ieškinį bet kuriam asmeniui, kuris nesilaiko reikalavimų (visų pirma reikalavimo turėti teisėtą leidimą), susijusių su vartojimo kredito ataskaitų rinkimu, platinimu ir naudojimu, arba tam tikromis sąlygomis toks ieškinys gali būti pareikštas vyriausybės agentūrai.

(118) Be to, pagal FOIA ([219]), JAV kodekso 5 antraštinės dalies 552 straipsnį kiekvienas asmuo turi teisę susipažinti su federalinės agentūros įrašais, įskaitant atvejus, kai juose yra jo asmens duomenys. Išnaudojęs administracines teisių gynimo priemones, asmuo gali pasinaudoti tokia teise susipažinti su dokumentais teisme, išskyrus atvejus, kai tokie įrašai nuo viešo atskleidimo saugomi taikant išimtį arba specialią vykdymo užtikrinimo netaikymo sąlygą ([220]). Šiuo atveju teismas įvertins, ar taikoma kokia nors išimtis arba ar atitinkama valdžios institucija ja rėmėsi teisėtai.

3.2. **JAV valdžios institucijų susipažinimas su duomenimis ir jų naudojimas nacionalinio saugumo tikslais**

(119) Jungtinių Amerikos Valstijų teisėje nustatyti įvairūs galimybės susipažinti su asmens duomenimis ir juos naudoti nacionalinio saugumo tikslais apribojimai ir apsaugos priemonės, taip pat numatyti priežiūros ir teisių gynimo mechanizmai, kurie atitinka šio sprendimo 89 konstatuojamojoje dalyje nurodytus reikalavimus. Paskesniuose skirsniuose išsamiai įvertinamos sąlygos, kuriomis tokia galimybė susipažinti su duomenimis gali būti suteikta, ir naudojantis tokiais įgaliojimais taikomos apsaugos priemonės.

3.2.1. ***Teisiniai pagrindai, apribojimai ir apsaugos priemonės***

3.2.1.1. *Taikoma teisinė sistema*

(120) Iš Sąjungos ES ir JAV DPS organizacijoms perduodamus asmens duomenis JAV valdžios institucijos nacionalinio saugumo tikslais gali rinkti remdamosi įvairiomis teisinėmis priemonėmis, laikydamosi konkrečių sąlygų ir apsaugos priemonių.

(121) Po to, kai Jungtinėse Amerikos Valstijose įsikūrusios organizacijos gavo asmens duomenis, JAV žvalgybos agentūros nacionalinio saugumo tikslais gali prašyti leisti susipažinti su tokiais duomenimis tik jei tai leidžiama pagal įstatymus, visų pirma pagal Užsienio žvalgybos informacijos sekimo aktą (FISA) arba įstatymų nuostatas, pagal kurias leidžiama susipažinti su duomenimis naudojant nacionalinio saugumo raštus (NSR) ([221]). FISA nustatyti keli teisiniai pagrindai, kuriais remiantis gali būti renkami (ir vėliau tvarkomi) pagal ES ir JAV DPS perduodami Sąjungos duomenų subjektų asmens duomenys (FISA 105 straipsnis ([222]), FISA 302 straipsnis ([223]), FISA 402 straipsnis ([224]), FISA 501 straipsnis ([225]) ir FISA 702 straipsnis ([226])), kaip išsamiau aprašyta 142–152 konstatuojamosiose dalyse.

([219]) JAV kodekso 5 antraštinės dalies 552 straipsnis.

([220]) Vis dėlto tokios išimtys yra aiškiai apibrėžtos. Pavyzdžiui, pagal JAV kodekso 5 antraštinės dalies 552 straipsnio b dalies 7 punktą FOIA nustatytos teisės negalioja „teisėsaugos tikslais parengtiems įrašams arba informacijai, bet tik tiek, kiek pateikus tokius teisėsaugos įrašus ar informaciją a) būtų galima pagrįstai tikėtis, kad tai trukdys nagrinėti teisėsaugos bylą, b) asmuo netektų teisės į teisingą bylos nagrinėjimą arba nešališką klausimo sprendimą teisme, c) būtų galima pagrįstai tikėtis, kad taip būtų neteisėtai kišamasi į asmens privatų gyvenimą, d) būtų galima pagrįstai tikėtis, kad taip būtų atskleista konfidencialaus informacijos šaltinio, įskaitant valstybės, vietos ar užsienio agentūrą ar instituciją arba bet kurią konfidencialios informacijos pateikusią privačią instituciją, tapatybė ir, jeigu įrašą arba informaciją parengė baudžiamosios teisėsaugos institucija vykdydama nusikalstamos veikos tyrimą arba agentūra atlikdama teisėtą nacionalinio saugumo žvalgybos tyrimą, konfidencialaus šaltinio pateikta informacija, e) būtų atskleisti teisėsaugos tyrimų ar baudžiamojo persekiojimo būdai ir procedūros arba būtų atskleistos teisėsaugos tyrimų ar baudžiamojo persekiojimo rekomendacijos, jeigu galima pagrįstai tikėtis, kad toks informacijos atskleidimas galėtų sukelti riziką, kad bus apeinami įstatymai, arba f) būtų galima pagrįstai tikėtis, kad dėl to kils pavojus bet kurio asmens gyvybei ar fiziniam saugumui“. Be to, „kai pateikiamas prašymas leisti susipažinti su įrašais [jei juos pateikus būtų galima pagrįstai tikėtis, kad tai trukdys nagrinėti teisėsaugos bylą] ir a) tyrimas arba byla yra susiję su galimu baudžiamosios teisės pažeidimu, ir b) yra pagrindo manyti, kad i) tyrimo arba bylos subjektas nežino apie vykstantį tyrimą ar bylą, ir ii) atskleidus informaciją apie įrašus būtų galima pagrįstai tikėtis, kad tai trukdys nagrinėti teisėsaugos bylą, agentūra gali tik tol, kol neišnyksta minėtos aplinkybės, įrašams netaikyti šio straipsnio reikalavimų“. (JAV kodekso 5 antraštinės dalies 552 straipsnio c dalies 1 punktas)

([221]) JAV kodekso 12 antraštinės dalies 3414 straipsnis, JAV kodekso 15 antraštinės dalies 1681u–1681v straipsniai ir JAV kodekso 18 antraštinės dalies 2709 straipsnis. Žr. 153 konstatuojamąją dalį.

([222]) JAV kodekso 50 antraštinės dalies 1804 straipsnis dėl tradicinio individualizuoto elektroninio stebėjimo.

([223]) JAV kodekso 50 antraštinės dalies 1822 straipsnis dėl fizinės kratos užsienio žvalgybos tikslais.

([224]) JAV kodekso 50 antraštinės dalies 1842 straipsnis su 18 antraštinės dalies 1841 straipsnio 2 dalimi ir 3127 straipsniu dėl renkamų numerių registratorių arba gaunamų skambučių sekiklių įrengimo.

([225]) JAV kodekso 50 antraštinės dalies 1861 straipsnis, pagal kurį FTB gali pateikti „prašymą išduoti įsakymą, kuriuo viešojo transporto vežėjui, viešajai apgyvendinimo įstaigai, fizinės saugyklos valdytojui ar transporto priemonių nuomos įmonei būtų leidžiama perduoti turimus įrašus tyrimui, kuriuo siekiama surinkti užsienio žvalgybos informacijos, arba tyrimui dėl tarptautinio terorizmo“.

([226]) JAV kodekso 50 antraštinės dalies 1881a straipsnis, pagal kurį JAV žvalgybos bendruomenės subjektams leidžiama prašyti JAV bendrovių leisti susipažinti su informacija, įskaitant interneto ryšių turinį, susijusia su tam tikrais ne Jungtinėse Amerikos Valstijose esančiais ne JAV piliečiais, naudojantis teisiškai privaloma elektroninių ryšių teikėjų pagalba.

(122) JAV žvalgybos agentūros taip pat turi galimybių rinkti asmens duomenis ne Jungtinėse Amerikos Valstijose, galimai įskaitant asmens duomenis, perduodamus tranzitu tarp Sąjungos ir Jungtinių Amerikos Valstijų. Duomenų rinkimas ne Jungtinėse Amerikos Valstijose grindžiamas Prezidento ([227]) išleistu Vykdomuoju potvarkiu Nr. 12333 (VP 12333) ([228]).

(123) Signalų žvalgybos duomenų rinkimas – žvalgybos duomenų rinkimo forma, aktualiausia šiai išvadai dėl tinkamumo, nes yra susijusi su elektroninių ryšių informacijos ir duomenų rinkimu iš informacinių sistemų. Tokiu būdu JAV žvalgybos agentūros gali rinkti duomenis tiek Jungtinėse Amerikos Valstijose (remdamosi FISA), tiek duomenis perduodant į Jungtines Amerikos Valstijas (remdamosi VP 12333).

(124) 2022 m. spalio 7 d. JAV prezidentas paskelbė VP 14086 dėl Jungtinių Amerikos Valstijų signalų žvalgybos apsaugos priemonių griežtinimo, kuriame visai JAV signalų žvalgybos veiklai nustatyti apribojimai ir apsaugos priemonės. Šiuo vykdomuoju potvarkiu, kuriuo iš esmės pakeičiama Prezidento politikos direktyva Nr. 28 (PPD-28) ([229]), sugriežtinamos sąlygos, apribojimai ir apsaugos priemonės, taikomi visai signalų žvalgybos veiklai (t. y. remiantis FISA ir VP 12333), nepriklausomai nuo to, kur ji vykdoma ([230]), ir sukuriamas naujas teisių gynimo mechanizmas, pagal kurį asmenys gali pasinaudoti šiomis apsaugos priemonėmis ir užtikrinti jų vykdymą ([231]) (išsamesnės informacijos pateikiama 176–194 konstatuojamosiose dalyse). Tokiu būdu JAV teisėje įgyvendinami ES ir JAV derybų, vykusių Teisingumo Teismui Komisijos sprendimą dėl privatumo skydo tinkamumo pripažinus negaliojančiu (žr. 6 konstatuojamąją dalį), rezultatai. Todėl tai yra ypač svarbus šiame sprendime vertinamos teisinės sistemos elementas.

(125) VP 14086 nustatytais apribojimais ir apsaugos priemonėmis papildomi FISA 702 straipsnyje ir VP 12333 nustatyti apribojimai ir apsaugos priemonės. Toliau (3.2.1.2 ir 3.2.1.3 skirsniuose) aprašytus reikalavimus žvalgybos agentūros turi taikyti vykdydamos signalų žvalgybos veiklą pagal FISA 702 straipsnį ir VP 12333, pvz., atrinkdamos ir (arba) nustatydamos pagal FISA 702 straipsnį gautinos užsienio žvalgybos informacijos kategorijas; rinkdamos užsienio žvalgybos ar kontržvalgybos duomenis pagal VP 12333 ir priimdamos individualius konkrečius sprendimus pagal FISA 702 straipsnį ir VP 12333.

(126) Šiame Prezidento paskelbtame vykdomajame potvarkyje nustatyti reikalavimai privalomi visai žvalgybos bendruomenei. Jie turi būti toliau įgyvendinami taikant agentūrų politiką ir procedūras, kad virstų konkrečiais nurodymais kasdienei veiklai. Šiuo atžvilgiu VP 14086 JAV žvalgybos agentūroms nustatomas ne ilgesnis kaip vienų metų laikotarpis esamai politikai ir procedūroms atnaujinti (t. y. iki 2023 m. spalio 7 d.), kad jos atitiktų vykdomajame potvarkyje nustatytus reikalavimus. Tokia atnaujinta politika ir procedūros turi būti parengtos konsultuojantis su generaliniu prokuroru, Nacionalinės žvalgybos direktoriaus tarnybos piliečių laisvių apsaugos pareigūnu (ODNI CLPO) ir PCLOB – nepriklausoma priežiūros įstaiga, įgaliota peržiūrėti vykdomosios valdžios politiką ir jos įgyvendinimą, siekiant apsaugoti privatumą ir piliečių laisves (žr. 110 konstatuojamąją dalį dėl PCLOB vaidmens ir statuso), – ir turi būti skelbiamos viešai ([232]). Be to, kai atnaujinta politika ir procedūros bus įdiegtos,

([227]) Pagal JAV Konstitucijos II straipsnį atsakomybė užtikrinti nacionalinį saugumą, įskaitant, visų pirma, užsienio žvalgybos informacijos rinkimą, priklauso Prezidento, kaip ginkluotųjų pajėgų vado, kompetencijai.

([228]) VP 12333. Jungtinių Amerikos Valstijų žvalgybos veikla, Federalinis registras, 40 tomas, Nr. 235 (1981 m. gruodžio 8 d. su pataisymais, padarytais 2008 m liepos 30 d.). VP 12333 plačiau apibrėžiami JAV žvalgybos veiklos tikslai, kryptys, pareigos ir atsakomybės sritys (įskaitant įvairių žvalgybos bendruomenės subjektų vaidmenį), taip pat nustatomi bendrieji žvalgybos veiklos vykdymo parametrai.

([229]) VP 14086 pakeičiama ankstesnė Prezidento direktyva, t. y. PPD 28, išskyrus jos 3 straipsnį ir papildomą priedą (pagal kurį reikalaujama, kad žvalgybos agentūros kasmet peržiūrėtų savo signalų žvalgybos prioritetus ir reikalavimus, atsižvelgdamos į signalų žvalgybos veiklos naudą JAV nacionaliniams interesams ir tos veiklos keliamą riziką), taip pat 6 straipsnį (kuriame pateikiamos bendrosios nuostatos); žr. Nacionalinio saugumo memorandumą dėl dalinio Prezidento politikos direktyvos Nr. 28 atšaukimo, pateikiamą adresu https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/.

([230]) Žr. VP 14086 5 straipsnio f dalį, kurioje paaiškinama, kad vykdomojo potvarkio taikymo sritis yra tokia pati kaip PPD-28, kuri, kaip nurodyta jo 3 išnašoje, buvo taikoma signalų žvalgybos veiklai, vykdomai siekiant rinkti ryšių duomenis ar informaciją apie ryšius, išskyrus signalų žvalgybos veiklą, vykdomą siekiant išbandyti ar plėsti signalų žvalgybos pajėgumus.

([231]) Šiuo klausimu žr., pvz., VP 14086 5 straipsnio h dalį, kurioje paaiškinama, kad vykdomajame potvarkyje nustatytomis apsaugos priemonėmis sukuriama teisiškai įtvirtinta teisė ir asmenys gali užtikrinti jų vykdymą naudodamiesi teisių gynimo mechanizmu.

([232]) Žr. VP 14086 2 straipsnio c dalies iv punkto C papunktį.

PCLOB atliks peržiūrą, siekdama užtikrinti, kad jos atitiktų vykdomąjį potvarkį. Per 180 dienų po to, kai PCLOB užbaigs tokią peržiūrą, kiekviena žvalgybos agentūra turi atidžiai apsvarstyti ir įgyvendinti visas PCLOB rekomendacijas arba kitaip į jas atsižvelgti. 2023 m. liepos 3 d. JAV vyriausybė paskelbė minėtą atnaujintą politiką ir procedūras ([233]).

3.2.1.2. *Apribojimai ir apsaugos priemonės, susiję su asmens duomenų rinkimu nacionalinio saugumo tikslais*

(127) VP 14086 nustatyti tam tikri bendrieji reikalavimai, taikomi visai signalų žvalgybos veiklai (asmens duomenų rinkimui, naudojimui, platinimui ir kt.).

(128) Pirma, tokia veikla turi būti grindžiama įstatymu arba Prezidento įgaliojimu ir vykdoma laikantis JAV teisės, įskaitant Konstituciją ([234]).

(129) Antra, turi būti įdiegtos tinkamos apsaugos priemonės, kuriomis būtų užtikrinama, kad privatumas ir piliečių laisvės būtų neatsiejami tokios veiklos planavimo aspektai ([235]).

(130) Visų pirma bet kokia signalų žvalgybos veikla gali būti vykdoma tik „remiantis pagrįstu visų aktualių veiksnių įvertinimu nustačius, kad tokia veikla yra būtina siekiant įgyvendinti patvirtintą žvalgybos prioritetą“ (dėl sąvokos „patvirtintas žvalgybos prioritetas“ žr. 135 konstatuojamąją dalį) ([236]).

(131) Be to, tokia veikla gali būti vykdoma tik „tokiu mastu ir tokiu būdu, kuris yra proporcingas patvirtintam žvalgybos prioritetui, dėl kurio buvo suteiktas leidimas“ ([237]). Kitaip tariant, turi būti pasiekta tinkama pusiausvyra „tarp žvalgybos prioriteto įgyvendinimo svarbos ir poveikio atitinkamų asmenų privatumui ir piliečių laisvėms, nepaisant tų asmenų pilietybės ar gyvenamosios vietos“ ([238]).

(132) Galiausiai, siekiant užtikrinti, kad būtų laikomasi šių bendrųjų reikalavimų, kurie atspindi teisėtumo, būtinumo ir proporcingumo principus, signalų žvalgybos veikla yra prižiūrima (išsamesnės informacijos pateikiama 3.2.2 skirsnyje) ([239]).

(133) Šie bendrieji reikalavimai dėl signalų žvalgybos duomenų rinkimo papildomi įvairiomis sąlygomis ir apribojimais, kuriais užtikrinama, kad asmenų teisės būtų ribojamos tik tiek, kiek yra būtina ir proporcinga siekiant teisėto tikslo.

(134) Pirma, vykdomuoju potvarkiu dvejopai apribojami pagrindai, kuriais remiantis gali būti renkami duomenys vykdant signalų žvalgybos veiklą. Viena vertus, vykdomajame potvarkyje nurodomi teisėti tikslai, kurių gali būti siekiama renkant signalų žvalgybos duomenis, pvz., suprasti ar įvertinti užsienio organizacijų, įskaitant tarptautines teroristines organizacijas, pajėgumus, ketinimus ar veiklą, kurie kelia arba gali kelti grėsmę Jungtinių Amerikos Valstijų nacionaliniam saugumui; apsaugoti nuo užsienio karinių pajėgumų ir veiklos; suprasti ar įvertinti tarpvalstybinio pobūdžio grėsmes, darančias poveikį pasaulio saugumui, pvz., klimato ir kitus ekologinius pokyčius, riziką visuomenės sveikatai ir humanitarines grėsmes ([240]). Kita vertus, vykdomajame potvarkyje nurodomi tam tikri

([233]) https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086.

([234]) VP 14086 2 straipsnio a dalies i punktas.

([235]) VP 14086 2 straipsnio a dalies ii punktas.

([236]) VP 14086 2 straipsnio a dalies ii punkto A papunktis. Signalų žvalgyba ne visada turi būti vienintelė priemonė siekiant įgyvendinti tam tikrus patvirtinto žvalgybos prioriteto aspektus. Pavyzdžiui, signalų žvalgybos duomenų rinkimas gali būti naudojamas siekiant užtikrinti alternatyvius patvirtinimo būdus (pvz., iš kitų žvalgybos šaltinių gautai informacijai patvirtinti) arba patikimą galimybę gauti tą pačią informaciją (VP 14086 2 straipsnio c dalies i punkto A papunktis).

([237]) VP 14086 2 straipsnio a dalies ii punkto B papunktis.

([238]) VP 14086 2 straipsnio a dalies ii punkto B papunktis.

([239]) VP 14086 2 straipsnio a dalies iii punktas kartu su 2 straipsnio d dalimi.

([240]) VP 14086 2 straipsnio b dalies i punktas. Vykdomajame potvarkyje teisėtų tikslų sąrašas yra ribotas ir neapima galimų būsimų grėsmių, todėl tame VP yra numatyta galimybė, kad, atsiradus naujų nacionalinio saugumo reikalavimų, pavyzdžiui, naujų grėsmių nacionaliniam saugumui, Prezidentas šį sąrašą gali atnaujinti. Tokie atnaujinimai iš esmės turi būti skelbiami viešai, nebent Prezidentas mano, kad tai padarius savaime kiltų rizika Jungtinių Amerikos Valstijų nacionaliniam saugumui (VP 14086 2 straipsnio b dalies i punkto B papunktis).

tikslai, kurių vykdant signalų žvalgybos veiklą niekada negali būti siekiama, pvz., sudaryti sunkesnes sąlygas asmenims ar žiniasklaidai kritikuoti, prieštarauti arba laisvai reikšti idėjas ar politines pažiūras; sudaryti nepalankias sąlygas asmenis dėl jų etninės kilmės, rasės, lyties, lytinės tapatybės, seksualinės orientacijos ar religijos; suteikti konkurencinį pranašumą JAV bendrovėms ([241]).

(135) Be to, siekdamos pagrįsti signalų žvalgybos duomenų rinkimą, žvalgybos agentūros negali tiesiog remtis VP 14086 nustatytais teisėtais tikslais, bet turi juos operatyviniais tikslais papildomai paremti konkretesniais prioritetais, pagal kuriuos gali būti renkami signalų žvalgybos duomenys. Kitaip tariant, faktiškai duomenys gali būti renkami tik siekiant įgyvendinti konkretesnį prioritetą. Tokie prioritetai nustatomi vykdant specialų procesą, kuriuo siekiama užtikrinti, kad būtų laikomasi taikomų teisinių reikalavimų, be kita ko, susijusių su privatumu ir piliečių laisvėmis. Konkrečiau, žvalgybos prioritetus pirmiausia parengia Nacionalinės žvalgybos direktorius (pagal vadinamąją Nacionalinę žvalgybos prioritetų sistemą) ir pateikia Prezidentui patvirtinti ([242]). Prieš siūlydamas žvalgybos prioritetus Prezidentui, direktorius pagal VP 14086 privalo iš Nacionalinės žvalgybos direktoriaus tarnybos piliečių laisvių apsaugos pareigūno (ODNI CLPO) gauti kiekvieno prioriteto vertinimą, ar 1) pagal jį siekiama vieno ar kelių vykdomajame potvarkyje nurodytų teisėtų tikslų; 2) jis nebuvo skirtas ar numatytas tam, kad signalų žvalgybos duomenys būtų renkami vykdomajame potvarkyje nurodytu draudžiamu tikslu ir 3) jis buvo nustatytas tinkamai atsižvelgus į visų asmenų privatumą ir piliečių laisves, nepaisant jų pilietybės ar gyvenamosios vietos ([243]). Jeigu direktorius su CLPO vertinimu nesutinka, Prezidentui turi būti pateikiamos abi nuomonės ([244]).

(136) Todėl šiuo procesu visų pirma užtikrinama, kad į privatumo aspektus būtų atsižvelgiama nuo pradinio etapo, kuriame nustatomi žvalgybos prioritetai.

(137) Antra, kai žvalgybos prioritetas jau nustatytas, sprendimas, ar galima rinkti signalų žvalgybos duomenis ir kokiu mastu tai galima daryti įgyvendinant tą prioritetą, priimamas paisant kelių reikalavimų. Šiais reikalavimais praktiškai įgyvendinami bendrieji būtinumo ir proporcingumo standartai, nustatyti Vykdomojo potvarkio 2 straipsnio a dalyje.

(138) Visų pirma signalų žvalgybos duomenys gali būti renkami tik „remiantis pagrįstu visų aktualių veiksnių įvertinimu nustačius, kad duomenis rinkti būtina siekiant įgyvendinti konkretų žvalgybos prioritetą“ ([245]). Nustatydamos, ar konkreti signalų žvalgybos duomenų rinkimo veikla yra būtina siekiant įgyvendinti patvirtintą žvalgybos prioritetą, JAV žvalgybos agentūros turi apsvarstyti, ar galima naudotis kitais mažiau intervenciniais šaltiniais ir metodais, be kita ko, iš diplomatinių ir viešų šaltinių, ir ar tokie šaltiniai ir metodai yra įmanomi ir tinkami ([246]). Jeigu įmanoma, pirmumas turi būti teikiamas tokiems alternatyviems, mažiau intervenciniams šaltiniams ir metodams ([247]).

(139) Kai taikant tokius kriterijus nusprendžiama, kad rinkti signalų žvalgybos duomenis būtina, tai turi būti daroma „kuo labiau pritaikant“ ir „nedarant neproporcingo poveikio privatumui ir piliečių laisvėms“ ([248]). Siekiant užtikrinti, kad privatumui ir piliečių laisvėms nebūtų daromas neproporcingas poveikis, t. y. siekiant tinkamos nacionalinio saugumo poreikių ir privatumo bei piliečių laisvių apsaugos pusiausvyros, reikia deramai atsižvelgti į visus aktualius veiksnius, kaip antai į siekiamo tikslo pobūdį; duomenų rinkimo veiklos intervencinį pobūdį, įskaitant jos trukmę; tikėtiną duomenų rinkimo indėlį siekiant tikslo; pagrįstai numatomas pasekmes asmenims; numatomų rinkti duomenų pobūdį ir būtinybę jų neskelbti ([249]).

([241]) VP 14086 2 straipsnio b dalies ii punktas.
([242]) Nacionalinio saugumo akto 102A straipsnis ir VP 14086 2 straipsnio b dalies iii punktas.
([243]) Išimtiniais atvejais (visų pirma, kai toks procesas negali būti vykdomas, nes reikia atsižvelgti į naują ar kylantį žvalgybos reikalavimą), tokius prioritetus gali tiesiogiai nustatyti Prezidentas arba žvalgybos bendruomenės subjekto vadovas, ir jie iš esmės turi taikyti tuos pačius kriterijus, kaip aprašytieji 2 straipsnio b dalies iii punkto A papunkčio 1–3 pastraipose; žr. VP 14086 4 straipsnio n dalį.
([244]) VP 14086 2 straipsnio b dalies iii punkto C papunktis.
([245]) VP 14086 2 straipsnio b dalis ir c dalies i punkto A papunktis.
([246]) VP 14086 2 straipsnio c dalies i punkto A papunktis.
([247]) VP 14086 2 straipsnio c dalies i punkto A papunktis.
([248]) VP 14086 2 straipsnio c dalies i punkto B papunktis.
([249]) VP 14086 2 straipsnio c dalies i punkto B papunktis.

(140) Atsižvelgiant į signalų žvalgybos duomenų rinkimo tipą, duomenų rinkimas Jungtinėse Amerikos Valstijose, kuris yra aktualiausias šiai išvadai dėl tinkamumo, nes yra susijęs su organizacijoms JAV perduotais duomenimis, visada turi būti tikslinis, kaip išsamiau paaiškinta 142–153 konstatuojamosiose dalyse.

(141) Vadinamasis masinis duomenų rinkimas ([250]) gali būti atliekamas tik ne Jungtinėse Amerikos Valstijose, remiantis VP 12333. Pagal VP 14086 ir tokiu atveju pirmumas turi būti teikiamas tiksliniam rinkimui ([251]). Priešingai, masinis duomenų rinkimas leidžiamas tik tuo atveju, jei informacijos, būtinos patvirtintam žvalgybos prioritetui įgyvendinti, pagrįstai negalima gauti duomenis renkant tikslingai ([252]). Kai būtina ne Jungtinėse Amerikos Valstijose vykdyti masinį duomenų rinkimą, pagal VP 14086 taikomos specialios apsaugos priemonės ([253]). Pirma, turi būti taikomi metodai ir techninės priemonės, kad duomenų būtų renkama ne daugiau, nei būtina patvirtintam žvalgybos prioritetui įgyvendinti, taip pat būtų renkama kuo mažiau nesusijusios informacijos ([254]). Antra, vykdomajame potvarkyje nustatyta, kad masiškai surinkta informacija (įskaitant užklausas) gali būti naudojama tik šešiais konkrečiais tikslais, be kita ko, siekiant užtikrinti apsaugą nuo užsienio valstybės valdžios, organizacijos ar asmens arba jų vardu vykdomo terorizmo, įkaitų paėmimo ir asmenų laisvės apribojimo; siekiant užtikrinti apsaugą nuo užsienio šnipinėjimo, sabotažo ar nužudymo; siekiant užtikrinti apsaugą nuo masinio naikinimo ginklų ar susijusių technologijų kūrimo, turėjimo ar platinimo grėsmės ir susijusių grėsmių ([255]). Galiausiai bet kokia užklausa dėl masiškai gaunamų signalų žvalgybos duomenų gali būti teikiama tik jei tai būtina patvirtintam žvalgybos prioritetui įgyvendinti, siekiant tų šešių tikslų ir laikantis politikos bei procedūrų, kuriomis tinkamai atsižvelgiama į užklausų poveikį visų asmenų privatumui ir piliečių laisvėms, neatsižvelgiant į jų pilietybę ar gyvenamąją vietą ([256]).

(142) Organizacijai Jungtinėse Amerikos Valstijose perduotų duomenų signalų žvalgybos duomenų rinkimui taikomi ne tik VP 14086 nustatyti reikalavimai, bet ir specialūs apribojimai bei apsaugos priemonės, reglamentuojami FISA 702 straipsniu ([257]). Pagal FISA 702 straipsnį leidžiama rinkti užsienio žvalgybos informaciją stebint ne JAV piliečius, kaip pagrįstai manoma, esančius ne Jungtinėse Amerikos Valstijose, naudojantis būtinąja JAV elektroninių ryšių paslaugų teikėjų pagalba ([258]). Kad galėtų rinkti užsienio žvalgybos informaciją pagal FISA 702 straipsnį,

([250]) T. y. didelio kiekio signalų žvalgybos duomenų, kurie dėl techninių ar operatyvinių priežasčių gaunami nenaudojant atskyrimo priemonių (pvz., netaikant konkrečių identifikatorių ar atrankos sąlygų), rinkimas; žr. VP 14086 4 straipsnio b dalį. Remiantis VP 14086 ir kaip išsamiau paaiškinta 141 konstatuojamojoje dalyje, pagal VP 12333 duomenys masiškai renkami tik jei tai būtina siekiant įgyvendinti konkrečius patvirtintus žvalgybos prioritetus ir paisant tam tikrų apribojimų ir apsaugos priemonių, skirtų užtikrinti, kad su duomenimis nebūtų galima susipažinti be atrankos. Todėl masinis duomenų rinkimas turi būti skiriamas nuo duomenų rinkimo bendrai ir be atrankos (masinio stebėjimo), netaikant apribojimų ir apsaugos priemonių.

([251]) VP 14086 2 straipsnio c dalies ii punkto A papunktis.

([252]) VP 14086 2 straipsnio c dalies ii punkto A papunktis.

([253]) VP 14086 nustatytos specialios taisyklės dėl masinio duomenų rinkimo taip pat taikomos tikslinio signalų žvalgybos duomenų rinkimo veiklai, kurią vykdant laikinai naudojami duomenys, gauti nenaudojant atskyrimo priemonių (pvz., netaikant konkrečių atrankos sąlygų ar identifikatorių), t. y. masiškai (tai įmanoma daryti tik už Jungtinių Amerikos Valstijų teritorijos ribų). Taip nėra, kai tokie duomenys naudojami pradiniam tikslinio signalų žvalgybos duomenų rinkimo veiklos techniniam etapui remti, saugomi tik trumpą laiką, kiek reikia šiam etapui užbaigti, ir iš kart po to ištrinami (VP 14086 2 straipsnio c dalies ii punkto D papunktis). Šiuo atveju vienintelis pradinio duomenų rinkimo nenaudojant atrankos priemonių tikslas – sudaryti sąlygas tiksliniam informacijos rinkimui taikant konkretų identifikatorių arba atrankos sąlygą. Pagal tokį scenarijų į valdžios sektoriaus duomenų bazes įrašomi tik tam tikrą taikomą atrankos priemonę atitinkantys duomenys, o kiti duomenys sunaikinami. Todėl toks tikslinis duomenų rinkimas ir toliau reglamentuojamas bendrosiomis taisyklėmis, galiojančiomis renkant signalų žvalgybos duomenis, be kita ko, VP 14086 2 straipsnio a ir b dalimis ir 2 straipsnio c dalies i punktu.

([254]) VP 14086 2 straipsnio c dalies ii punkto A papunktis.

([255]) VP 14086 2 straipsnio c dalies ii punkto B papunktis. Jeigu atsiranda naujų nacionalinio saugumo reikalavimų, pvz., naujų grėsmių nacionaliniam saugumui, Prezidentas šį sąrašą gali atnaujinti. Tokie atnaujinimai iš esmės turi būti skelbiami viešai, nebent Prezidentas mano, kad tai padarius savaime kiltų rizika Jungtinių Amerikos Valstijų nacionaliniam saugumui (VP 14086 2 straipsnio c dalies ii punkto C papunktis). Dėl užklausų, susijusių su masiškai surinktais duomenimis, žr. VP 14086 2 straipsnio c dalies iii punkto D papunktį.

([256]) VP 14086 2 straipsnio a dalies ii punkto A papunktis kartu su 2 straipsnio c dalies iii punkto D papunkčiu. Taip pat žr. VII priedą.

([257]) JAV kodekso 50 antraštinės dalies 1881 straipsnis.

([258]) JAV kodekso 50 antraštinės dalies 1881a straipsnio a dalis. Visų pirma, kaip pažymėjo PCLOB, stebėjimas pagal 702 straipsnį „taikomas tik konkretiems asmenims (ne JAV piliečiams), kurių informaciją norima rinkti, dėl kurių priimtas individualus sprendimas“ (Privatumo ir piliečių laisvių priežiūros valdyba, 2014 m. liepos 2 d. ataskaita dėl pagal Užsienio žvalgybos informacijos sekimo akto 702 straipsnį vykdomos stebėjimo programos (Ataskaita dėl 702 straipsnio), p. 111). Taip pat žr. NSA CLPO, 2014 m. balandžio 16 d. NSA užsienio žvalgybos akto 702 straipsnio įgyvendinimo ataskaitą. Sąvoka „elektroninių ryšių paslaugų teikėjas“ apibrėžta JAV kodekso 50 antraštinės dalies 1881 straipsnio a dalies 4 punkte.

generalinis prokuroras ir Nacionalinės žvalgybos direktorius Užsienio žvalgybos stebėjimo teismui (FISC) pateikia metinius sertifikatus, kuriuose nurodomos gautinos užsienio žvalgybos informacijos kategorijos ([259]). Kartu su sertifikavimu turi būti nurodomos asmenų, kurių informaciją norima rinkti, nustatymo, duomenų kiekio mažinimo ir užklausų teikimo procedūros, kurias taip pat patvirtina Teismas ir kurios JAV žvalgybos agentūroms yra teisiškai privalomos.

(143) FISC – federaliniu įstatymu įsteigtas nepriklausomas teismas ([260]), kurio sprendimai gali būti skundžiami Užsienio žvalgybos stebėjimo apeliaciniam teismui (FISCR) ([261]) ir galiausiai Jungtinių Amerikos Valstijų Aukščiausiajam Teismui ([262]). FISC (ir FISCR) padeda nuolatinė penkių teisininkų ir penkių techninių ekspertų kolegija, turinti kompetenciją spręsti nacionalinio saugumo ir su piliečių laisvėmis susijusius klausimus ([263]). Iš šios grupės teismas paskiria asmenį, kuris veikia kaip *amicus curiae* ir padeda nagrinėti visus prašymus dėl nutarties arba peržiūros, kai, teismo nuomone, pateikiamas naujas ar reikšmingas teisės paaiškinimas, nebent teismas nustato, kad paskirti tokį asmenį netikslinga ([264]). Taip visų pirma užtikrinama, kad teismo vertinime būti tinkamai atsižvelgiama į privatumo aspektus. Teismas taip pat gali paskirti asmenį arba organizaciją, kuris (-i) veiktų kaip *amicus curiae*, be kita ko, teiktų technines konsultacijas, kai mano, kad tai tikslinga, arba gavęs prašymą suteikti asmeniui arba organizacijai leidimą pateikti *amicus curiae* raštą ([265]).

(144) FISC peržiūri sertifikatus ir susijusias procedūras (visų pirma asmenų, kurių informaciją norima rinkti, nustatymo ir duomenų kiekio mažinimo procedūras), ar jie atitinka FISA reikalavimus. Jeigu mano, kad reikalavimų nesilaikoma, jis gali visiškai arba iš dalies atsisakyti išduoti sertifikatą ir prašyti iš dalies pakeisti procedūras ([266]). Šiuo atžvilgiu FISC ne kartą patvirtino, kad peržiūri ne tik 702 straipsnyje pateiktus asmenų, kurių informaciją norima rinkti, nustatymo ir duomenų kiekio mažinimo procedūrų aprašymus, bet ir tai, kaip valdžios sektorius įgyvendina šias procedūras ([267]).

(145) Individualius sprendimus dėl asmenų, kurių informaciją norima rinkti, nustatymo priima Nacionalinio saugumo agentūra (NSA, žvalgybos agentūra, atsakinga už asmenų, kurių informaciją norima rinkti, nustatymą pagal FISA 702 skirsnį) laikydamasi FISC patvirtintų asmenų, kurių informaciją norima rinkti, nustatymo procedūrų, pagal kurias reikalaujama, kad NSA, atsižvelgdama į visas aplinkybes, įvertintų, ar renkant konkretaus asmens informaciją veikiausiai bus gauta sertifikate nurodytos tam tikros kategorijos užsienio žvalgybos informacijos ([268]). Toks

([259]) JAV kodekso 50 antraštinės dalies 1881a straipsnio g dalis.

([260]) FISC sudaro teisėjai, Jungtinių Amerikos Valstijų vyriausiojo teisėjo paskirti iš dirbančių JAV apygardų teismų teisėjų, kuriuos anksčiau paskyrė Prezidentas ir patvirtino Senatas. Teisėjai, kurie eiti pareigas skiriami iki gyvos galvos ir gali būti atleisti tik dėl svarios priežasties, FISC pareigas eina po septynerių metų kadenciją. FISA reikalaujama, kad teisėjai būtų atrinkti bent iš septynių skirtingų JAV teismo apygardų. Žr. JAV kodekso 50 antraštinės dalies 1803 straipsnio a dalį. Teisėjams padeda patyrę teismų tarnautojai – teismų darbuotojai teisininkai, kurie rengia prašymų rinkti duomenis teisinę analizę. Žr. JAV užsienio žvalgybos stebėjimo teismo pirmininko Reggie B. Waltono raštą JAV Senato Teisminių institucijų komiteto pirmininkui Patrickui J. Leahy (2013 m. liepos 29 d.) (toliau – Waltono raštas), p. 2, pateikiamą adresu https://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([261]) FISCR sudaro Jungtinių Amerikos Valstijų vyriausiojo teisėjo paskirti, iš JAV apygardų teismų ar apeliacinių teismų atrinkti teisėjai, ir jie šias pareigas eina po septynerių metų kadenciją. Žr. JAV kodekso 50 antraštinės dalies 1803 straipsnio b dalį.

([262]) Žr. JAV kodekso 50 antraštinės dalies 1803 straipsnio b dalį, 1861a straipsnio f dalį, 1881a straipsnio h dalį, 1881a straipsnio i dalies 4 punktą.

([263]) JAV kodekso 50 antraštinės dalies 1803 straipsnio i dalies 1 punktas ir 3 punkto A papunktis.

([264]) JAV kodekso 50 antraštinės dalies 1803 straipsnio i dalies 2 punkto A papunktis.

([265]) JAV kodekso 50 antraštinės dalies 1803 straipsnio i dalies 2 punkto B papunktis.

([266]) Žr., pvz., 2018 m. spalio 18 d. FISC nuomonę, pateikiamą adresu athttps://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf , kaip patvirtinta 2019 m. liepos 12 d. Užsienio žvalgybos apeliacinio teismo nuomonėje, pateikiamoje adresu athttps://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf .

([267]) Žr., pvz., FISC memorandumo nuomonę ir įsakymą, p. 35 (2020 m. lapkričio 18 d.) (leista viešai skelbti 2021 m. balandžio 26 d.) (D priedas).

([268]) JAV kodekso 50 antraštinės dalies 1881a straipsnio a dalis. 2018 m. kovo mėn. paskelbtos procedūros, kurias taiko Nacionalinio saugumo agentūra, siekdama nustatyti ne Jungtinių Amerikos Valstijų piliečius, kurie, kaip pagrįstai manoma, yra ne Jungtinėse Amerikos Valstijose, kad gautų užsienio žvalgybos informacijos pagal 1978 m. Užsienio žvalgybos informacijos sekimo akto su pakeitimais 702 straipsnį (NSA asmenų, kurių informaciją norima rinkti, nustatymo procedūros), pateikiamos adresu athttps://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, p. 1–4, išsamiau paaiškinamos PCLOB ataskaitoje, p. 41–42.

vertinimas turi būti individualus ir pagrįstas faktais, paremtas analitiko analitiniu vertinimu, specialiu išsilavinimu ir patirtimi, taip pat turi būti atsižvelgiama į gautinos užsienio žvalgybos informacijos pobūdį ([269]). Asmenys, kurių informaciją norima rinkti, nustatomi identifikuojant vadinamuosius atrinktuvus, kuriais nustatomos konkrečios ryšio priemonės, pvz., objekto el. pašto adresą ar telefono numerį, bet ne raktinius žodžius ar asmenų vardus ir pavardes ([270]).

(146) NSA analitikai pirmiausia nustatys užsienyje esančius ne JAV piliečius, kuriuos stebint, analitikų vertinimu, bus gauta sertifikate nurodytos atitinkamos užsienio žvalgybos informacijos ([271]). Kaip nurodyta NSA asmenų, kurių informaciją norima rinkti, nustatymo procedūrose, NSA gali tiesiogiai stebėti objektą tik kai jau turi tam tikrų žinių apie jį ([272]). Tam gali būti remiamasi įvairių šaltinių, pvz., žmonių žvalgybos, informacija. Iš tokių kitų šaltinių analitikas taip pat turi gauti žinių apie konkretų atrinktuvą (t. y. ryšių paskyrą), naudojamą asmens, kurio informaciją gali būti norima rinkti. Nustačius tokius konkrečius asmenis ir NSA pagal išsamų peržiūros mechanizmą ([273]) patvirtinus jų nustatymą, bus pradedami naudoti (t. y. parengiami ir taikomi) ryšių priemones leidžiantys nustatyti atrinktuvai (pvz., el. pašto adresai) ([274]).

(147) NSA turi dokumentuoti faktinį asmens, kurio informaciją norima rinkti, pasirinkimo pagrindą ([275]) ir reguliariais intervalais po pradinio tokio asmens nustatymo patvirtinti, kad asmenų, kurių informaciją norima rinkti, nustatymo standarto vis dar laikomasi ([276]). Kai asmenų, kurių informaciją norima rinkti, nustatymo standarto nebesilaikoma, duomenų rinkimas turi būti nutrauktas ([277]). Teisingumo departamento žvalgybos priežiūros tarnybų pareigūnai kas du mėnesius peržiūri, ar NSA kiekvieną asmenį, kurio informaciją norima rinkti, atrenka ir kiekvieną užfiksuotą asmenų, kurių informaciją norima rinkti, nustatymo vertinimą ir pagrindimą registruoja laikydamasi asmenų, kurių informaciją norima rinkti, nustatymo procedūrų, ir privalo apie bet kokį pažeidimą pranešti FISC ir Kongresui ([278]). Remiantis NSA rašytiniais dokumentais FISC lengviau prižiūrėti, ar konkretūs asmenys tinkamai nustatomi pagal FISA 702 straipsnį, laikantis 173 ir 174 konstatuojamosiose dalyse aprašytų priežiūros įgaliojimų ([279]). Galiausiai taip pat reikalaujama, kad Nacionalinės žvalgybos direktorius kasmet viešose metinėse statistikos skaidrumo ataskaitose nurodytų bendrą asmenų, kurių informacija renkama pagal FISA 702 straipsnį, skaičių. Nurodymus pagal FISA 702 straipsnį gaunančios bendrovės gali skelbti suvestinius gautų prašymų duomenis (per skaidrumo ataskaitas) ([280]).

([269]) NSA asmenų, kurių informaciją norima rinkti, nustatymo procedūros, p. 4.

([270]) Žr. PCLOB ataskaitą dėl 702 straipsnio, p. 32–33 ir p. 45 su papildomomis nuorodomis. Taip pat žr. generalinio prokuroro ir Nacionalinės žvalgybos direktoriaus pateiktą pagal Užsienio žvalgybos informacijos sekimo akto 702 straipsnį paskelbtų procedūrų ir gairių laikymosi pusmečio vertinimą už laikotarpį nuo 2016 m. gruodžio 1 d. iki 2017 m. gegužės 31 d., p. 41 (2018 m. spalio mėn.), pateikiamą adresu https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([271]) PCLOB ataskaita dėl 702 straipsnio, p. 42–43.

([272]) NSA asmenų, kurių informaciją norima rinkti, nustatymo procedūros, p. 2.

([273]) PCLOB ataskaita dėl 702 straipsnio, p. 46. Pavyzdžiui, NSA privalo patikrinti, ar tarp sekamo asmens, kurio informaciją norima rinkti, ir atrinktuvo yra ryšys, dokumentuoti užsienio žvalgybos informaciją, kurios tikimasi gauti, taip pat šią informaciją turi peržiūrėti ir patvirtinti du vyresnieji NSA analitikai, o visas procesas bus stebimas, kad vėliau ODNI ir Teisingumo departamentas galėtų atlikti atitikties peržiūrą. Žr. NSA CLPO, 2014 m. balandžio 16 d. NSA užsienio žvalgybos akto 702 straipsnio įgyvendinimo ataskaitą.

([274]) JAV kodekso 50 antraštinės dalies 1881a straipsnio h dalis.

([275]) NSA asmenų, kurių informaciją norima rinkti, nustatymo procedūros, p. 8. Taip pat žr. PCLOB ataskaitą dėl 702 straipsnio, p. 46. Tai, kad nepateikiama raštiško pagrindimo, laikoma dokumentacijos reikalavimų nesilaikymo incidentu, apie kurį turi būti pranešta FISC ir Kongresui. Žr. generalinio prokuroro ir Nacionalinės žvalgybos direktoriaus pateiktą pagal Užsienio žvalgybos informacijos sekimo akto 702 straipsnį paskelbtų procedūrų ir gairių laikymosi pusmečio vertinimą už laikotarpį nuo 2016 m. gruodžio 1 d. iki 2017 m. gegužės 31 d., p. 41 (2018 m. spalio mėn.), FISC skirtą Teisingumo ir ODNI reikalavimų laikymosi ataskaitą už laikotarpį nuo 2016 m. gruodžio mėn. iki 2017 m. gegužės mėn., p. A-6, pateikiamą adresu https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([276]) Žr. JAV vyriausybės Užsienio žvalgybos stebėjimo teismui pateiktą medžiagą, 2015 m. svarbių 702 straipsnio reikalavimų santrauką, p. 2–3 (2015 m. liepos 15 d.) ir VII priede pateikiamą informaciją.

([277]) Žr. JAV vyriausybės Užsienio žvalgybos stebėjimo teismui pateiktą medžiagą, 2015 m. svarbių 702 straipsnio reikalavimų santrauką, p. 2–3 (2015 m. liepos 15 d.), kurioje nustatyta, kad „jei vyriausybė vėliau įvertina, kad toliau naudojant asmens, kurio informaciją norima rinkti, atrinktuvą gauti užsienio žvalgybos informacijos nesitikima, užduotį reikia skubiai nutraukti, o delsimas gali būti traktuojamas kaip reikalavimų nesilaikymo incidentas, apie kurį turi būti pranešama“. Taip pat žr. VII priede pateikiamą informaciją.

([278]) PCLOB ataskaita dėl 702 straipsnio, p. 70–72; Jungtinių Amerikos Valstijų žvalgybos stebėjimo teismo darbo tvarkos taisyklių 13 taisyklės b punktas, pateikiamas adresu https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([279]) Taip pat žr. FISC skirtą Teisingumo departamento ir ODNI reikalavimų laikymosi ataskaitą už laikotarpį nuo 2016 m. gruodžio mėn. iki 2017 m. gegužės mėn., p. A-6.

([280]) JAV kodekso 50 antraštinės dalies 1874 straipsnis.

(148) Kitiems JAV organizacijoms perduodamų asmens duomenų rinkimo teisiniams pagrindams taikomi skirtingi apribojimai ir apsaugos priemonės. Apskritai pagal FISA 402 straipsnį (dėl įgaliojimų dėl renkamų numerių registratorių ir gaunamų skambučių sekiklių) ir remiantis NSR masiškai rinkti duomenis konkrečiai draudžiama – vietoj to reikalaujama taikyti konkrečias atrankos sąlygas ([281]).

(149) Kad galėtų vykdyti tradicinį individualizuotą elektroninį stebėjimą (pagal FISA 105 straipsnį), žvalgybos agentūros turi pateikti prašymą FISC, kuriame nurodomi faktai ir aplinkybės, kuriais remiamasi siekiant pagrįsti įsitikinimą, kad yra tikėtina priežastis manyti, jog užsienio valstybė arba užsienio valstybės agentas naudojasi arba ketina naudotis ta priemone ([282]). FISC, be kita ko, įvertins, ar, remiantis pateiktais faktais, yra tikėtina priežastis manyti, kad iš tikrųjų taip yra ([283]).

(150) Norint pagal FISA 301 straipsnį atlikti patalpų ar turto kratą, per kurią numatoma patikrinti, konfiskuoti ar pan. informaciją, medžiagą ar turtą (pvz., kompiuterinį įrenginį), būtina pateikti prašymą, kad FISC išduotų orderį ([284]). Tokiame prašyme, *inter alia*, turi būti įrodyta, jog yra tikėtina priežastis manyti, kad kratos objektas yra užsienio valstybė arba užsienio valstybės agentas, kad patalpoje ar turto vienete, kurių kratą numatoma atlikti, yra užsienio žvalgybos informacijos ir kad patalpa, kurios kratą numatoma atlikti, priklauso užsienio valstybei (ar jos agentui), yra jos (jo) naudojama, valdoma arba jai (jam) ar jos (jo) perduodama ([285]).

(151) Taip pat norint įrengti renkamų numerių registratorius arba gaunamų skambučių sekiklius (pagal FISA 402 straipsnį), reikia pateikti prašymą, kad FISC (arba JAV magistratas) išduotų orderį, ir taikyti konkrečią atrankos sąlygą, t. y. sąlygą, pagal kurią konkrečiai identifikuojamas asmuo, paskyra ir kt. ir kuo labiau, kiek pagrįstai įmanoma, apribojama siekiamos gauti informacijos apimtis ([286]). Šis įgaliojimas nesusijęs su ryšių turiniu, bet labiau taikomas informacijai apie klientą arba abonentą, kuris naudojasi paslauga (pvz., vardas ir pavardė, adresas, abonento numeris, gautos paslaugos trukmė ir (arba) rūšis, mokėjimo šaltinis ir (arba) būdas).

(152) FISA 501 straipsnyje ([287]), pagal kurį leidžiama rinkti viešojo transporto vežėjo (t. y. asmens ar subjekto, už atlygį vežančio žmones ar turtą sausumos, geležinkelių, vandens ar oro transporto priemonėmis), viešosios apgyvendinimo įstaigos (pvz., viešbučio, motelio ar svečių namų), transporto priemonių nuomos įstaigos ar fizinės saugyklos (kurioje suteikiama vietos prekėms ir medžiagoms saugoti arba teikiamos susijusios paslaugos) ([288]) verslo įrašus, taip pat reikalaujama pateikti prašymą FISC arba magistratui. Tokiame prašyme reikia nurodyti norimus gauti įrašus ir konkrečius bei aiškius faktus, dėl kurių yra priežasčių manyti, kad asmuo, su kuriuo susiję įrašai, yra užsienio subjektas arba užsienio valstybės agentas ([289]).

(153) Galiausiai, pagal įvairius įstatymus leidžiama naudoti NSR, o pagal NSR leidžiama tyrimus atliekančioms agentūroms iš tam tikrų subjektų (pvz., finansų įstaigų, kredito informaciją teikiančių agentūrų, elektroninių ryšių teikėjų) gauti tam tikrą informaciją (neįskaitant ryšių turinio), pateikiamą kredito ataskaitose, finansiniuose įrašuose ir elektroniniuose abonentų bei sandorių įrašuose ([290]). NSR įstatymu, pagal kurį leidžiama prieiga prie elektroninių ryšių, gali naudotis tik FTB, taip pat pagal jį reikalaujama, kad prašymuose būtų nurodoma sąlyga, pagal kurią konkrečiai identifikuojamas asmuo, subjektas, telefono numeris arba paskyra, ir patvirtinama, kad informacija yra svarbi įgaliotam nacionalinio saugumo tyrimui, siekiant užtikrinti apsaugą nuo tarptautinio terorizmo arba slaptos žvalgybos veiklos ([291]). NSR gavėjai turi teisę jį ginčyti teisme ([292]).

([281]) JAV kodekso 50 antraštinės dalies 1842 straipsnio c dalies 3 punktas ir, kiek tai susiję su NSR, JAV kodekso 12 antraštinės dalies 3414 straipsnio a dalies 2 punktas, JAV kodekso 15 antraštinės dalies 1681u straipsnis, JAV kodekso 15 antraštinės dalies 1681v straipsnio a dalis ir JAV kodekso 18 antraštinės dalies 2709 straipsnio a dalis.

([282]) Užsienio valstybės agentais gali būti laikomi ne JAV piliečiai, dalyvaujantys tarptautinio terorizmo arba tarptautinio masinio naikinimo ginklų platinimo veikloje (įskaitant parengiamąją veiklą) (JAV 50 antraštinės dalies 1801 straipsnio b dalies 1 punktas).

([283]) JAV kodekso 50 antraštinės dalies 1804 straipsnis. Dėl atrankos sąlygų pasirinkimo taip pat žr. 1841 straipsnio 4 punktą.

([284]) JAV kodekso 50 antraštinės dalies 1821 straipsnio 5 punktas.

([285]) JAV kodekso 50 antraštinės dalies 1823 straipsnio a dalis.

([286]) JAV kodekso 50 antraštinės dalies 1842 straipsnis su 1841 straipsnio 2 punktu ir 18 antraštinės dalies 3127 straipsnis.

([287]) JAV kodekso 50 antraštinės dalies 1862 straipsnis.

([288]) JAV kodekso 50 antraštinės dalies 1861–1862 straipsniai.

([289]) JAV kodekso 50 antraštinės dalies 1862 straipsnio b dalis.

([290]) JAV kodekso 12 antraštinės dalies 3414 straipsnis, JAV kodekso 15 antraštinės dalies 1681u–1681v straipsniai ir JAV kodekso 18 antraštinės dalies 2709 straipsnis.

([291]) JAV kodekso 18 antraštinės dalies 2709 straipsnio b dalis.

([292]) Pvz., JAV kodekso 18 antraštinės dalies 2709 straipsnio d dalis.

3.2.1.3. *Tolesnis surinktos informacijos naudojimas*

(154) Tvarkant JAV žvalgybos agentūrų signalų žvalgybos būdu surinktus asmens duomenis taikomos įvairios apsaugos priemonės.

(155) Pirma, kiekviena žvalgybos agentūra privalo užtikrinti pakankamą duomenų saugumą ir neleisti leidimo neturintiems asmenims susipažinti su signalų žvalgybos būdu surinktais asmens duomenimis. Šiuo atžvilgiu įvairiose priemonėse, įskaitant įstatymus, gaires ir standartus, išsamiau apibrėžiami nustatytini minimalūs informacijos saugumo reikalavimai (pvz., daugiaveiksnis tapatumo nustatymas, šifravimas ir kt.) ([293]). Galimybė susipažinti su surinktais duomenimis turi būti suteikiama tik įgaliotiems, mokymus baigusiems darbuotojams, kuriems reikia žinoti informaciją, kad galėtų vykdyti savo užduotis ([294]). Apskritai žvalgybos agentūros turi rengti tinkamus mokymus savo darbuotojams, be kita ko, apie pranešimo apie įstatymų (įskaitant VP 14086) pažeidimus ir tų pažeidimų nagrinėjimo procedūras ([295]).

(156) Antra, žvalgybos agentūros privalo laikytis žvalgybos bendruomenės tikslumo ir objektyvumo standartų, visų pirma susijusių su duomenų kokybės ir patikimumo užtikrinimu, alternatyvių informacijos šaltinių apsvarstymu ir objektyvumu atliekant analizę ([296]).

(157) Trečia, dėl duomenų saugojimo VP 14086 aiškiai nurodoma, kad ne JAV piliečių asmens duomenims taikomi tokie pat saugojimo laikotarpiai kaip ir JAV piliečių duomenims, ([297]). Žvalgybos agentūros privalo nustatyti konkrečius saugojimo laikotarpius ir (arba) veiksnius, į kuriuos reikia atsižvelgti nustatant taikomų saugojimo laikotarpių trukmę (pvz., ar informacija yra nusikaltimo įrodymas; ar informacija yra užsienio žvalgybos informacija; ar informacija reikalinga siekiant apsaugoti asmenų ar organizacijų, įskaitant tarptautinio terorizmo aukas ar taikinius, saugumą), kurie nustatyti įvairiose teisinėse priemonėse ([298]).

(158) Ketvirta, signalų žvalgybos būdu surinktų asmens duomenų platinimui taikomos specialios taisyklės. Paprastai ne JAV piliečių asmens duomenys gali būti platinami tik jei jie apima tos pačios rūšies informaciją, kuri gali būti platinama apie JAV piliečius, pvz., informaciją, reikalingą asmens ar organizacijos (pvz., tarptautinių teroristinių organizacijų taikinių, aukų ar įkaitų) saugumui užtikrinti ([299]). Be to, asmens duomenys negali būti platinami vien dėl asmens pilietybės ar gyvenamosios valstybės arba siekiant apeiti VP 14086 reikalavimus ([300]). JAV valdžios

([293]) VP 14086 2 straipsnio c dalies iii punkto B papunkčio 1 dalis. Taip pat žr. Nacionalinio saugumo akto VIII antraštinę dalį (kurioje pateikiami išsamūs reikalavimai dėl teisės susipažinti su įslaptinta informacija), VP 12333 1.5 skirsnį (kuriame reikalaujama, kad žvalgybos bendruomenės agentūrų vadovai laikytųsi dalijimosi informacija ir saugumo gairių, informacijos privatumo ir kitų teisinių reikalavimų), Nacionalinio saugumo direktyvą Nr. 42 dėl nacionalinio saugumo telekomunikacijų ir informacinių sistemų saugumo nacionalinės politikos (pagal kurią Nacionalinių saugumo sistemų komitetui pavedama vykdomiesiems departamentams ir agentūroms teikti nacionalinių saugumo sistemų saugumo gaires), ir Nacionalinio saugumo memorandumą Nr. 8 dėl Nacionalinio saugumo, Gynybos departamento ir žvalgybos bendruomenės sistemų kibernetinio saugumo didinimo (kuriame nustatomi terminai ir gairės, kaip bus įgyvendinami nacionalinių saugumo sistemų kibernetinio saugumo reikalavimai, įskaitant daugiaveiksnį tapatumo nustatymą, šifravimą, debesijos technologijas ir grėsmės galiniuose įrenginiuose aptikimo paslaugas).

([294]) VP 14086 2 straipsnio c dalies iii punkto B papunkčio 2 dalis. Be to, su asmens duomenimis, dėl kurių saugojimo nebuvo priimtas galutinis sprendimas, galima susipažinti tik siekiant priimti ar pagrįsti tokį sprendimą arba atlikti leidžiamas administracines, bandymų, kūrimo, saugumo ar priežiūros funkcijas (VP 14086 2 straipsnio c dalies iii punkto B papunkčio 3 dalis).

([295]) VP 14086 2 straipsnio d dalies ii punktas.

([296]) VP 14086 2 straipsnio c dalies iii punkto C papunktis.

([297]) VP 14086 2 straipsnio c dalies iii punkto A papunkčio 2 dalies a–c punktai. Apskritai kiekviena agentūra turi nustatyti politiką ir procedūras, kad kuo mažiau platintų ir saugotų signalų žvalgybos būdu surinktų asmens duomenų (VP 14086 2 straipsnio c dalies iii punkto A papunktis).

([298]) Žr., pvz., 2015 finansinių metų Žvalgybos įgaliojimų akto 309 straipsnį; atskirų žvalgybos agentūrų pagal FISA 702 straipsnį priimtas ir FISC patvirtintas duomenų kiekio mažinimo procedūras; generalinio prokuroro ir FRA patvirtintas procedūras (pagal kurį reikalaujama, kad JAV federalinės agentūros, įskaitant nacionalines saugumo agentūras, nustatytų savo įrašų saugojimo laikotarpius, o juos turi patvirtinti Nacionalinė archyvų ir įrašų administracija).

([299]) VP 14086 2 straipsnio c dalies iii punkto A papunkčio 1 dalies a punktas ir 5 dalies d punktas kartu su VP 12333 2.3 skirsniu.

([300]) VP 14086 2 straipsnio c dalies iii punkto A papunkčio 1 dalies b ir e punktai.

sektoriuje informacija gali būti platinama tik jei įgaliotas ir mokymus baigęs asmuo pagrįstai mano, kad gavėjui reikia žinoti tą informaciją ([301]) ir jis ją tinkamai apsaugos ([302]). Siekiant nustatyti, ar asmens duomenys gali būti platinami JAV valdžios sektoriui nepriklausantiems gavėjams (įskaitant užsienio vyriausybę ar tarptautinę organizaciją), būtina atsižvelgti į platinimo tikslą, platinamų duomenų pobūdį ir apimtį, taip pat į žalingo poveikio atitinkamam (-iems) asmeniui (-ims) galimybę ([303]).

(159) Galiausiai, be kita ko, siekiant palengvinti taikomų teisinių reikalavimų laikymosi priežiūrą ir veiksmingą teisių gynimą, pagal VP 14086 kiekviena žvalgybos agentūra privalo saugoti atitinkamus dokumentus apie signalų žvalgybos duomenų rinkimą. Dokumentacijos reikalavimai apima tokius elementus kaip faktinis pagrindas, kuriuo remiantis vertinama, ar konkreti duomenų rinkimo veikla yra būtina siekiant įgyvendinti patvirtintą žvalgybos prioritetą ([304]).

(160) Be pirmiau minėtų VP 14086 numatytų apsaugos priemonių, taikomų naudojant informaciją, surinktą vykdant signalų žvalgybą, visoms JAV žvalgybos agentūroms taikomi bendresnio pobūdžio reikalavimai dėl tikslo apribojimo, duomenų kiekio mažinimo, tikslumo, saugumo, saugojimo ir platinimo, visų pirma pagal VBT aplinkraštį Nr. A-130, E. valdžios aktą, Federalinių registrų aktą (žr. 101–106 konstatuojamąsias dalis) ir Nacionalinių saugumo sistemų komiteto (CNSS) gaires ([305]).

3.2.2. ***Priežiūra***

(161) JAV žvalgybos agentūrų veiklą prižiūri įvairios įstaigos.

(162) Pirma, VP 14086 reikalaujama, kad kiekviena žvalgybos agentūra turėtų vyresniuosius teisės, priežiūros ir atitikties užtikrinimo pareigūnus, kurie užtikrintų, kad būtų laikomasi taikomų JAV teisės aktų ([306]). Visų pirma jie turi vykdyti periodinę signalų žvalgybos veiklos priežiūrą ir užtikrinti, kad bet koks reikalavimų nesilaikymas būtų ištaisytas. Žvalgybos agentūros privalo tokiems pareigūnams sudaryti sąlygas susipažinti su visa aktualia informacija, kad jie galėtų vykdyti priežiūros funkcijas, ir negali imtis veiksmų, kurie jiems trukdytų vykdyti priežiūros veiklą arba tokiai veiklai darytų nederamą įtaką ([307]). Be to, apie visus už priežiūrą atsakingo pareigūno ar bet kurio kito darbuotojo nustatytus reikšmingus reikalavimų nesilaikymo incidentus ([308]) turi būti nedelsiant pranešama žvalgybos agentūros vadovui ir Nacionalinės žvalgybos direktoriui, o šie turi užtikrinti, kad būtų imtasi visų būtinų veiksmų siekiant ištaisyti padėtį ir neleisti, kad reikšmingas reikalavimų nesilaikymo incidentas pasikartotų ([309]).

(163) Šią priežiūros funkciją vykdo pareigūnai, kuriems pavesta rūpintis, kad būtų laikomasi reikalavimų, taip pat privatumo ir piliečių laisvių apsaugos pareigūnai ir generaliniai inspektoriai ([310]).

([301]) Pvz., AGG-DOM numatoma, kad FTB gali platinti informaciją, jeigu gavėjui reikia ją žinoti, kad jis galėtų įvykdyti savo užduotį arba apsaugoti visuomenę.

([302]) VP 14086 2 straipsnio c dalies iii punkto A papunkčio 1 dalies c punktas. Žvalgybos agentūros gali, pavyzdžiui, platinti informaciją aplinkybėmis, susijusiomis su nusikalstamų veikų tyrimu arba su nusikaltimu, be kita ko, pavyzdžiui, platinti įspėjimus apie grasinimus nužudyti, sunkiai fiziškai sužaloti ar pagrobti asmenis; platinti informaciją apie kibernetines grėsmes, incidentus ar reagavimo į įsibrovimą priemones ir informuoti aukas arba įspėti asmenis, kurie gali tapti nusikaltimų aukomis.

([303]) VP 14086 2 straipsnio c dalies iii punkto A papunkčio 1 dalies d punktas.

([304]) VP 14086 2 straipsnio c dalies iii punkto E papunktis.

([305]) Žr. CNSS politiką Nr. 22 „Kibernetinio saugumo rizikos valdymo politika“ ir CNSS instrukciją Nr. 1253, kurioje pateikiamos išsamios gairės dėl nacionalinių saugumo sistemų saugumo priemonių.

([306]) VP 14086 2 straipsnio d dalies i punkto A–B papunkčiai.

([307]) VP 14086 2 straipsnio d dalies i punkto B–C papunkčiai.

([308]) T. y. sisteminis arba tyčinis taikomų JAV teisės aktų nesilaikymas, dėl kurio gali būti suabejota žvalgybos bendruomenės subjekto reputacija ar sąžiningumu arba kitaip kvestionuojamas žvalgybos bendruomenės veiklos deramumas, be kita ko, atsižvelgiant į bet kokį reikšmingą poveikį atitinkamo (-ių) asmens (-ų) su privatumu ir piliečių laisvėmis susijusiems interesams; žr. VP 14086 5 straipsnio l dalį.

([309]) VP 14086 2 straipsnio d dalies iii punktas.

([310]) VP 14086 2 straipsnio d dalies i punkto B papunktis.

(164) Kaip ir baudžiamosios teisėsaugos institucijose, privatumo ir piliečių laisvių apsaugos pareigūnai veikia ir visose žvalgybos agentūrose ([311]). Šių pareigūnų įgaliojimai paprastai apima procedūrų priežiūrą siekiant užtikrinti, kad atitinkamas departamentas ar agentūra tinkamai atsižvelgtų į privatumo ir piliečių laisvių aspektus ir nustatytų tinkamas procedūras, kaip turi būti nagrinėjami asmenų, manančių, kad jų privatumas arba piliečių laisvės buvo pažeisti, skundai (o kai kuriais atvejais, panašiai kaip ir ODNI, jie gali turėti įgaliojimus skundus tirti patys ([312])). Žvalgybos agentūrų vadovai turi užtikrinti, kad privatumo ir piliečių laisvių apsaugos pareigūnai turėtų išteklių savo įgaliojimams vykdyti, galėtų naudotis visa medžiaga ir darbuotojų paslaugomis, reikalingais jų funkcijoms vykdyti, ir būtų informuojami apie siūlomus politikos pakeitimus ir dėl tokių pakeitimų su jais būtų konsultuojamasi ([313]). Privatumo ir piliečių laisvių apsaugos pareigūnai periodiškai teikia ataskaitas Kongresui ir PCLOB, be kita ko, nurodydami departamento ar agentūros gautų skundų skaičių ir pobūdį, taip pat tokių skundų nagrinėjimo, atliktų peržiūrų bei tyrimų ir pareigūno vykdytos veiklos poveikio santrauką ([314]).

(165) Antra, kiekviena žvalgybos agentūra turi nepriklausomą generalinį inspektorių, be kita ko, atsakingą už užsienio žvalgybos veiklos priežiūrą. Taigi ODNI struktūroje veikia žvalgybos bendruomenės Generalinio inspektoriaus tarnyba, turinti plačią jurisdikciją visai žvalgybos bendruomenei ir įgaliojimus tirti skundus ar informaciją, susijusius su įtariamu neteisėtu elgesiu ar piktnaudžiavimu įgaliojimais, kiek tai susiję su ODNI ir (arba) žvalgybos bendruomenės programomis ir veikla ([315]). Kaip ir baudžiamosios teisėsaugos institucijose (žr. 109 konstatuojamąją dalį), tokie generaliniai inspektoriai yra teisiškai nepriklausomi ([316]) ir atsakingi už auditą ir tyrimus, susijusius su nacionalinės žvalgybos tikslais atitinkamos agentūros vykdomomis programomis ir operacijomis, be kita ko, dėl piktnaudžiavimo teise ar teisės pažeidimo ([317]). Jie turi galimybę susipažinti su visais įrašais, ataskaitomis, audito

([311]) Žr. JAV kodekso 42 antraštinės dalies 2000ee-1 straipsnį. Tai yra, pvz., Valstybės departamentas, Teisingumo departamentas, Vidaus saugumo departamentas, Gynybos departamentas, NSA, CŽA, FTB ir ODNI.

([312]) Žr. VP 14086 3 straipsnio c dalį.

([313]) JAV kodekso 42 antraštinės dalies 2000ee-1 straipsnio d dalis.

([314]) Pavyzdžiui, iš NSA Piliečių laisvių, privatumo ir skaidrumo tarnybos 2021 m. sausio mėn.–2021 m. birželio mėn. ataskaitos matyti, kad ji atliko 591 peržiūrą dėl poveikio piliečių laisvėms ir privatumui įvairiomis aplinkybėmis, pvz., susijusiomis su duomenų rinkimo veikla, dalijimosi informacija tvarka ir sprendimais, sprendimais dėl duomenų saugojimo ir kt., atsižvelgdama į įvairius veiksnius, pvz., su veikla susijusios informacijos kiekį ir rūšį, susijusius asmenis, duomenų paskirtį ir numatomą naudojimą, taikomas apsaugos priemones galimai rizikai privatumui mažinti ir kt. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Taip pat CŽA Privatumo ir piliečių laisvių apsaugos tarnybos 2019 m. sausio–birželio mėn. ataskaitose pateikiama informacijos apie tarnybos vykdytą priežiūros veiklą, pvz., peržiūrą, kaip laikomasi generalinio prokuroro gairių pagal VP 12333 informacijos saugojimo ir platinimo srityse, PPD 28 įgyvendinimo gairių ir reikalavimų nustatyti ir šalinti duomenų saugumo pažeidimus, taip pat asmeninės informacijos naudojimo ir tvarkymo peržiūrą (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf).

([315]) Šį generalinį inspektorių skiria Prezidentas Senatui patvirtinus ir gali atleisti tik Prezidentas.

([316]) Generalinių inspektorių postas yra užtikrintas ir juos gali atleisti tik Prezidentas, kuris privalo Kongresui raštu nurodyti tokio atleidimo priežastis. Tai nebūtinai reiškia, kad jie gali visiškai nepaisyti nurodymų. Tam tikrais atvejais departamento vadovas gali drausti generaliniam inspektoriui pradėti, vykdyti arba užbaigti auditą ar tyrimą, jeigu manoma, kad tai būtina siekiant apsaugoti svarbius nacionalinius (saugumo) interesus. Tačiau pasinaudojus šiuo įgaliojimu būtina informuoti Kongresą ir tuo remiantis atitinkamas direktorius gali būti laikomas atsakingu. Žr., pvz., 1978 m. Generalinių inspektorių akto 8 straipsnį (dėl Gynybos departamento), 8E straipsnį (dėl Teisingumo departamento), 8G straipsnio d dalies 2 punkto A ir B papunkčius (dėl NSA), JAV kodekso 50 antraštinės dalies 403q straipsnio b dalį (dėl CŽA); 2010 finansinių metų Žvalgybos įgaliojimų akto 405 straipsnio f dalį (dėl žvalgybos bendruomenės).

([317]) 1978 m. Generalinių inspektorių aktas su pakeitimais, Oficialusis leidinys Nr. L. 117/108, 2022 m. balandžio 8 d. Pavyzdžiui, kaip paaiškinta jo pusmečio ataskaitose Kongresui, apimančiose laikotarpį nuo 2021 m. balandžio 1 d. iki 2022 m. kovo 31 d., NSA generalinis inspektorius įvertino pagal VP 12333 surinktos JAV piliečių informacijos tvarkymą, signalų žvalgybos duomenų ištrynimo procesą, NSA naudojamą automatinę asmenų, kurių informaciją norima rinkti, nustatymo priemonę, taip pat dokumentų ir užklausų teikimo taisyklių laikymąsi pagal FISA 702 straipsnį ir pateikė keletą susijusių rekomendacijų (žr. https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, p. 5–8 ir https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907, p. 10–13). Taip pat žr. žvalgybos bendruomenės generalinio inspektoriaus neseniai atliktus auditus ir tyrimus dėl informacijos saugumo ir neleidžiamo įslaptintos nacionalinio saugumo informacijos atskleidimo (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf), p. 8, 11 ir https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, p. 19–20.

medžiaga, peržiūrų medžiaga, dokumentais, užrašais, rekomendacijomis ar kita susijusia medžiaga, prireikus remdamiesi potvarkiu, be to, gali priimti parodymus ([318]). Generaliniai inspektoriai įtariamų baudžiamųjų pažeidimų atvejus perduoda baudžiamajam persekiojimui ir agentūrų vadovams teikia rekomendacijas dėl taisomųjų veiksmų ([319]). Nors jų rekomendacijos neprivalomos, jų ataskaitos, be kita ko, dėl tolesnių veiksmų (arba neveikimo) ([320]), paprastai skelbiamos viešai ir siunčiamos Kongresui, o šis tuo pagrindu gali vykdyti savo priežiūros funkciją (žr. 168 ir 169 konstatuojamąsias dalis) ([321]).

(166) Trečia, Prezidento žvalgybos patariamojoje taryboje (PIAB) įsteigta Žvalgybos priežiūros valdyba (IOB) prižiūri, kaip JAV žvalgybos institucijos laikosi Konstitucijos ir visų taikomų taisyklių ([322]). PIAB yra Prezidento vykdomosios tarnybos patariamasis organas, kurį sudaro 16 narių, Prezidento skiriamų ne iš JAV vyriausybės. IOB sudaro daugiausia penki nariai, Prezidento skiriami iš PIAB narių. Pagal VP 12333 ([323]) visų žvalgybos agentūrų vadovai privalo pranešti IOB apie bet kokią žvalgybos veiklą, jei yra priežasčių manyti, kad ji gali būti neteisėta arba prieštarauti vykdomajam potvarkiui ar Prezidento direktyvai. Siekiant užtikrinti, kad IOB galėtų susipažinti su informacija, kurios reikia jos funkcijoms vykdyti, VP 13462 nurodoma Nacionalinės žvalgybos direktoriui ir žvalgybos agentūrų vadovams teikti visą informaciją ir pagalbą, kurios, IOB nuomone, reikia jos funkcijoms vykdyti, kiek tai leidžiama pagal įstatymus ([324]). IOB savo ruožtu privalo informuoti Prezidentą apie žvalgybos veiklą, kuria, jos nuomone, gali būti pažeidžiama JAV teisė (įskaitant vykdomuosius potvarkius), o generalinis prokuroras, Nacionalinės žvalgybos direktorius ar žvalgybos agentūros vadovas į tai deramai neatsižvelgia ([325]). Be to, apie galimus baudžiamosios teisės pažeidimus IOB privalo informuoti generalinį prokurorą.

(167) Ketvirta, žvalgybos agentūras prižiūri PCLOB. Pagal PCLOB steigimo sutartį jai patikėta atsakomybė kovos su terorizmu politikos ir jos įgyvendinimo srityje, siekiant apsaugoti privatumą ir piliečių laisves. Peržiūrėdama žvalgybos agentūrų veiksmus, ji gali susipažinti su visais aktualiais agentūros įrašais, ataskaitomis, audito medžiaga, peržiūrų medžiaga, dokumentais, užrašais ir rekomendacijomis, įskaitant įslaptintą informaciją, rengti pokalbius ir išklausyti parodymus ([326]). Ji gauna ataskaitas iš kelių federalinių departamentų ar agentūrų piliečių laisvių ir privatumo apsaugos pareigūnų ([327]), gali teikti rekomendacijas vyriausybei ir žvalgybos agentūroms ir reguliariai teikia ataskaitas Kongreso komitetams ir Prezidentui ([328]). Valdybos ataskaitos, įskaitant ataskaitas Kongresui, turi būti kuo plačiau skelbiamos viešai ([329]). PCLOB paskelbė keletą priežiūros ir tolesnių veiksmų ataskaitų, įskaitant pagal FISA 702 straipsnį vykdomų programų ir privatumo apsaugos tomis aplinkybėmis analizės, taip pat PPD 28 ir VP 12333 įgyvendinimo ataskaitas ([330]). PCLOB taip pat įpareigota vykdyti konkrečias priežiūros

([318]) Žr. 1978 m. Generalinių inspektorių akto 6 straipsnį.

([319]) Žr. ten pat, 4 straipsnį ir 6 straipsnio 5 dalį.

([320]) Dėl tolesnių veiksmų, susijusių su generalinių inspektorių ataskaitomis ir rekomendacijomis, žr., pvz., atsakymą į Teisingumo departamento generalinio inspektoriaus ataskaitą, kurioje nustatyta, kad FTB 2014–2019 m. teikdamas prašymus FISC elgėsi nepakankamai skaidriai, todėl buvo imtasi reformų, kuriomis FTB siekiama pagerinti reikalavimų laikymąsi, priežiūrą ir atskaitomybę (pvz., FTB direktorius nurodė imtis daugiau nei 40 taisomųjų veiksmų, įskaitant 12 konkrečiai FISA procesui skirtų taisomųjų veiksmų, susijusių su dokumentavimu, priežiūra, bylų tvarkymu, mokymu ir auditu) (žr. https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance ir https://oig.justice.gov/reports/2019/o20012.pdf). Taip pat žr., pvz., Teisingumo departamento generalinio inspektoriaus atliktą auditą dėl FTB generalinio patarėjo tarnybos vaidmens ir atsakomybės prižiūrint, kaip laikomasi taikomų teisės aktų, politikos ir procedūrų, susijusių su FTB nacionalinio saugumo veikla, ir 2 priedėlio, į kurį įtrauktas FTB raštas, kuriame pritariama visoms rekomendacijoms. Šiuo atžvilgiu 3 priedėlyje apžvelgiami tolesni veiksmai ir pateikiama informacija, kurią generalinis inspektorius reikalavo pateikti FTB, kad galėtų užbaigti savo rekomendacijų įgyvendinimą (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

([321]) Žr. 1978 m. Generalinių inspektorių akto 4 straipsnio 5 dalį ir 5 straipsnį.

([322]) Žr. VP 13462.

([323]) Žr. VP 12333 1.6 straipsnio c dalį.

([324]) VP 13462 8 straipsnio a dalis.

([325]) VP 13462 6 straipsnio b dalis.

([326]) JAV kodekso 42 antraštinės dalies 2000ee straipsnio g dalis.

([327]) Žr. JAV kodekso 42 antraštinės dalies 2000ee-1 straipsnio f dalies 1 punkto A papunkčio iii dalį. Be kita ko, bent iš Teisingumo departamento, Gynybos departamento, Vidaus saugumo departamento, Nacionalinės žvalgybos direktoriaus ir Centrinės žvalgybos agentūros, taip pat bet kurio kito departamento, agentūros arba vykdomosios valdžios subjekto, kurį PCLOB paskyrė kaip tinkamą veikti tam tikroje srityje.

([328]) JAV kodekso 42 antraštinės dalies 2000ee straipsnio e dalis.

([329]) JAV kodekso 42 antraštinės dalies 2000ee straipsnio f dalis.

([330]) Pateikiama adresu https://www.pclob.gov/Oversight.

funkcijas, susijusias su VP 14086 įgyvendinimu, visų pirma peržiūrėti, ar agentūros procedūros atitinka vykdomąjį potvarkį (žr. 126 konstatuojamąją dalį), ir įvertinti, ar tinkamai veikia teisių gynimo mechanizmas (žr. 194 konstatuojamąją dalį).

(168) Penkta, be vykdomosios valdžios priežiūros mechanizmų, už visos JAV užsienio žvalgybos veiklos priežiūrą taip pat atsakingi konkretūs JAV Kongreso komitetai (Atstovų Rūmų ir Senato žvalgybos ir teismų komitetai). Šių komitetų nariai gali susipažinti su įslaptinta informacija, taip pat su žvalgybos metodais ir programomis ([331]). Komitetai vykdo priežiūros funkcijas įvairiais būdais, visų pirma rengdami posėdžius, vykdydami tyrimus, peržiūras ir teikdami ataskaitas ([332]).

(169) Kongreso komitetai be kita ko, iš generalinio prokuroro, Nacionalinės žvalgybos direktoriaus, žvalgybos agentūrų ir kitų priežiūros įstaigų (pvz., generalinių inspektorių) reguliariai gauna ataskaitas dėl žvalgybos veiklos (žr. 164 ir165 konstatuojamąsias dalis). Visų pirma, pagal Nacionalinio saugumo aktą „Prezidentas užtikrina, kad Kongreso žvalgybos komitetai būtų išsamiai ir laiku informuojami apie Jungtinių Amerikos Valstijų žvalgybos veiklą, įskaitant visus numatomus reikšmingus žvalgybos veiksmus, kaip reikalaujama pagal šį straipsnio punktą“ ([333]). Be to, „Prezidentas užtikrina, kad Kongreso žvalgybos komitetams nedelsiant būtų pranešama apie bet kokią neteisėtą žvalgybos veiklą, taip pat apie visus taisomuosius veiksmus, kurių buvo imtasi arba kurių planuojama imtis dėl tokios neteisėtos veiklos“ ([334]).

(170) Be to, papildomų ataskaitų teikimo reikalavimų kyla iš konkrečių įstatymų. Visų pirma, FISA reikalaujama, kad generalinis prokuroras „išsamiai informuotų“ Senato ir Atstovų Rūmų žvalgybos ir teismų komitetus apie vyriausybės veiklą pagal tam tikrus FISA straipsnius ([335]). Jame taip pat reikalaujama, kad vyriausybė pateiktų Kongreso komitetams visų FISC arba FISCR sprendimų, nutarčių ar nuomonių, kuriose pateikiamas FISA nuostatų „reikšmingas vertinimas ar aiškinimas“, kopijas. Stebėjimo pagal FISA 702 straipsnį parlamentinė priežiūra vykdoma žvalgybos ir teismų komitetams teikiant pagal įstatymą reikalaujamas ataskaitas, taip pat reguliariai rengiant informacinius susirinkimus ir posėdžius. Tai apima generalinio prokuroro pusmečio ataskaitas, kuriose aprašomas FISA 702 straipsnio taikymas ir prie kurių pridedami patvirtinamieji dokumentai, be kita ko, Teisingumo departamento ir ODNI reikalavimų laikymosi ataskaitos ir bet kokių reikalavimų nesilaikymo incidentų aprašymas ([336]), taip pat atskiras generalinio prokuroro ir Nacionalinės žvalgybos direktoriaus atliekamas pusmečio vertinimas, kuriame dokumentuojama, kaip laikomasi asmenų, kurių informaciją norima rinkti, nustatymo ir duomenų kiekio mažinimo procedūrų ([337]).

([331]) JAV kodekso 50 antraštinės dalies 3091 straipsnis.

([332]) Pavyzdžiui, komitetai rengia teminius posėdžius (žr., pvz., neseniai surengtą Atstovų Rūmų teismų komiteto posėdį dėl nusikaltėlių skaitmeninių paieškos sistemų (https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983) ir Atstovų Rūmų žvalgybos komiteto posėdį dėl dirbtinio intelekto naudojimo žvalgybos bendruomenėje (https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263), taip pat, pvz., FTB ir Teisingumo departamento nacionalinio saugumo skyriaus reguliariai rengiamus priežiūros posėdžius (žr. https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation, https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 ir https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899). Kaip tyrimo pavyzdį žr. Senato žvalgybos komiteto tyrimą dėl Rusijos kišimosi į 2016 m. JAV rinkimus (žr. https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures). Dėl ataskaitų teikimo žr., pvz., Senato žvalgybos komiteto ataskaitoje už laikotarpį nuo 2019 m. sausio 4 d. iki 2021 m. sausio 3 d. Senatui pateiktą Komiteto (priežiūros) veiklos apžvalgą, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4.

([333]) Žr. JAV kodekso 50 antraštinės dalies 3091 straipsnio a dalies 1 punktą. Šioje nuostatoje įtvirtinti bendrieji reikalavimai, susiję su Kongreso vykdoma priežiūra nacionalinio saugumo srityje.

([334]) Žr. JAV kodekso 50 antraštinės dalies 3091 straipsnio b dalį.

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

([336]) Žr. JAV kodekso 50 antraštinės dalies 1881f straipsnį.

([337]) Žr. JAV kodekso 50 antraštinės dalies 1881a straipsnio l dalies 1 punktą.

(171) Be to, pagal FISA reikalaujama, kad JAV vyriausybė kasmet Kongresui (ir visuomenei) nurodytų pagal FISA prašomų ir išduotų nutarčių skaičių, taip pat, be kita ko, JAV ir ne JAV piliečių, kurių informaciją norima rinkti, apytikslį skaičių ([338]). Akte taip pat reikalaujama papildomai viešai nurodyti išduotų NSR skaičių – taip pat tiek dėl JAV, tiek dėl ne JAV piliečių (kartu leidžiama FISA nutarčių ir sertifikatų, taip pat prašymų dėl NSR gavėjams tam tikromis sąlygomis paskelbti skaidrumo ataskaitas) ([339]).

(172) Apskritai JAV žvalgybos bendruomenė deda įvairias pastangas, kad užtikrintų savo (užsienio) žvalgybos veiklos skaidrumą. Pavyzdžiui, 2015 m. ODNI priėmė Žvalgybos skaidrumo principus ir Skaidrumo įgyvendinimo planą ir nurodė kiekvienai žvalgybos agentūrai paskirti žvalgybos skaidrumo užtikrinimo pareigūną, kuris skatintų skaidrumą ir vadovautų skaidrumo užtikrinimo iniciatyvoms ([340]). Dėdama šias pastangas, žvalgybos bendruomenė viešai paskelbė ir toliau skelbia išslaptintas politikos, procedūrų, priežiūros ataskaitų, pagal FISA 702 straipsnį ir VP 12333 teikiamų veiklos ataskaitų, FISC sprendimų ir kitos medžiagos dalis, be kita ko, specialiame ODNI tvarkomame tinklalapyje „IC on the Record“ ([341]).

(173) Galiausiai asmens duomenų rinkimą pagal FISA 702 straipsnį prižiūri ne tik 162–168 konstatuojamosiose dalyse nurodytos priežiūros įstaigos, bet ir FISC ([342]). Pagal FISC darbo tvarkos taisyklių 13 taisyklę už reikalavimų laikymąsi atsakingi JAV žvalgybos agentūrų pareigūnai privalo apie visus su asmenų, kurių informaciją norima rinkti, nustatymo, duomenų kiekio mažinimo ir užklausų teikimo procedūromis susijusius FISA 702 straipsnio pažeidimus pranešti Teisingumo departamentui ir ODNI, o šie apie tai praneša FISC. Be to, Teisingumo departamentas ir ODNI kas pusmetį FISC teikia bendras priežiūros vertinimo ataskaitas, kuriose nurodomos asmenų, kurių informaciją norima rinkti, nustatymo atitikties tendencijos; pateikiama statistinių duomenų; apibūdinamos su reikalavimų laikymusi susijusių incidentų kategorijos; išsamiai apibūdinamos priežastys, dėl kurių įvyko tam tikri su reikalavimų laikymusi susiję incidentai, ir nurodomos priemonės, kurių ėmėsi žvalgybos agentūros, kad tokie atvejai nesikartotų ([343]).

(174) Prireikus (pvz., nustačius asmenų, kurių informaciją norima rinkti, nustatymo procedūrų pažeidimų) Teismas gali nurodyti atitinkamai žvalgybos agentūrai imtis taisomųjų veiksmų ([344]). Atitinkamos teisių gynimo priemonės gali būti įvairios – nuo individualių iki struktūrinių priemonių, pvz., nuo duomenų gavimo nutraukimo ir neteisėtai gautų duomenų ištrynimo iki duomenų rinkimo praktikos pakeitimo, įskaitant gaires ir darbuotojų mokymus ([345]). Be to, atlikdamas metinę pagal 702 straipsnį išduodamų sertifikatų peržiūrą FISC apsvarsto reikalavimų nesilaikymo

([338]) JAV kodekso 50 antraštinės dalies 1873 straipsnio b dalis. Be to, pagal 402 straipsnį „Nacionalinės žvalgybos direktorius, pasikonsultavęs su generaliniu prokuroru, atlieka kiekvieno Užsienio žvalgybos stebėjimo teismo arba Užsienio žvalgybos stebėjimo apeliacinio teismo priimto sprendimo, nutarties arba nuomonės, kurioje pateikiamas reikšmingas bet kurios teisės nuostatos vertinimas ar aiškinimas, įskaitant bet kokį naują ar reikšmingą sąvokos „konkreti atrankos sąlyga“ vertinimą arba aiškinimą, išslaptinimo galimybių peržiūrą (kaip apibrėžta 601 straipsnio e dalyje) ir, atsižvelgdamas į tos peržiūros rezultatus, kiekvieną tokį sprendimą, nutartį ar nuomonę kuo išsamiau paskelbia viešai“.

([339]) JAV kodekso 50 antraštinės dalies 1873 straipsnio b dalies 7 punktas ir 1874 straipsnis.

([340]) https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic.

([341]) Žr. „IC on the Record“ adresu https://icontherecord.tumblr.com/.

([342]) Anksčiau FISC padarė išvadą, kad „Teismui akivaizdu, kad įgyvendinančiosios agentūros, taip pat [ODNI] ir [Teisingumo departamento Nacionalinio saugumo skyrius] skiria daug išteklių savo reikalavimų laikymosi užtikrinimo ir priežiūros pareigoms pagal 702 straipsnį vykdyti. Dažniausiai reikalavimų nesilaikymo atvejai nustatomi nedelsiant ir imamasi tinkamų taisomųjų veiksmų, be kita ko, ištrinama informacija, kuri buvo gauta netinkamai arba kurią pagal taikomas procedūras reikalaujama sunaikinti“. FISA teismas, memorandumo nuomonė ir įsakymas [antraštė redaguota] (2014 m.), skelbiami adresu https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

([343]) Žr., pvz., FISC skirtą Teisingumo departamento ir ODNI FISA 702 straipsnio laikymosi ataskaitą už 2018 m. birželio mėn. – 2018 m. lapkričio mėn., p. 21–65.

([344]) JAV kodekso 50 antraštinės dalies 1803 straipsnio h dalis. Taip pat žr. PCLOB ataskaitą dėl 702 straipsnio, p. 76. Be to, žr. 2011 m. spalio 3 d. FISC memorandumo nuomonę ir įsakymą kaip įsako pašalinti trūkumus pavyzdį, kuriuo vyriausybei buvo nurodyta per 30 dienų ištaisyti nustatytus trūkumus. Pateikiama adresu https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. Žr. Waltono rašto 4 skirsnį, p. 10–11. Taip pat žr. 2018 m. spalio 18 d. FISC nuomonę, pateikiamą adresu https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, kaip patvirtinta 2019 m. liepos 12 d. Užsienio žvalgybos priežiūros apeliacinio teismo nuomonėje, pateikiamoje adresu https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, kurioje FISC, *inter alia*, nurodė vyriausybei laikytis tam tikrų pranešimo, dokumentavimo ir ataskaitų teikimo FISC reikalavimų.

([345]) Žr., pvz., FISC memorandumo nuomonę ir įsakymą, p. 76 (2019 m. gruodžio 6 d.) (kuriuos leista viešai skelbti 2020 m. rugsėjo 4 d.), kuriuose FISC nurodė vyriausybei iki 2020 m. vasario 28 d. pateikti raštišką ataskaitą dėl veiksmų, kurių ėmėsi vyriausybė, kad pagerintų ataskaitų, teikiamų pagal FISA 702 straipsnio informavimo nuostatas ir atšauktų dėl reikalavimų laikymosi priežasčių, nustatymo ir pašalinimo procesus, taip pat dėl kitų klausimų. Taip pat žr. VII priedą.

incidentus siekdamas nustatyti, ar pateikti sertifikatai atitinka FISA reikalavimus. Taip pat nustatęs, kad vyriausybės sertifikatų nepakako, be kita ko, dėl konkrečių su reikalavimų laikymusi susijusių incidentų, FISC gali paskelbti vadinamąjį įsaką pašalinti trūkumus, kuriuo reikalaujama, kad vyriausybė per 30 dienų ištaisytų pažeidimą, arba reikalaujama, kad vyriausybė nutrauktų sertifikavimą pagal 702 straipsnį arba jo nepradėtų. Galiausiai FISC vertina nagrinėjant reikalavimų laikymosi problemas pastebėtas tendencijas ir gali pareikalauti pakeisti procedūras arba užtikrinti papildomą priežiūrą ir ataskaitų teikimą, kad būtų atsižvelgta į reikalavimų laikymosi tendencijas ([346]).

3.2.3. ***Teisių gynimas***

(175) Kaip išsamiau paaiškinta šiame skirsnyje, Jungtinėse Amerikos Valstijose Sąjungos duomenų subjektams suteikiama galimybė keliais būdais imtis teisinių veiksmų nepriklausomame ir nešališkame teisme, turinčiame privalomus įgaliojimus. Visais šiais būdais kartu asmenys gali susipažinti su savo asmens duomenimis, pasiekti, kad būtų peržiūrėtas valdžios sektoriaus galimybių susipažinti su jų duomenimis teisėtumas ir, nustačius pažeidimą, toks pažeidimas būtų ištaisytas, be kita ko, ištaisant ar ištrinant jų asmens duomenis.

(176) Pirma, pagal VP 14086 sukuriamas specialus teisių gynimo mechanizmas, kurį papildo GP reglamentas, kuriuo įsteigiamas Duomenų apsaugos apeliacinis teismas, nagrinėsiantis ir spręsiantis asmenų skundus dėl JAV signalų žvalgybos veiklos. Kiekvienas asmuo ES turi teisę pateikti skundą pagal teisių gynimo mechanizmą dėl įtariamo JAV teisės aktų, kuriais reglamentuojama signalų žvalgybos veikla (pvz., VP 14086, FISA 702 straipsnio, VP 12333), pažeidimo, turinčio neigiamą poveikį su privatumu ir piliečių laisvėmis susijusiems jo interesams ([347]). Šiuo teisių gynimo mechanizmu gali naudotis asmenys iš valstybių arba regioninių ekonominės integracijos organizacijų, kurias JAV generalinis prokuroras pripažino reikalavimus atitinkančiomis valstybėmis ([348]). 2023 m. birželio 30 d. Europos Sąjungą ir tris Europos laisvosios prekybos asociacijos šalis, kurios kartu sudaro Europos ekonominę erdvę, generalinis prokuroras pagal VP 14086 3 straipsnio f punktą pripažino reikalavimus atitinkančiomis valstybėmis ([349]). šis pripažinimas nedaro poveikio Europos Sąjungos sutarties 4 straipsnio 2 daliai;

(177) Tokį skundą norintis pateikti Sąjungos duomenų subjektas turi jį pateikti ES valstybės narės priežiūros institucijai, kurios kompetencija – prižiūrėti valdžios institucijų atliekamą asmens duomenų tvarkymą ([350]). Taip užtikrinamos sąlygos lengvai pasinaudoti teisių gynimo mechanizmu, nes asmenims suteikiama galimybė kreiptis į instituciją „arčiau namų“, su kuria jie gali bendrauti savo kalba. Patikrinusi, ar laikomasi 178 konstatuojamojoje dalyje nurodytų skundo pateikimo reikalavimų, kompetentinga DAI per Europos duomenų apsaugos valdybos sekretoriatą skundą perduos nagrinėti pagal teisių gynimo mechanizmą.

(178) Teikiant skundą pagal teisių gynimo mechanizmą taikomi nedideli priimtinumo reikalavimai, nes asmenims nereikia įrodyti, kad su jų duomenimis iš tiesų buvo vykdoma JAV signalų žvalgybos veikla ([351]). Tuo pat metu, siekiant nustatyti teisių gynimo mechanizmo pradžios tašką, kad būtų galima atlikti peržiūrą, turi būti pateikta tam tikra pagrindinė informacija, pvz., susijusi su asmens duomenimis, kurie, kaip pagrįstai manoma, buvo perduoti JAV, ir priemonėmis, kuriomis, kaip manoma, jie buvo perduoti; JAV vyriausybės subjektų, kurie, kaip manoma, dalyvavo darant įtariamą pažeidimą, tapatybe (jei žinoma); pagrindu, kuriuo remiantis teigiama, kad buvo pažeista JAV teisė (nors tam taip pat nereikia įrodyti, kad JAV žvalgybos agentūros iš tikrųjų rinko asmens duomenis), ir prašomos teisės gynimo priemonės pobūdžiu.

([346]) Žr. VII priedą.

([347]) Žr. VP 14086 4 straipsnio k dalies iv punktą, kuriame nustatyta, kad skundą pagal teisių gynimo mechanizmą asmuo turi pateikti savo vardu (t. y. ne kaip vyriausybės, nevyriausybinės ar tarpvyriausybinės organizacijos atstovas). Sąvoka „nukentėjo“ nereiškia, kad skundo pateikėjas turi atitikti tam tikrus minimalius reikalavimus, kad galėtų pasinaudoti teisių gynimo mechanizmu (šiuo klausimu žr. 178 konstatuojamąją dalį). Ja paaiškinama, kad ODNI CLPO ir DPRC turi įgaliojimus ištaisyti JAV teisės aktų, kuriais reglamentuojama signalų žvalgybos veikla, pažeidimus, dėl kurių nukentėjo skundo pateikėjo asmeninis privatumas ir piliečių laisvių interesai. O taikytinos JAV teisės reikalavimų, kurie nėra skirti asmenims apsaugoti (pvz., biudžeto reikalavimų), pažeidimai į ODNI CLPO ir DPRC jurisdikciją nepatenka.

([348]) VP 14086 3 straipsnio f dalis.

([349]) https://www.justice.gov/opcl/executive-order-14086.

([350]) VP 14086 4 straipsnio d dalies v punktas.

([351]) Žr. VP 14086 4 straipsnio k dalies i–iv punktus.

(179) Pirminį pagal šį teisių gynimo mechanizmą pateiktų skundų nagrinėjimą atlieka ODNI CLPO, kurio dabartinis teisės aktais nustatytas vaidmuo ir įgaliojimai išplėsti, kad jis galėtų imtis tokių konkrečių veiksmų pagal VP 14086 ([352]). Žvalgybos bendruomenėje CLPO, *inter alia*, yra atsakingas už užtikrinimą, kad piliečių laisvių ir privatumo apsauga būtų tinkamai įtraukta į ODNI ir žvalgybos agentūrų politiką ir procedūras; priežiūrą, kaip ODNI laikosi taikomų piliečių laisvių ir privatumo reikalavimų; poveikio privatumui vertinimus ([353]). Nacionalinės žvalgybos direktorius gali atleisti ODNI CLPO tik dėl svarios priežasties, t. y. netinkamo elgesio, piktnaudžiavimo, saugumo pažeidimo, pareigų nevykdymo ar neveiksmingumo ([354]).

(180) Atlikdamas peržiūrą ODNI CLPO gali susipažinti su informacija, kad atliktų vertinimą, ir gali kliautis privaloma įvairių žvalgybos agentūrų privatumo ir piliečių laisvių apsaugos pareigūnų pagalba ([355]). Žvalgybos agentūroms draudžiama trukdyti arba daryti nederamą įtaką ODNI CLPO peržiūroms. Tai taikoma ir Nacionalinės žvalgybos direktoriui – jis taip pat negali kištis atliekant peržiūrą ([356]). Nagrinėdamas skundą, ODNI CLPO privalo teisės aktus taikyti „nešališkai“, atsižvelgdamas tiek į nacionalinio saugumo interesus vykdant signalų žvalgybos veiklą, tiek į privatumo apsaugą ([357]).

(181) Atlikdamas peržiūrą ODNI CLPO nustato, ar taikomi JAV teisės aktai buvo pažeisti, o jei buvo, priima sprendimą dėl tinkamo žalos ištaisymo ([358]). Pastarajame nurodomos priemonės, kuriomis nustatytas pažeidimas visiškai ištaisomas, pvz., neteisėto duomenų gavimo nutraukimas, neteisėtai surinktų duomenų ištrynimas, netinkamai pateiktų užklausų dėl apskritai teisėtai surinktų duomenų rezultatų ištrynimas, galimybės susipažinti su teisėtai surinktais duomenimis suteikimas tik tinkamai parengtiems darbuotojams arba žvalgybos ataskaitų, kuriose yra neturint teisėto leidimo gautų arba neteisėtai platinamų duomenų, atšaukimas ([359]). ODNI CLPO sprendimai dėl asmenų skundų (be kita ko, dėl žalos ištaisymo) atitinkamoms žvalgybos agentūroms yra privalomi ([360]).

(182) ODNI CLPO privalo saugoti savo peržiūros dokumentus ir parengti įslaptintą sprendimą, kuriame būtų paaiškintas pagrindas, kuriuo remiantis jis nustatė faktus, nutarimas, ar atitinkamas pažeidimas buvo padarytas, ir nutarimas, kaip tinkamai ištaisyti žalą ([361]). Jeigu ODNI CLPO atlikus peržiūrą nustatoma, kad pažeidimą padarė kuri nors FISC prižiūrima institucija, CLPO taip pat privalo pateikti įslaptintą ataskaitą generalinio prokuroro padėjėjui nacionalinio saugumo klausimais, šis privalo apie reikalavimų nesilaikymą pranešti FISC, o pastarasis gali imtis tolesnių vykdymo užtikrinimo veiksmų (laikydamasis 173 ir 174 konstatuojamosiose dalyse aprašytos procedūros) ([362]).

(183) Užbaigęs peržiūrą, ODNI CLPO per nacionalinę instituciją informuoja skundą pateikusį asmenį, kad „per peržiūrą atitinkamų pažeidimų nenustatyta arba ODNI CLPO priėmė nutarimą, kuriuo reikalaujama tinkamai ištaisyti žalą“ ([363]). Taip užtikrinamas veiklos, vykdomos siekiant užtikrinti nacionalinį saugumą, konfidencialumas, o asmenims pateikiamas sprendimas, kuriuo patvirtinama, kad jų skundas buvo tinkamai išnagrinėtas ir dėl jo priimtas sprendimas. Be to, šį sprendimą asmuo gali ginčyti. Šiuo tikslu jis bus informuojamas apie galimybę kreiptis į DPRC dėl CLPO nutarimų peržiūros (žr. 184 ir tolesnes konstatuojamąsias dalis) ir apie tai, kad, jei bus kreipiamasi į Teismą, bus išrinktas specialus advokatas skundą pateikusio asmens interesams ginti ([364]).

([352]) VP 14086 3 straipsnio c dalies iv punktas. Taip pat žr. 1947 m. Nacionalinio saugumo aktą, JAV kodekso 50 antraštinės dalies 403–3d straipsnį, 103D straipsnį dėl CLPO vaidmens ODNI.
([353]) JAV kodekso 50 antraštinės dalies 3029 straipsnio b dalis.
([354]) VP 14086 3 straipsnio c dalies iv punktas.
([355]) VP 14086 3 straipsnio c dalies iii punktas.
([356]) VP 14086 3 straipsnio c dalies iv punktas.
([357]) VP 14086 3 straipsnio c dalies i punkto B papunkčio i ir iii papunkčiai.
([358]) VP 14086 3 straipsnio c dalies i punktas.
([359]) VP 14086 4 straipsnio a dalis.
([360]) VP 14086 3 straipsnio c ir d dalys.
([361]) VP 14086 3 straipsnio c dalies i punkto F–G papunkčiai.
([362]) Taip pat žr. VP 14086 3 straipsnio c dalies i punkto D papunktį.
([363]) VP 14086 3 straipsnio c dalies i punkto E papunkčio 1 dalis.
([364]) VP 14086 3 straipsnio c dalies i punkto E papunkčio 2–3 dalys.

(184) Bet kuris skundą pateikęs asmuo ir kiekvienas žvalgybos bendruomenės subjektas gali prašyti ODNI CLPO sprendimą peržiūrėti Duomenų apsaugos apeliaciniame teisme (DPRC). Tokie prašymai dėl peržiūros turi būti pateikti per 60 dienų nuo ODNI CLPO pranešimo, kad peržiūra baigta, gavimo dienos ir juose turi būti pateikta visa informacija, kurią asmuo nori pateikti DPRC (pvz., argumentai dėl teisės klausimų arba teisės taikymo bylos faktams) ([365]). Sąjungos duomenų subjektai prašymą gali dar kartą pateikti kompetentingai DAI (žr. 177 konstatuojamąją dalį).

(185) DPRC yra nepriklausomas teismas, įsteigtas generalinio prokuroro, remiantis VP 14086 ([366]). Jį sudaro bent šeši teisėjai, kuriuos skiria generalinis prokuroras, pasikonsultavęs su PCLOB, Prekybos sekretoriumi ir Nacionalinės žvalgybos direktoriumi, ketverių metų kadencijai, kuri gali būti pratęsta ([367]). Generaliniam prokurorui skiriant teisėjus remiamasi kriterijais, kuriuos taiko vykdomoji valdžia vertindama kandidatus į federalines teismines institucijas, daugiau reikšmės skiriant bet kokiai ankstesnei darbo teisme patirčiai ([368]). Be to, teisėjai turi būti praktikuojantys teisininkai (t. y. aktyvūs ir geros reputacijos advokatūros nariai, turintys tinkamą licenciją verstis teisės praktika) ir turėti pakankamai patirties privatumo ir nacionalinio saugumo teisės srityse. Generalinis prokuroras turi stengtis užtikrinti, kad bent pusė teisėjų bet kuriuo metu turėtų ankstesnės darbo teisme patirties, taip pat visi teisėjai turi turėti patikimumo pažymėjimus, kad galėtų susipažinti su įslaptinta nacionalinio saugumo informacija ([369]).

(186) Į DPRC gali būti skiriami tik asmenys, kurie paskyrimo metu arba per pastaruosius dvejus metus atitinka 185 konstatuojamojoje dalyje nurodytus kvalifikacijos reikalavimus ir nėra vykdomosios valdžios institucijų darbuotojai. Be to, kadencijos DPRC metu teisėjai negali eiti jokių oficialių pareigų ar dirbti JAV vyriausybėje (išskyrus DPRC teisėjų pareigas) ([370]).

(187) Sprendimų priėmimo proceso nepriklausomumas užtikrinamas įvairiomis garantijomis. Visų pirma vykdomajai valdžiai (generaliniam prokurorui ir žvalgybos agentūroms) draudžiama kištis į DPRC vykdomą peržiūrą arba daryti jai nederamą įtaką ([371]). Pats DPRC turi bylose priimti nešališkus sprendimus ([372]) ir veikia pagal savo darbo tvarkos taisykles (priimtas balsų dauguma). Be to, DPRC teisėjus gali atleisti tik generalinis prokuroras ir tik dėl svarios priežasties (t. y. netinkamo elgesio, piktnaudžiavimo, saugumo pažeidimo, pareigų nevykdymo ar neveiksmingumo), deramai atsižvelgdamas į federaliniams teisėjams taikomus standartus, išdėstytus Teismų elgesio ir teismų nepajėgumo procedūrų taisyklėse ([373]).

([365]) GP reglamento 201.6 straipsnio a–b punktai.

([366]) GP reglamento 3 straipsnio d dalies i punktas. Jungtinių Amerikos Valstijų Aukščiausiasis Teismas pripažino, kad generalinis prokuroras gali steigti nepriklausomas įstaigas, turinčias įgaliojimus priimti sprendimus, be kita ko, priimti sprendimus atskirose bylose (visų pirma žr. *Jungtinės Amerikos Valstijos ex rel. Accardi / Shaughnessy,* 347 U.S. 260 (1954) ir *Jungtinės Amerikos Valstijos / Nixon*, 418 U.S. 683, 695 (1974). Ar laikomasi įvairių VP 14086 reikalavimų, pvz., DPRC teisėjų skyrimo ir atleidimo kriterijų ir tvarkos, visų pirma prižiūri Teisingumo departamento generalinis inspektorius (taip pat žr. 109 konstatuojamąją dalį dėl įstatymais suteiktų generalinių inspektorių įgaliojimų).

([367]) VP 14086 3 straipsnio d dalies i punkto A papunktis ir GP reglamento 201.3 straipsnio a dalis.

([368]) GP reglamento 201.3 straipsnio b punktas.

([369]) VP 14086 3 straipsnio d dalies i punkto B papunktis.

([370]) VP 14086 3 straipsnio d dalies i punkto A papunktis ir GP reglamento 201.3 straipsnio a ir c dalys. Į DPRC paskirti asmenys gali dalyvauti neteisminėje veikloje, įskaitant verslo, finansinę, ne pelno lėšų rinkimo ir patikėtinio veiklą, taip pat verstis teisės praktika, jeigu tokia veikla netrukdo nešališkai vykdyti pareigų arba nekenkia DPRC veiksmingumui ar nepriklausomumui (GP reglamento 201.7 straipsnio c dalis).

([371]) VP 14086 3 straipsnio d dalies iii–iv punktai ir GP reglamento 201.7 straipsnio d dalis.

([372]) VP 14086 3 straipsnio d dalies i punkto D papunktis ir GP reglamento 201.9 straipsnis.

([373]) VP 14086 3 straipsnio d dalies iv punktas ir GP reglamento 201.7 straipsnio d dalis. Taip pat žr. Sprendimą *Bumap / Jungtinės Amerikos Valstijos,* 252 U.S. 512, 515 (1920), kuriuo patvirtintas ilgalaikis JAV teisėje įtvirtintas principas, pagal kurį įgaliojimas atleisti yra susijęs su įgaliojimu paskirti (kaip priminė ir Teisingumo departamento Patarėjo Teisės klausimais biuras leidinyje „Konstitucinis Prezidento ir Kongreso valdžių padalijimas“, 20 Op. O.L.C. 124, 166 (1996).

(188) DPRC pateiktus prašymus nagrinėja trijų teisėjų kolegijos, įskaitant pirmininkaujantį teisėją, kuris privalo veikti pagal JAV teisėjų elgesio kodeksą ([374]). Kiekvienai kolegijai padeda specialusis advokatas ([375]), kuris gali susipažinti su visa su byla susijusia informacija, įskaitant įslaptintą informaciją ([376]). Specialiojo advokato vaidmuo – užtikrinti, kad būtų atstovaujama skundą pateikusio asmens interesams ir kad DPRC kolegija būtų gerai informuota apie visus aktualius teisinius ir faktinius klausimus ([377]). Norėdamas išsamiau pagrįsti savo poziciją dėl asmens DPRC pateikto prašymo atlikti peržiūrą, specialusis advokatas gali prašyti skundą pateikusio asmens pateikti informacijos raštu užduodamas klausimų ([378]).

(189) DPRC peržiūri ODNI CLPO priimtus nutarimus (tiek tai, ar buvo pažeista taikoma JAV teisė, tiek dėl tinkamo žalos ištaisymo), remdamasis bent ODNI CLPO tyrimo įrašais, taip pat bet kokia skundą pateikusio asmens, specialiojo advokato arba žvalgybos agentūros pateikta informacija ir pastabomis ([379]). DPRC kolegija gali susipažinti su visa peržiūrai atlikti būtina informacija, kurią gali gauti per ODNI CLPO (pvz., kolegija gali prašyti, kad CLPO papildytų savo įrašą papildoma informacija arba nustatytais faktais, jei to reikia peržiūrai atlikti) ([380]).

(190) Baigdamas peržiūrą DPRC gali: 1) nuspręsti, jog nėra įrodymų, kad buvo vykdoma signalų žvalgybos veikla, susijusi su skundą pateikusio asmens duomenimis, 2) nuspręsti, kad ODNI CLPO nutarimai buvo teisiškai teisingi ir pagrįsti esminiais įrodymais, arba 3) jei nesutinka su ODNI CLPO nutarimais (dėl to, ar buvo pažeisti taikomi JAV teisės aktai arba dėl tinkamo žalos ištaisymo), priimti savo nutarimus ([381]).

([374]) VP 14086 3 straipsnio d dalies i punkto B papunktis ir GP reglamento 201.7 straipsnio a–c dalys. Teisingumo departamento Privatumo ir piliečių laisvių tarnyba (OPCL), kuri yra atsakinga už administracinės paramos teikimą DPRC ir specialiesiems advokatams (žr. GP reglamento 201.5 straipsnį), rotacijos tvarka atrenka trijų asmenų kolegiją, siekdama užtikrinti, kad kiekvienoje kolegijoje būtų bent vienas teisėjas, turintis ankstesnės teisminės patirties (jeigu tokios patirties neturi nė vienas kolegijos teisėjas, pirmininkaujantis teisėjas bus pirmasis OPCL pasirinktas teisėjas).

([375]) GP reglamento 201.4 straipsnis. Generalinis prokuroras, pasikonsultavęs su Prekybos sekretoriumi, Nacionalinės žvalgybos direktoriumi ir PCLOB, skiria bent du specialiuosius advokatus kadencijai, kuri gali būti dukart pratęsta. Specialieji advokatai turi turėti pakankamai patirties privatumo ir nacionalinio saugumo teisės srityse, būti patyrę advokatai, aktyvūs ir geros reputacijos advokatūros nariai ir turėti tinkamą licenciją verstis teisės praktika. Be to, kai yra paskiriami pirmą kartą, jie pastaruosius dvejus metus negali būti buvę vykdomosios valdžios institucijos darbuotojais. Kiekvienai prašymo peržiūrai pirmininkaujantis teisėjas pasirenka specialųjį advokatą padėti kolegijai (žr. GP reglamento 201.8 straipsnio a dalį).

([376]) GP reglamento 201.8 straipsnio c dalis ir 201.11 straipsnis.

([377]) VP 14086 3 straipsnio d dalies i punkto C papunktis ir GP reglamento 201.8 straipsnio e dalis. Specialusis advokatas neveikia kaip skundą pateikusio asmens atstovas ir nepalaiko su juo ryšių kaip su klientu.

([378]) Žr. GP reglamento 201.8 straipsnio d dalies e punktą. Tokius klausimus pirmiausia peržiūri OPCL, konsultuodamasis su atitinkamu žvalgybos bendruomenės subjektu, kad nustatytų ir pašalintų bet kokią įslaptintą, neatskleistiną ar saugomą informaciją prieš ją perduodamas skundą pateikusiam asmeniui. Papildoma informacija, kurią specialusis advokatas gavo atsakymuose į tokius klausimus, pateikiama specialiojo advokato pastabose DPRC.

([379]) VP 14086 3 straipsnio d dalies i punkto D papunktis.

([380]) VP 14086 3 straipsnio d dalies iii punktas ir GP reglamento 201.9 straipsnio b dalis.

([381]) VP 14086 3 straipsnio d dalies i punkto E papunktis ir GP reglamento 201.9 straipsnio c–e dalys. Pagal termino „tinkamas žalos ištaisymas“ apibrėžtį, pateiktą VP 14086 4 skirsnio a punkte, DPRC, priimdamas sprendimą dėl taisomosios priemonės, skirtos pažeidimui visapusiškai ištaisyti, turi atsižvelgti į tai, „kaip paprastai būdavo taisomas nustatytas pažeidimas“, t. y. DPRC, be kitų veiksnių, apsvarstys, kaip panašios atitikties problemos buvo išspręstos praeityje, kad užtikrintų, jog taisomoji priemonė būtų veiksminga ir tinkama.

(191) Visais atvejais DPRC balsų dauguma priima raštišką sprendimą. Jeigu atliekant peržiūrą nustatoma, kad taikomos taisyklės buvo pažeistos, sprendime nurodoma, kaip tinkamai ištaisyti žalą, įskaitant neteisėtai surinktų duomenų ištrynimą, netinkamai atliktų užklausų rezultatų ištrynimą, galimybės susipažinti su teisėtai surinktais duomenimis suteikimą tik tinkamai parengtiems darbuotojams arba žvalgybos ataskaitų, kuriose yra neturint teisėto leidimo gautų arba neteisėtai platinamų duomenų, atšaukimą ([382]). DPRC sprendimas dėl jam pateikto skundo yra privalomas ir galutinis ([383]). Be to, jeigu atlikus peržiūrą nustatoma, kad pažeidimą padarė kuri nors FISC prižiūrima institucija, DPRC taip pat privalo pateikti įslaptintą ataskaitą generalinio prokuroro padėjėjui nacionalinio saugumo klausimais, šis privalo apie reikalavimų nesilaikymą pranešti FISC, o pastarasis gali imtis tolesnių vykdymo užtikrinimo veiksmų (laikydamasis 173 ir 174 konstatuojamosiose dalyse aprašytos procedūros) ([384]).

(192) Kiekvienas DPRC kolegijos sprendimas perduodamas ODNI CLPO ([385]). Jeigu DPRC peržiūra buvo pradėta gavus skundą pateikusio asmens prašymą, skundą pateikusiam asmeniui per nacionalinę instituciją pranešama, kad DPRC užbaigė peržiūrą ir kad „per peržiūrą atitinkamų pažeidimų nenustatyta arba DPRC priėmė nutarimą, kuriuo reikalaujama tinkamai ištaisyti žalą“ ([386]). Teisingumo departamento Privatumo ir piliečių laisvių tarnyba saugo visos DPRC peržiūrėtos informacijos ir visų paskelbtų sprendimų įrašus ir pateikia juos būsimoms DPRC kolegijoms, kad jos galėtų į tai atsižvelgti kaip į neprivalomą precedentą ([387]).

(193) Taip pat reikalaujama, kad Prekybos departamentas saugotų įrašus apie kiekvieną skundą pateikusį asmenį ([388]). Kad būtų padidintas skaidrumas, Prekybos departamentas privalo bent kas penkerius metus kreiptis į atitinkamas žvalgybos agentūras, kad patikrintų, ar su DPRC atliekama peržiūra susijusi informacija yra išslaptinta ([389]). Jeigu taip yra, asmeniui bus pranešta, kad tokia informacija gali būti prieinama pagal taikomus teisės aktus (t. y. kad asmuo gali prašyti leisti su ja susipažinti pagal Informacijos laisvės aktą; žr. 199 konstatuojamąją dalį).

(194) Galiausiai bus atliekamas reguliarus ir nepriklausomas vertinimas, ar šis teisių gynimo mechanizmas veikia tinkamai. Konkrečiau, pagal VP 14086 teisių gynimo mechanizmo veikimą kasmet peržiūri nepriklausoma įstaiga PCLOB (žr. 110 konstatuojamąją dalį) ([390]). Atlikdama šią peržiūrą, PCLOB, be kita ko, įvertins, ar ODNI CLPO ir DPRC skundus išnagrinėjo laiku; ar jiems buvo sudarytos sąlygos visapusiškai susipažinti su reikiama informacija; ar peržiūros procese tinkamai atsižvelgta į VP 14086 nustatytas esmines apsaugos priemones ir ar žvalgybos bendruomenė visapusiškai laikėsi ODNI CLPO ir DPRC nutarimų. PCLOB pateiks savo peržiūros rezultatų ataskaitą Prezidentui, generaliniam prokurorui, Nacionalinės žvalgybos direktoriui, žvalgybos agentūrų vadovui, ODNI CLPO ir Kongreso žvalgybos komitetams, taip pat bus viešai paskelbta jos neįslaptinta redakcija, be to, ja bus remiamasi Komisijai atliekant periodinę šio sprendimo veikimo peržiūrą. Generalinis prokuroras, Nacionalinės žvalgybos direktorius, ODNI CLPO ir žvalgybos agentūrų vadovai privalo įgyvendinti visas į tokias ataskaitas įtrauktas rekomendacijas arba kitaip į jas atsižvelgti. Be to, PCLOB kasmet vykdys viešą sertifikavimą, atsižvelgdama į tai, ar skundų nagrinėjimas pagal teisių gynimo mechanizmą atitinka VP 14086 reikalavimus.

([382]) VP 14086 4 straipsnio a dalis.

([383]) VP 14086 3 straipsnio d dalies ii punktas ir GP reglamento 201.9 straipsnio g dalis. Kadangi DPRC sprendimas yra galutinis ir privalomas, jokia kita vykdomoji ar administracinė institucija ar įstaiga (įskaitant Jungtinių Amerikos Valstijų prezidentą) negali panaikinti DPRC sprendimo. Tai taip pat patvirtinta Aukščiausiojo Teismo praktikoje, kurioje išaiškinta, kad generalinis prokuroras, deleguodamas vykdomajai valdžiai išskirtinius generalinio prokuroro įgaliojimus priimti privalomus sprendimus nepriklausomai įstaigai, atsisako galimybės kokiu nors būdu daryti įtaką tos institucijos sprendimui (žr. Sprendimą *Jungtinės Amerikos Valstijos ex rel. Accardi / Shaughnessy*, 347 U.S. 260 (1954).

([384]) VP 14086 3 straipsnio d dalies i punkto F papunktis ir GP reglamento 201.9 straipsnio i dalis.

([385]) GP reglamento 201.9 straipsnio h dalis.

([386]) VP 14086 3 straipsnio d dalies i punkto H papunktis ir GP reglamento 201.9 straipsnio h dalis. Dėl pranešimo pobūdžio žr. GP reglamento 201.9 straipsnio h dalies 3 punktą.

([387]) GP reglamento 201.9 straipsnio j dalis.

([388]) VP 14086 3 straipsnio d dalies v punkto A papunktis.

([389]) VP 14086 3 straipsnio d dalies v punktas.

([390]) VP 14086 3 straipsnio e dalis. Taip pat žr. https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

(195) Visų asmenų (nepaisant pilietybės ar gyvenamosios vietos) teisių gynimą galima užtikrinti ne tik pagal VP 14086 nustatytu specialiu teisių gynimo mechanizmu, bet ir kreipiantis į JAV bendrosios kompetencijos teismus ([391]).

(196) Visų pirma FISA ir susijusiuose įstatymuose numatyta galimybė asmenims pareikšti civilinį ieškinį dėl piniginio žalos atlyginimo Jungtinėms Amerikos Valstijoms, kai informacija apie juos buvo neteisėtai ir tyčia panaudota arba atskleista ([392]); pareikšti ieškinį dėl piniginio žalos atlyginimo JAV vyriausybės pareigūnams kaip individualiems asmenims ([393]) ir ginčyti stebėjimo teisėtumą (ir prašyti panaikinti informaciją), jeigu JAV vyriausybė ketina naudoti arba atskleisti bet kokią informaciją, gautą arba įgytą vykdant asmens elektroninį stebėjimą JAV teismo arba administraciniuose procesuose ([394]). Apskritai, jei vyriausybė ketina naudoti informaciją, gautą vykdant žvalgybos operacijas, prieš įtariamąjį baudžiamojoje byloje, Konstitucija ir įstatymais nustatytais reikalavimais ([395]) įpareigojama atskleisti tam tikrą informaciją, kad atsakovas galėtų ginčyti vyriausybės vykdomo įrodymų rinkimo ir naudojimo teisėtumą.

(197) Be to, esama konkrečių būdų pasinaudoti teisių gynimo priemonėmis prieš valdžios sektoriaus pareigūnus dėl neteisėto valdžios sektoriaus susipažinimo su asmens duomenimis arba neteisėto jų naudojimo, be kita ko, tariamais nacionalinio saugumo tikslais (t. y. pagal Kompiuterinio sukčiavimo ir piktnaudžiavimo aktą ([396]), Elektroninių ryšių privatumo aktą ([397]) ir Teisės į finansinį privatumą aktą ([398])). Visi tokie teisiniai veiksmai susiję su konkrečiais duomenimis, susipažinimo su jais tikslais ir (arba) tipais (pvz., nuotolinė prieiga prie kompiuterio per internetą) ir gali būti pradėti tam tikromis sąlygomis (pvz., sąmoningas ar tyčinis elgesys, elgesys veikiant kaip privačiam asmeniui, patirta žala).

(198) APA ([399]) nustatyta bendresnio pobūdžio galimybė ginti teises, pagal kurią „asmuo, kuris dėl agentūros veiksmų patyrė neigiamų teisinių padarinių, nukentėjo arba jo padėtis pablogėjo“, turi teisę kreiptis dėl teisminės peržiūros ([400]). Tai apima galimybę prašyti, kad teismas „agentūros veiksmus, sprendimus ir išvadas, kurie, kaip nustatyta <...> yra šališki, savavališki, kilę iš piktnaudžiavimo įgaliojimais ar kitaip neatitinka įstatymų, pripažintų neteisėtais ir panaikintų“ ([401]). Pavyzdžiui, 2015 m. federalinis apeliacinis teismas dėl pagal APA pateikto ieškinio priėmė sprendimą, kad JAV vyriausybės masinis telefonijos metaduomenų rinkimas nebuvo leidžiamas pagal FISA 501 straipsnį ([402]).

([391]) Galimybė naudotis šiais būdais priklauso nuo to, ar įrodoma, kad asmuo „patyrė žalą“. Šis visiems asmenims, neatsižvelgiant į pilietybę, taikomas standartas kyla iš „bylos arba ginčo“ reikalavimo, nustatyto JAV Konstitucijos III straipsnyje. Anot Aukščiausiojo Teismo, tai reiškia, kad 1) asmuo patyrė „faktinę žalą“ (t. y. teisiškai saugomas suinteresuotasis asmuo iš tiesų patyrė arba neišvengiamai patirs konkrečią ir aiškiai įvardijamą žalą), 2) yra priežastinis ryšys tarp žalos ir veiksmų, dėl kurių kreipiamasi į teismą, ir 3) tikėtina, o ne vien spėjama, kad palankiu teismo sprendimu žala bus ištaisoma (žr. *Lujan / Defenders of Wildlife*, 504 U.S. 555 (1992)).

([392]) JAV kodekso 18 antraštinės dalies 2712 straipsnis.

([393]) JAV kodekso 50 antraštinės dalies 1810 straipsnis.

([394]) JAV kodekso 50 antraštinės dalies 1806 straipsnis.

([395]) Žr. atitinkamai *Brady / Maryland*, 373 U.S. 83 (1963) ir Jenckso aktą, JAV kodekso 18 antraštinės dalies 3500 straipsnį.

([396]) JAV kodekso 18 antraštinės dalies 1030 straipsnis.

([397]) JAV kodekso 18 antraštinės dalies 2701–2712 straipsniai.

([398]) JAV kodekso 12 antraštinės dalies 3417 straipsnis.

([399]) JAV kodekso 5 antraštinės dalies 702 straipsnis.

([400]) Paprastai atliekama tik „galutinio“ (o ne „išankstinio, procesinio ar tarpinio“) agentūros veiksmo teisminė peržiūra. Žr. JAV kodekso 5 antraštinės dalies 704 straipsnį.

([401]) JAV kodekso 5 antraštinės dalies 706 straipsnio 2 dalies A punktas.

([402]) *ACLU / Clapper*, 785 F.3d 787 (2d Cir. 2015). Šiose bylose ginčijama masinio telefonijos duomenų rinkimo programa buvo nutraukta 2015 m. JAV Laisvės aktu.

(199) Galiausiai, be 176–198 konstatuojamosiose dalyse nurodytų teisių gynimo būdų, kiekvienas asmuo turi teisę prašyti leisti susipažinti su esamais federalinių agentūrų įrašais pagal FOIA, įskaitant atvejus, kai juose yra to asmens duomenų ([403]). Gavus tokią galimybę taip pat gali būti lengviau iškelti bylą bendrosios kompetencijos teismuose, be kita ko, tai gali padėti įrodyti „patirtą žalą“. Agentūros gali neatskleisti informacijos, kuriai taikomos tam tikros išvardytos išimtys, įskaitant galimybę susipažinti su įslaptinta nacionalinio saugumo informacija ir su teisėsaugos tyrimais susijusia informacija ([404]), tačiau skundą pateikę asmenys, kurių netenkina atsakymas, turi galimybę jį užginčyti prašydami administracinės ir vėliau teisminės peržiūros (federaliniuose teismuose) ([405]).

(200) Iš to, kas išdėstyta, darytina išvada, kad kai JAV teisėsaugos ir nacionalinio saugumo institucijos susipažįsta su asmens duomenimis, kuriems taikomas šis sprendimas, toks susipažinimas su duomenimis reglamentuojamas pagal teisinę sistemą, kurioje nustatytos sąlygos, pagal kurias galimybė susipažinti su duomenimis gali būti suteikta, ir kuriuo užtikrinama, kad su duomenimis susipažįstama ir jie toliau naudojami tik tiek, kiek būtina ir proporcinga atsižvelgiant į siekiamą viešojo intereso tikslą. Šiomis apsaugos priemonėmis gali remtis asmenys, turintys teisę į veiksmingą teisių gynimą.

4. **IŠVADA**

(201) Komisija mano, kad Jungtinės Amerikos Valstijos, taikydamos JAV Prekybos departamento paskelbtus Principus, užtikrina pagal ES ir JAV duomenų privatumo sistemą iš Sąjungos sertifikuotoms organizacijoms Jungtinėse Amerikos Valstijose perduodamų asmens duomenų apsaugos lygį, kuris yra iš esmės lygiavertis Reglamentu (ES) 2016/679 užtikrinamai apsaugai.

(202) Be to, Komisija mano, kad veiksmingas Principų taikymas užtikrinamas skaidrumo įpareigojimais ir Prekybos departamento administruojama DPS. Be to, JAV teisėje numatytais priežiūros mechanizmais ir teisių gynimo būdais apskritai sudaromos sąlygos praktiškai nustatyti duomenų apsaugos taisyklių pažeidimus ir už juos taikyti sankcijas, o duomenų subjektui suteikiama teisių gynimo priemonių, kad jis galėtų gauti galimybę susipažinti su asmens duomenimis, kurie yra susiję su juo, ir galiausiai ištaisyti ar ištrinti tokius duomenis.

(203) Galiausiai, remdamasi turima informacija apie JAV teisinę tvarką, įskaitant VI ir VII prieduose pateikiamą informaciją, Komisija mano, kad bet koks JAV valdžios institucijų vykdomas asmenų, kurių asmens duomenys iš Sąjungos perduodami į Jungtines Amerikos Valstijas pagal ES ir JAV duomenų privatumo sistemą, pagrindinių teisių ribojimas viešojo intereso tikslais, visų pirma baudžiamosios teisėsaugos ir nacionalinio saugumo tikslais, bus griežtai apribojamas jį taikant tik tada, kai būtina atitinkamam teisėtam tikslui pasiekti, ir kad egzistuoja veiksminga teisinė apsauga tokio ribojimo atžvilgiu. Todėl, atsižvelgiant į pirmiau pateiktas išvadas, turėtų būti nuspręsta, kad Jungtinės Amerikos Valstijos užtikrina tinkamą asmens duomenų, perduodamų iš Europos Sąjungos pagal ES ir JAV duomenų privatumo sistemą sertifikuotoms organizacijoms, apsaugos lygį, kaip nustatyta Reglamento (ES) 2016/679 45 straipsnyje, aiškinamame atsižvelgiant į Europos Sąjungos pagrindinių teisių chartiją.

(204) Atsižvelgiant į tai, kad VP 14086 nustatyti apribojimai, apsaugos priemonės ir teisių gynimo mechanizmas yra esminiai JAV teisinės sistemos, kuria remiasi Komisijos vertinimas, elementai, šio sprendimo priėmimas visų pirma priklauso nuo to, ar visos JAV žvalgybos agentūros patvirtino atnaujintą VP 14086 įgyvendinimo politiką bei procedūras ir ar Sąjunga teisių gynimo mechanizmo tikslais paskelbta reikalavimus atitinkančia organizacija atitinkamai 2023 m. liepos 3 d. (žr. 126 konstatuojamąją dalį) ir 2023 m. birželio 30 d. (žr. 176 konstatuojamąją dalį.).

([403]) JAV kodekso 5 antraštinės dalies 552 straipsnis. Panašūs teisės aktai galioja valstijų lygmeniu.

([404]) Tokiu atveju asmuo paprastai gauna tik standartinį atsakymą, kuriame agentūra atsisako patvirtinti arba paneigti, kad kokių įrašų esama. Žr. *ACLU / CIA*, 710 F.3d 422 (D.C. Cir. 2014). Slaptumo kriterijai ir trukmė nustatyti Vykdomajame potvarkyje Nr. 13526, kuriame numatyta, kad paprastai, atsižvelgiant į informacijos slaptumo dėl nacionalinio saugumo trukmę, turi būt nustatoma konkreti išslaptinimo data ar įvykis, kada informacija turi būti automatiškai išslaptinama (žr. VP 13526 1.5 skirsnį).

([405]) Teismas *de novo* nustato, ar įrašai saugomi teisėtai, ir gali liepti vyriausybei suteikti galimybę susipažinti su įrašais (JAV kodekso 5 antraštinės dalies 552 straipsnio a dalies 4 punkto B papunktis).

5. **ŠIO SPRENDIMO PADARINIAI IR DUOMENŲ APSAUGOS INSTITUCIJŲ VEIKSMAI**

(205) Valstybės narės ir jų institucijos privalo imtis priemonių, kurios yra būtinos siekiant užtikrinti atitiktį Sąjungos institucijų aktams, nes preziumuojama, kad Sąjungos institucijų 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 neteisėtumu grindžiamą prieštaravimą.

(206) Todėl Komisijos sprendimas dėl tinkamumo, kurį ji priėmė pagal Reglamento (ES) 2016/679 45 straipsnio 3 dalį, yra privalomas visoms valstybių narių, kurioms yra skirtas, institucijoms, įskaitant tų valstybių narių nepriklausomas priežiūros institucijas. Visų pirma Sąjungoje esantys duomenų valdytojai arba duomenų tvarkytojai duomenis sertifikuotoms organizacijoms Jungtinėse Amerikos Valstijose gali perduoti be papildomo leidimo.

(207) Reikėtų priminti, kad pagal Reglamento (ES) 2016/679 58 straipsnio 5 dalį ir kaip išaiškinta Teisingumo Teismo sprendime *Schrems* ([406]), jeigu nacionalinei duomenų apsaugos institucijai kyla klausimų, be kita ko, kai pateikiamas skundas, dėl Komisijos sprendimo dėl tinkamumo derėjimo su asmens pagrindinėmis teisėmis į privatumą ir duomenų apsaugą, nacionalinėje teisėje jai turi būti numatyta teisinė teisių gynimo priemonė, kad ji šiuos prieštaravimus galėtų pareikšti nacionaliniame teisme, o šiam gali reikėti pateikti Teisingumo Teismui prašymą priimti prejudicinį sprendimą ([407]).

6. **ŠIO SPRENDIMO STEBĖSENA IR PERŽIŪRA**

(208) Remiantis Teisingumo Teismo praktika ([408]), ir, kaip pripažįstama Reglamento (ES) 2016/679 45 straipsnio 4 dalyje, Komisija po sprendimo dėl tinkamumo priėmimo turėtų nuolat stebėti atitinkamus pokyčius trečiojoje valstybėje, kad įvertintų, ar ta trečioji valstybė vis dar užtikrina iš esmės lygiavertį apsaugos lygį. Tokia patikra turi būti atliekama visais atvejais, kai Komisija gauna informacijos, dėl kurios jai šiuo atžvilgiu kyla pagrįstų abejonių.

(209) Todėl Komisija turėtų nuolat stebėti su šiame sprendime įvertinta asmens duomenų tvarkymo teisine sistema ir faktine praktika susijusią padėtį Jungtinėse Amerikos Valstijose. Kad palengvintų šį procesą, JAV valdžios institucijos turėtų nedelsdamos informuoti Komisiją apie esminius JAV teisinės tvarkos pokyčius, kurie turi poveikio pagal šį sprendimą reglamentuojamai teisinei sistemai, taip pat apie bet kokius praktikos, susijusios su šiame sprendime įvertintu asmens duomenų tvarkymu, pokyčius, kiek tai susiję su sertifikuotų organizacijų Jungtinėse Amerikos Valstijose vykdomu asmens duomenų tvarkymu, taip pat apribojimais ir apsaugos priemonėmis, taikomais valdžios institucijoms susipažįstant su asmens duomenimis.

(210) Be to, tam, kad Komisija galėtų veiksmingai vykdyti stebėsenos funkciją, valstybės narės turėtų Komisijai pranešti apie visus susijusius veiksmus, kurių ėmėsi nacionalinės duomenų apsaugos institucijos, visų pirma dėl Sąjungos duomenų subjektų užklausų ar skundų, susijusių su asmens duomenų perdavimu iš Sąjungos sertifikuotoms organizacijoms Jungtinėse Amerikos Valstijose. Komisijai taip pat reikėtų pranešti apie bet kokius požymius, kad JAV valdžios institucijų, atsakingų už nusikalstamų veikų prevenciją, tyrimą, nustatymą ar baudžiamąjį persekiojimą už jas, arba atsakingų už nacionalinį saugumą, įskaitant visas priežiūros įstaigas, veiksmais reikiamo lygio apsauga neužtikrinama.

([406]) Sprendimas *Schrems*, 65 punktas.

([407]) Sprendimas *Schrems*, 65 punktas: „Šiuo atžvilgiu nacionalinis teisės aktų leidėjas turi numatyti teisių gynimo priemones, leidžiančias atitinkamai nacionalinei priežiūros institucijai remtis nacionaliniuose teismuose kaltinimais, kurie, jos nuomone, yra pagrįsti, tam, kad šie teismai, vertindami Komisijos sprendimo galiojimą, pateiktų prašymą priimti prejudicinį sprendimą, jei, kaip ir ši institucija, turėtų abejonių dėl šio sprendimo galiojimo.“

([408]) Sprendimas *Schrems*, 76 punktas.

(211) Taikydama Reglamento (ES) 2016/679 ([409]) 45 straipsnio 3 dalį, Komisija, priėmus šį sprendimą, turėtų periodiškai peržiūrėti, ar su Jungtinių Amerikos Valstijų pagal ES ir JAV DPS užtikrinamo apsaugos lygio tinkamumu susijusios išvados vis dar yra faktiškai ir teisiškai pagrįstos. Kadangi visų pirma VP 14086 ir GP reglamente reikalaujama sukurti naujus mechanizmus ir įgyvendinti naujas apsaugos priemones, šis sprendimas pirmą kartą turėtų būti peržiūrėtas per vienus metus nuo įsigaliojimo, siekiant patikrinti, ar visi susiję elementai yra visiškai įgyvendinti ir veiksmingai veikia praktiškai. Po pirmosios peržiūros, atsižvelgdama į jos rezultatus, Komisija, glaudžiai konsultuodamasi su pagal Reglamento (ES) 2016/679 93 straipsnio 1 dalį įsteigtu komitetu ir Europos duomenų apsaugos valdyba, nuspręs, kaip dažnai ateityje reikia atlikti peržiūras ([410]).

(212) Kad atliktų peržiūras, Komisija turėtų susitikti su Prekybos departamento, FPK ir Transporto departamento, taip pat prireikus su kitų departamentų ir agentūrų, dalyvaujančių įgyvendinant ES ir JAV DPS, atstovais, o dėl klausimų, susijusių su valdžios sektoriaus galimybe susipažinti su duomenimis, – su Teisingumo departamento, ODNI (įskaitant CLPO), kitų žvalgybos bendruomenės subjektų ir DPRC atstovais, taip pat specialiaisiais advokatais. Turėtų būti suteiktos galimybės tokiame susitikime dalyvauti Europos duomenų apsaugos valdybos atstovams.

(213) Peržiūros turėtų apimti visus šio sprendimo veikimo aspektus, susijusius su asmens duomenų tvarkymu Jungtinėse Amerikos Valstijose, visų pirma Principų taikymą ir įgyvendinimą, ypatingą dėmesį skiriant toliau perduodant duomenis taikomoms apsaugos priemonėms; atitinkamiems teismų praktikos pokyčiams; naudojimosi asmens teisėmis veiksmingumui; stebėsenai, kaip laikomasi Principų, ir užtikrinimui, kad jų būtų laikomasi; taip pat apribojimams ir apsaugos priemonėms, susijusiems su valdžios sektoriaus galimybėmis susipažinti su informacija, visų pirma VP 14086 nustatytų apsaugos priemonių įgyvendinimui ir taikymui, be kita ko, taikant žvalgybos agentūrų parengtą politiką ir procedūras; VP 14086 ir FISA 702 straipsnio bei VP 12333 sąveikai ir priežiūros mechanizmų bei teisių gynimo priemonių veiksmingumui (įskaitant naujo teisių gynimo mechanizmo, nustatyto pagal VP 14086, veikimą). Atliekant tokias peržiūras dėmesys bus skiriamas ir DAI bei Jungtinių Amerikos Valstijų kompetentingų institucijų bendradarbiavimui, įskaitant gairių ir kitų aiškinamųjų priemonių, susijusių su Principų taikymu ir kitais sistemos veikimo aspektais, rengimą.

(214) Remdamasi peržiūra, Komisija turėtų parengti viešą ataskaitą, kuri bus teikiama Europos Parlamentui ir Tarybai.

7. **SPRENDIMO GALIOJIMO SUSTABDYMAS, PANAIKINIMAS ARBA PAKEITIMAS**

(215) Jeigu iš turimos informacijos, ypač iš informacijos, surinktos vykdant šio sprendimo įgyvendinimo stebėseną arba pateiktos JAV arba valstybių narių valdžios institucijų, paaiškėja, kad tinkamas pagal šį sprendimą perduodamų duomenų apsaugos lygis galbūt jau neužtikrinamas, Komisija turėtų nedelsdama apie tai informuoti kompetentingas JAV institucijas ir paprašyti per nustatytą pagrįstą terminą imtis tinkamų priemonių.

(216) Jeigu pasibaigus tam nustatytam terminui kompetentingos JAV institucijos nesiima tokių priemonių arba kitaip įtikinamai neįrodo, kad šis sprendimas ir toliau grindžiamas tinkamu apsaugos lygiu, Komisija pradės Reglamento (ES) 2016/679 93 straipsnio 2 dalyje nurodytą procedūrą, siekdama iš dalies arba visiškai sustabdyti šio sprendimo galiojimą arba jį panaikinti.

(217) Kita vertus, Komisija pradės tą procedūrą siekdama iš dalies pakeisti sprendimą, visų pirma nustatydama, kad duomenų perdavimui turi būti taikomos papildomos sąlygos, arba apribodama išvadą dėl duomenų apsaugos tinkamumo taip, kad ji būtų taikoma tik tokiam duomenų perdavimui, kurį vykdant ir toliau užtikrinama tinkamo lygio apsauga.

([409]) Pagal Reglamento (ES) 2016/679 45 straipsnio 3 dalį „[į]gyvendinimo akte numatomas periodinės peržiūros, <...> kuria atsižvelgiama į visus atitinkamus pokyčius trečiojoje valstybėje ar tarptautinėje organizacijoje, mechanizmas."

([410]) Reglamento (ES) 2016/679 45 straipsnio 3 dalyje nustatyta, kad periodinė peržiūra turi būti atliekama „bent kas ketverius metus". Taip pat žr. Europos duomenų apsaugos valdybos darbinį dokumentą „Orientaciniai tinkamumo kriterijai", WP 254, 1-oji peržiūrėta versija.

(218) Komisija galiojimo sustabdymo arba panaikinimo procedūrą visų pirma turėtų pradėti, jeigu:

(a) yra požymių, kad organizacijos, pagal šį sprendimą gavusios asmens duomenų iš Sąjungos, nesilaiko Principų ir kad kompetentingos priežiūros ir vykdymo užtikrinimo įstaigos veiksmingai nesprendžia tokio nesilaikymo problemos;

(b) yra požymių, kad JAV valdžios institucijos nesilaiko taikomų sąlygų ir apribojimų, susijusių su galimybe JAV valdžios institucijoms teisėsaugos ir nacionalinio saugumo tikslais susipažinti su asmens duomenimis, perduotais pagal ES ir JAV DPS, arba

(c) nėra veiksmingai nagrinėjami Sąjungos duomenų subjektų skundai, be kita ko, to veiksmingai nedaro ODNI CLPO ir (arba) DPRC.

(219) Komisija taip pat turėtų apsvarstyti galimybę pradėti procedūrą dėl šio sprendimo pakeitimo, galiojimo sustabdymo ar panaikinimo, jeigu JAV kompetentingos institucijos nepateikia informacijos arba paaiškinimų, kurie yra būtini norint įvertinti užtikrinamą iš Sąjungos į Jungtines Amerikos Valstijas perduodamų asmens duomenų apsaugos lygį arba tai, kaip laikomasi šio sprendimo. Šiuo atžvilgiu Komisija turėtų atsižvelgti į tai, kiek atitinkamos informacijos galima gauti iš kitų šaltinių.

(220) Dėl tinkamai pagrįstų skubos priežasčių, pvz., jei VP 14086 arba GP reglamentas būtų iš dalies pakeisti taip, kad būtų sumažintas šiame sprendime apibūdintas apsaugos lygis, arba generalinis prokuroras atšauks Sąjungos pripažinimą teisių gynimo mechanizmo tikslais reikalavimus atitinkančia organizacija, Komisija pasinaudos galimybe laikydamasi Reglamento (ES) 2016/679 93 straipsnio 3 dalyje nurodytos procedūros priimti nedelsiant taikytinus įgyvendinimo aktus, kuriais sustabdomas šio sprendimo galiojimas, šis sprendimas panaikinamas arba iš dalies keičiamas.

8. **BAIGIAMOSIOS PASTABOS**

(221) Europos duomenų apsaugos valdyba paskelbė savo nuomonę ([411]), į kurią buvo atsižvelgta rengiant šį sprendimą.

(222) Europos Parlamentas priėmė rezoliuciją dėl ES ir JAV duomenų privatumo sistema užtikrinamos apsaugos tinkamumo ([412]).

(223) Šiame sprendime numatytos priemonės atitinka pagal Reglamento (ES) 2016/679 93 straipsnio 1 dalį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Atsižvelgdamos į Reglamento (ES) 2016/679 45 straipsnį, Jungtinės Amerikos Valstijos užtikrina tinkamą asmens duomenų, perduodamų iš Sąjungos Jungtinėse Amerikos Valstijose esančioms organizacijoms, įtrauktoms į Duomenų privatumo sistemos sąrašą, kurį pagal I priedo I.3 skirsnį tvarko ir viešai skelbia JAV Prekybos departamentas, apsaugos lygį.

2 straipsnis

Jeigu valstybių narių kompetentingos institucijos, siekdamos apsaugoti asmenis tvarkant jų asmens duomenis, dėl šio sprendimo 1 straipsnyje nurodyto duomenų perdavimo įgyvendina savo įgaliojimus pagal Reglamento (ES) 2016/679 58 straipsnį, atitinkama valstybė narė nedelsdama apie tai informuoja Komisiją.

([411]) 2023 m. vasario 28 d. Nuomonė 5/2023 dėl Europos Komisijos įgyvendinimo sprendimo dėl tinkamos asmens duomenų apsaugos pagal ES ir JAV duomenų privatumo sistemą projekto.

([412]) Europos Parlamento rezoliucija dėl ES ir JAV duomenų privatumo sistema užtikrinamos apsaugos tinkamumo (2023/2501(RSP).

3 straipsnis

1. Komisija nuolat stebi, kaip taikoma teisinė sistema, kuri yra šio sprendimo dalykas, įskaitant sąlygas, kuriomis vykdomas tolesnis duomenų perdavimas, naudojamasi asmens teisėmis ir JAV valdžios institucijoms suteikiama galimybė susipažinti su duomenimis, kurie buvo perduoti pagal šį sprendimą, siekdama įvertinti, ar Jungtinės Amerikos Valstijos ir toliau užtikrina 1 straipsnyje nurodytą tinkamą apsaugos lygį.

2. Valstybės narės ir Komisija informuoja viena kitą apie atvejus, kai atrodo, kad Jungtinių Amerikos Valstijų įstaigos, naudodamosi įstatymais suteiktais įgaliojimais užtikrinti, kad būtų laikomasi I priede išdėstytų Principų, nenustato veiksmingų nustatymo ir priežiūros mechanizmų, leidžiančių praktiškai nustatyti I priede išdėstytų Principų pažeidimus ir už juos skirti sankcijas.

3. Valstybės narės ir Komisija informuoja viena kitą apie bet kokius požymius, kad JAV valdžios institucijos, atsakingos už nacionalinį saugumą, teisėsaugą ar kitus viešuosius interesus, asmenų teises į jų asmens duomenų apsaugą riboja labiau, nei būtina ir proporcinga, ir (arba) kad nėra veiksmingos teisinės apsaugos nuo tokio ribojimo.

4. Po vienų metų nuo pranešimo apie šį sprendimą valstybėms narėms dienos, o vėliau tokiu periodiškumu, kuris bus nustatytas glaudžiai konsultuojantis su pagal Reglamento (ES) 2016/679 93 straipsnio 1 dalį įsteigtu komitetu ir Europos duomenų apsaugos valdyba, Komisija įvertina 1 straipsnio 1 dalyje nurodytą išvadą remdamasi visa turima informacija, įskaitant informaciją, gautą kartu su Jungtinių Amerikos Valstijų kompetentingomis institucijomis atliekant peržiūrą.

5. Nustačiusi požymių, kad tinkamas apsaugos lygis jau neužtikrinamas, Komisija apie tai informuoja JAV kompetentingas institucijas. Prireikus Komisija pagal Reglamento (ES) 2016/679 45 straipsnio 5 dalį priima sprendimą laikinai sustabdyti šio sprendimo galiojimą, jį iš dalies pakeisti ar panaikinti arba apriboti jo taikymo sritį. Komisija taip pat gali priimti tokį sprendimą, jei JAV vyriausybei nepakankamai bendradarbiaujant negali nustatyti, ar Jungtinės Amerikos Valstijos ir toliau užtikrina tinkamą apsaugos lygį.

4 straipsnis

Šis sprendimas skirtas valstybėms narėms.

Priimta Briuselyje 2023 m. liepos 10 d.

Komisijos vardu
Didier REYNDERS
Komisijos narys

I PRIEDAS

JAV PREKYBOS DEPARTAMENTO PASKELBTI ES IR JAV DUOMENŲ PRIVATUMO SISTEMOS PRINCIPAI

I. APŽVALGA

1. Nors Jungtinės Amerikos Valstijos ir Europos Sąjunga (toliau – ES) yra bendrai įsipareigojusios stiprinti privatumo apsaugą bei teisinės valstybės principą ir pripažįsta transatlantinių duomenų srautų svarbą atitinkamai savo piliečiams, ekonomikai ir visuomenei, Jungtinės Amerikos Valstijos laikosi kitokio požiūrio į privatumo apsaugą nei ES. Jungtinėse Amerikos Valstijose taikomas sektorių metodas, paremtas teisės aktų, reguliavimo ir savireguliavimo deriniu. JAV prekybos departamentas (toliau – Departamentas), remdamasis įstatymais suteiktais įgaliojimais skatinti, palaikyti ir plėtoti tarptautinę prekybą (JAV kodekso 15 antraštinės dalies 1512 straipsnis), skelbia ES ir JAV duomenų privatumo sistemos principus, įskaitant papildomus principus (toliau kartu – Principai) ir Principų I priedą (toliau – I priedas). Principai parengti konsultuojantis su Europos Komisija (toliau – Komisija), sektoriaus atstovais ir kitais suinteresuotaisiais subjektais, siekiant palengvinti prekybą ir komercinę veiklą tarp Jungtinių Amerikos Valstijų ir ES. Principais, kurie yra viena pagrindinių ES ir JAV duomenų privatumo sistemos (toliau – ES ir JAV DPS) sudedamųjų dalių, organizacijoms Jungtinėse Amerikos Valstijose suteikiamas patikimas asmens duomenų perdavimo iš ES į Jungtines Amerikos Valstijas mechanizmas ir kartu užtikrinama, kad ES duomenų subjektai ir toliau galėtų naudotis veiksmingomis apsaugos priemonėmis ir apsauga, kaip reikalaujama pagal Europos teisės aktus, kiek tai susiję su jų asmens duomenų tvarkymu, kai duomenys perduodami į ES nepriklausančias šalis. Principai skirti taikyti tik reikalavimus atitinkančioms Jungtinėse Amerikos Valstijose veikiančioms organizacijoms, iš ES gaunančioms asmens duomenų, kad jos turėtų teisę dalyvauti ES ir JAV DPS ir remtis Komisijos sprendimu dėl tinkamumo ([1]). Principai nedaro poveikio ES valstybėse narėse tvarkant asmens duomenis galiojančio Reglamento (ES) 2016/679 (toliau – Bendrasis duomenų apsaugos reglamentas arba BDAR) ([2]) taikymui. Principais taip pat neribojamos kitais atvejais pagal JAV teisę taikomos su privatumu susijusios prievolės.

2. Kad galėtų pagal ES ir JAV DPS perduoti asmens duomenis iš ES, organizacija privalo vykdyti savarankišką sertifikavimą, kuriuo Departamentui (ar jo paskirtai institucijai) patvirtintų savo įsipareigojimą laikytis Principų. Nors sprendimą dėl dalyvavimo ES ir JAV DPS organizacijos priima visiškai savanoriškai, faktiškai laikytis reikalavimų privaloma: organizacijos, kurios vykdydamos savarankišką sertifikavimą patvirtina Departamentui savo įsipareigojimą laikytis Principų ir viešai apie tai paskelbia, privalo visapusiškai laikytis Principų. Norėdama dalyvauti ES ir JAV DPS, organizacija privalo: a) būti tokia, kurios atžvilgiu gali būti naudojamasi Federalinės prekybos komisijos (FPK), JAV Transporto departamento arba kitos valstybinės įstaigos, kuri veiksmingai užtikrins Principų laikymąsi, tyrimų ir vykdymo užtikrinimo įgaliojimais *(kitos ES pripažįstamos JAV valstybinės įstaigos ateityje gali būti nurodytos priede)*; b) viešai paskelbti savo įsipareigojimą laikytis Principų; c) viešai atskleisti savo privatumo politiką, atitinkančią šiuos Principus; d) visiškai juos įgyvendinti ([3]). Jeigu organizacija nesilaiko Principų, vykdymą užtikrina FPK pagal Federalinės prekybos komisijos (FPK) akto 5 straipsnį, kuriuo draudžiama vykdyti nesąžiningus ar apgaulingus veiksmus prekyboje arba darančius jai poveikį (JAV kodekso 15 antraštinės dalies 45 straipsnis), Transporto departamentas pagal JAV kodekso 49 antraštinės dalies 41712 straipsnį, kuriuo vežėjui arba bilietų pardavėjui draudžiama vykdyti nesąžiningą ar apgaulingą veiklą oro transporto arba oro transporto paslaugų pardavimo srityse, arba pagal kitus įstatymus ar teisės aktus, kuriais draudžiami tokie veiksmai.

([1]) Kadangi Komisijos sprendimas dėl ES ir JAV DPS užtikrinamos apsaugos tinkamumo taikomas Islandijai, Lichtenšteinui ir Norvegijai, ES ir JAV DPS bus taikoma tiek ES, tiek šioms trims valstybėms. Todėl nuorodos į ES ir jos valstybes nares laikomos apimančiomis ir Islandiją, Lichtenšteiną bei Norvegiją.

([2]) 2016 m. balandžio 27 d. EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS (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]) ES ir JAV privatumo skydo sistemos principai iš dalies pakeisti tapo ES ir JAV duomenų privatumo sistemos principais. (Žr. papildomą savarankiško sertifikavimo principą.)

3. Departamentas tvarkys ir viešai skelbs patikimą sąrašą, kuriame bus nurodomos JAV organizacijos, kurios atliko savarankišką sertifikavimą Departamente ir pareiškė, kad įsipareigoja laikytis Principų, (toliau – Duomenų privatumo sistemos sąrašas). ES ir JAV DPS teikiami privalumai užtikrinami nuo dienos, kurią Departamentas įtraukia organizaciją į Duomenų privatumo sistemos sąrašą. Departamentas iš Duomenų privatumo sistemos sąrašo išbrauks organizacijas, kurios savo noru pasitraukia iš ES ir JAV DPS arba neatlieka metinio pakartotinio sertifikavimo Departamente; tokios organizacijos turi toliau taikyti Principus pagal ES ir JAV DPS jų gautai asmeninei informacijai ir kasmet Departamentui patvirtinti savo įsipareigojimą tai daryti (t. y. tol, kol saugo tokią informaciją), kitomis leidžiamomis priemonėmis užtikrinti tinkamą informacijos apsaugą (pvz., sudarydamos sutartį, kuri visiškai atitinka Komisijos patvirtintose atitinkamose standartinėse sutarčių sąlygose nustatytus reikalavimus) arba grąžinti ar ištrinti informaciją. Departamentas iš Duomenų privatumo sistemos sąrašo taip pat išbrauks organizacijas, kurios nuolat nesilaiko Principų; tokios organizacijos privalo grąžinti arba ištrinti pagal ES ir JAV DPS jų gautą asmeninę informaciją. Iš Duomenų privatumo sistemos sąrašo išbraukta organizacija nebeturi teisės remtis Komisijos sprendimu dėl tinkamumo, kad gautų asmeninės informacijos iš ES.

4. Departamentas taip pat tvarkys ir viešai skelbs patikimą registrą, kuriame bus nurodomos JAV organizacijos, kurios anksčiau buvo atlikusios savarankišką sertifikavimą Departamente, bet buvo pašalintos iš Duomenų privatumo sistemos sąrašo. Departamentas aiškiai įspės, kad šios organizacijos nebedalyvauja ES ir JAV DPS; kad išbrauktos iš Duomenų privatumo sistemos sąrašo organizacijos nebegali teigti, kad atitinka ES ir JAV DPS reikalavimus, ir privalo vengti bet kokių pareiškimų arba klaidinančios praktikos, iš kurių būtų galima suprasti, kad jos dalyvauja ES ir JAV DPS; kad tokios organizacijos nebeturi teisės remtis Komisijos sprendimu dėl tinkamumo, kad gautų asmeninės informacijos iš ES. FPK, Transporto departamentas ar kitos vykdymo užtikrinimo institucijos gali imtis vykdymo užtikrinimo veiksmų dėl organizacijos, kuri po to, kai buvo išbraukta iš Duomenų privatumo sistemos sąrašo,, toliau teigia dalyvaujanti ES ir JAV DPS arba kitaip klaidingai pateikia su ES ir JAV DPS susijusius faktus.

5. Šių Principų laikymasis gali būti ribojamas: a) tiek, kiek būtina, kad būtų laikomasi teismo nutarties arba viešojo intereso, teisėsaugos ar nacionalinio saugumo reikalavimų, be kita ko, kai įstatymu ar vyriausybės reglamentu nustatomos prieštaraujančios prievolės; b) pagal įstatymą, teismo nutartį ar vyriausybės reglamentą, kuriais aiškiai duodami leidimai, jeigu naudodamasi tokiu leidimu organizacija gali įrodyti, kad Principų nesilaiko tik tiek, kiek būtina įgyvendinant tokiu leidimu palaikomus viršesnius teisėtus interesus, arba c) jeigu išimtys ar nukrypti leidžiančios nuostatos leidžiamos pagal BDAR jame nustatytomis sąlygomis, su sąlyga, kad tokios išimtys ar nukrypti leidžiančios nuostatos taikomos panašiomis aplinkybėmis. Šiomis aplinkybėmis JAV teisėje numatytos apsaugos priemonės, kuriomis siekiama apsaugoti privatumą ir piliečių laisves, apima apsaugos priemones, kurių reikalaujama pagal Vykdomąjį potvarkį Nr. 14086 ([4]) jame nustatytomis sąlygomis (įskaitant jame nustatytus būtinumo ir proporcingumo reikalavimus). Paisydamos tikslo stiprinti privatumo apsaugą, organizacijos turėtų stengtis visapusiškai ir skaidriai laikytis šių Principų, be kita ko, pasistengti savo privatumo politikos dokumentuose nurodyti, kur taikomos pirmesnio sakinio b punkte nurodytos išimtys. Dėl tos pačios priežasties tikimasi, kad tais atvejais, kai pagal Principus ir (arba) JAV teisę leidžiama pasirinkti kelis variantus, organizacijos, jei įmanoma, rinktųsi didžiausią apsaugą suteikiantį variantą.

6. Organizacijos, tapusios ES ir JAV DPS narėmis, privalo taikyti Principus visiems pagal ES ir JAV DPS perduodamiems asmens duomenims. Organizacija, nusprendusi išplėsti ES ir JAV DPS privalumų taikymą iš ES perduodamai žmogiškųjų išteklių asmeninei informacijai, skirtai naudoti darbo santykių aplinkybėmis, privalo tai nurodyti, kai atlieka savarankišką sertifikavimą Departamente, ir laikytis pagal papildomą savarankiško sertifikavimo principą nustatytų reikalavimų.

([4]) 2022 m. spalio 7 d. Vykdomasis potvarkis dėl Jungtinių Amerikos Valstijų signalų žvalgybos veiklos apsaugos priemonių griežtinimo.

7. Su Principų aiškinimu ir laikymusi, taip pat su atitinkama ES ir JAV DPS dalyvaujančių organizacijų privatumo politika susiję klausimai bus sprendžiami pagal JAV teisę, išskyrus atvejus, kai tokios organizacijos įsipareigojo bendradarbiauti su ES duomenų apsaugos institucijomis (DAI). Jei nenurodyta kitaip, visos Principų nuostatos taikomos pagal paskirtį.

8. Apibrėžtys:

   a. *asmens duomenys* ir *asmeninė informacija* – į BDAR taikymo sritį patenkantys bet kokia forma įrašyti duomenys apie asmenį, kurio tapatybė nustatyta arba gali būti nustatyta, kuriuos organizacija Jungtinėse Amerikos Valstijose gauna iš ES;

   b. asmens duomenų *tvarkymas* – automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, saugojimas, pritaikymas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas ar platinimas, taip pat ištrynimas ar sunaikinimas;

   c. *duomenų valdytojas* – asmuo ar organizacija, kuris (-i) vienas (-a) ar drauge su kitais nustato asmens duomenų tvarkymo tikslus ir priemones.

9. Principai ir jų I priedas įsigalioja nuo Europos Komisijos sprendimo dėl tinkamumo įsigaliojimo datos.

II. **PRINCIPAI**

1. **PRANEŠIMAS**

a. Organizacija privalo informuoti asmenis apie:

   i. tai, kad dalyvauja ES ir JAV DPS, ir pateikti nuorodą į Duomenų privatumo sistemos sąrašą arba to sąrašo interneto svetainės adresą;

   ii. renkamų asmens duomenų rūšis ir, kai tinkama, organizacijos JAV subjektus arba JAV patronuojamąsias įmones, kurie taip pat laikosi Principų;

   iii. savo įsipareigojimą visus asmens duomenis, pagal ES ir JAV DPS gautus iš ES, tvarkyti laikantis Principų;

   iv. tikslus, kuriais renka ir naudoja jų asmeninę informaciją;

   v. tai, kaip organizacijai pateikti užklausas ar skundus, be kita ko, apie bet kokią ES veikiančią susijusią įstaigą, kuri gali atsakyti į tokias užklausas ar skundus;

   vi. trečiųjų šalių, kurioms organizacija atskleidžia asmeninę informaciją, rūšį ar tapatybę, taip pat tokio atskleidimo tikslus;

   vii. asmenų teisę susipažinti su savo asmens duomenimis;

   viii. sprendimus ir priemones, kuriuos organizacija siūlo asmenims, norintiems riboti jų asmens duomenų naudojimą ir atskleidimą;

   ix. nepriklausomą ginčų sprendimo įstaigą, paskirtą nagrinėti skundus ir asmeniui nemokamai teikti tinkamas teisių gynimo galimybes, taip pat apie tai, ar tai yra: 1) DAI sudaryta kolegija, 2) ES įsisteigęs alternatyvaus ginčų sprendimo paslaugų teikėjas arba 3) Jungtinėse Amerikos Valstijose įsisteigęs alternatyvaus ginčų sprendimo paslaugų teikėjas;

   x. tai, ar organizacijai taikomi FPK, Transporto departamento ar bet kurios kitos JAV įgaliotos valstybinės įstaigos tyrimo ir vykdymo užtikrinimo įgaliojimai;

   xi. galimybę tam tikromis sąlygomis asmeniui kreiptis dėl privalomo arbitražo ([5]);

   xii. reikalavimą atskleisti asmeninę informaciją tenkinant teisėtus valdžios institucijų prašymus, be kita ko, siekiant laikytis nacionalinio saugumo arba teisėsaugos reikalavimų;

   xiii. savo atsakomybę toliau perduodant duomenis trečiosioms šalims.

([5]) Žr., pvz., teisių gynimo, vykdymo užtikrinimo ir atsakomybės principo c skirsnį.

b. Toks pranešimas turi būti pateiktas aiškia ir suprantama kalba tada, kai asmenų pirmą kartą prašoma pateikti asmeninę informaciją organizacijai arba kuo greičiau po to, tačiau bet kuriuo atveju prieš organizacijai naudojant tokią informaciją kitu tikslu, nei tas, kuriuo 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 (t. y. atsisakyti sutikti), ar jų asmeninė informacija gali būti: i) atskleista trečiajai šaliai arba ii) naudojama tikslu, kuris iš esmės skiriasi nuo to (tų) tikslo (-ų), kuriuo (-iais) ji buvo iš pradžių surinkta ar vėliau asmenys leido ją naudoti. Asmenims turi būti suteikti aiškūs, suprantami ir lengvai prieinami pasirinkimo mechanizmai.

b. Nukrypstant nuo ankstesnės pastraipos, pasirinkimo galimybės užtikrinti nebūtina, jeigu duomenys atskleidžiami trečiajai šaliai, kuri veikia kaip atstovė, vykdanti užduotį (-is) organizacijos vardu arba pagal jos nurodymus. Tačiau organizacija su tokiu atstovu visada turi sudaryti 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 asmenų sutikimą (pasirinktą sutikimą), jeigu tokią informaciją ketinama i) atskleisti trečiajai šaliai arba ii) naudoti kitu tikslu nei tie, kuriais ji iš pradžių buvo surinkta ar asmenys vėliau leido ją naudoti, pasinaudodami pritarimo galimybe. Be to, organizacija iš trečiosios šalies gautą asmeninę informaciją visada turėtų tvarkyti kaip neskelbtiną, jeigu ta trečioji šalis tą informaciją laiko neskelbtina ir atitinkamai ją tvarko.

3. **ATSKAITOMYBĖ UŽ TOLESNĮ DUOMENŲ PERDAVIMĄ**

a. Norėdamos perduoti asmeninę informaciją trečiajai šaliai, kuri veikia kaip duomenų valdytoja, organizacijos privalo laikytis pranešimo ir pasirinkimo principų. Organizacijos taip pat privalo su trečiąja šalimi duomenų valdytoja sudaryti sutartį, kurioje nustatoma, kad tokie duomenys gali būti tvarkomi tik ribotais ir konkrečiais tikslais, atitinkančiais asmens duoto sutikimo sąlygas, ir kad duomenų gavėjas užtikrins tokį pat apsaugos lygį, koks yra užtikrinamas pagal Principus, ir praneš organizacijai, jeigu nustatys, kad nebegali vykdyti šios prievolės. Sutartyje nurodoma, kad tai nustačius, trečioji šalis duomenų valdytoja nustoja tvarkyti duomenis arba imasi kitų pagrįstų ir tinkamų priemonių padėčiai ištaisyti.

b. Norėdamos perduoti asmens duomenis trečiajai šaliai, kuri veikia kaip atstovė, organizacijos privalo: i) perduoti tokius duomenis tik ribotais ir konkrečiais tikslais; ii) patvirtinti, kad atstovas yra įpareigotas užtikrinti bent tokį pat privatumo apsaugos lygį, kokio reikalaujama pagal Principus; iii) imtis pagrįstų ir tinkamų priemonių, kuriomis būtų užtikrinama, kad atstovas veiksmingai tvarkytų asmeninę informaciją, perduotą laikantis organizacijos įsipareigojimų pagal Principus; iv) reikalauti, kad atstovas, nustatęs, kad nebegali laikytis prievolės užtikrinti tokį pat apsaugos lygį, kokio reikalaujama pagal Principus, apie tai praneštų organizacijai; v) gavusios pranešimą, be kita ko, pagal iv punktą, imtis pagrįstų ir tinkamų priemonių neteisėtam duomenų tvarkymui sustabdyti ir padėčiai ištaisyti; vi) Departamentui paprašius, pateikti Departamentui atitinkamų savo sutarties su tuo atstovu privatumo nuostatų santrauką arba reprezentatyvią kopiją.

4. **SAUGUMAS**

a. Organizacijos, kurios kuria, laiko, naudoja ar platina asmeninę informaciją, deramai atsižvelgdamos į su asmens duomenų tvarkymu susijusią riziką ir tokių duomenų pobūdį, privalo imtis pagrįstų ir tinkamų priemonių duomenims apsaugoti, kad jie nebūtų prarasti, netinkamai naudojami, su jais nebūtų be leidimo susipažįstama, jie nebūtų be leidimo atskleidžiami, keičiami ar sunaikinami.

5. **DUOMENŲ VIENTISUMAS IR TIKSLO APRIBOJIMAS**

a. Pagal Principus asmeninė informacija turi būti tik informacija, atitinkanti tikslus, kuriais yra tvarkoma ([6]). Organizacija negali tvarkyti asmeninės informacijos tokiais būdais, kurie neatitinka tikslų, kuriais ji buvo surinkta ar vėliau asmuo leido ją naudoti. Tiek, kiek būtina dėl tokių tikslų, organizacija privalo imtis pagrįstų priemonių užtikrinti, kad asmens duomenys patikimai atitiktų numatomą jų naudojimo paskirtį, būtų tikslūs, išsamūs ir naujausi. Organizacija privalo laikytis Principų tol, kol saugo tokią informaciją.

b. Tokia forma, iš kurios nustatoma arba gali būti nustatoma asmens tapatybė ([7]), informacija gali būti saugoma tik tol, kol yra reikalinga duomenų tvarkymo tikslu, kaip nurodyta 5 dalies a punkte. Ši prievolė neužkerta kelio organizacijoms tvarkyti asmeninę informaciją ilgiau – tol ir tokiu mastu, kokiu toks tvarkymas pagrįstai padeda siekti archyvavimo dėl viešojo intereso, žurnalistikos, literatūros ir meno, mokslinių ar istorinių tyrimų ir statistinės analizės tikslų. Tokiais atvejais tokiam duomenų tvarkymui taikomi kiti ES ir JAV DPS principai ir nuostatos. Organizacijos turėtų imtis pagrįstų ir tinkamų priemonių, kad laikytųsi šios nuostatos.

6. **SUSIPAŽINIMAS SU DUOMENIMIS**

a. Asmenims turi būti suteikta galimybė susipažinti su organizacijos saugoma asmenine informacija apie juos, tą informaciją ištaisyti, pakeisti ar ištrinti, jei ji netiksli arba tvarkoma pažeidžiant Principus, nebent atitinkamu atveju sudarant galimybę susipažinti su duomenimis patiriama našta ar išlaidos būtų neproporcingos, palyginti su rizika to asmens privatumui, arba būtų pažeistos kitų asmenų teisės.

7. **TEISIŲ GYNIMAS, VYKDYMO UŽTIKRINIMAS IR ATSAKOMYBĖ**

a. Veiksmingai privatumo apsaugai būtini patikimi mechanizmai, kuriais užtikrinamas Principų laikymasis, asmenų, kurie patyrė poveikį dėl Principų nesilaikymo, galimybė ginti teises ir padariniai organizacijai, kai nesilaikoma Principų. Tokie mechanizmai turi atitikti bent šiuos reikalavimus:

i. tai turi būti lengvai prieinami nepriklausomi teisių gynimo mechanizmai, pagal kuriuos laikantis Principų nemokamai būtų tiriami ir operatyviai sprendžiami kiekvieno asmens skundai bei ginčai ir nurodoma atlyginti žalą, jeigu tai numatyta taikomuose teisės aktuose ar pagal privačiojo sektoriaus iniciatyvas;

ii. turi būti nustatytos paskesnės procedūros, skirtos patikrinti, ar organizacijų teiginiai ir pareiškimai apie jų privatumo užtikrinimo praktiką yra teisingi ir ar tokia privatumo užtikrinimo praktika įgyvendinama taip, kaip skelbiama, ypač atsižvelgiant į reikalavimų nesilaikymo atvejus; taip pat

iii. turi būti nustatytos prievolės išspręsti problemas, kylančias dėl to, kad organizacijos nesilaiko Principų, nors nurodo, kad jų laikosi, ir nustatyti padariniai tokioms organizacijoms. Sankcijos turi būti pakankamai griežtos, kad priverstų organizacijas laikytis reikalavimų.

b. Organizacijos ir jų pasirinkti nepriklausomi teisių gynimo mechanizmai greitai reaguos į Departamento užklausas ir prašymus pateikti su ES ir JAV DPS susijusios informacijos. Visos organizacijos privalo operatyviai reaguoti į skundus dėl Principų nesilaikymo, kuriuos ES valstybės narės valdžios institucijos perdavė per Departamentą. Organizacijos, kurios nusprendė bendradarbiauti su DAI, įskaitant žmogiškųjų išteklių duomenis tvarkančias organizacijas, privalo nagrinėjant ir sprendžiant skundus tiesiogiai bendrauti su tokiomis institucijomis.

([6]) Priklausomai nuo aplinkybių, suderinami duomenų tvarkymo tikslai gali būti, pvz., pagrįstai naudingi ryšiams su klientais, dėl reikalavimų laikymosi ir teisinių sumetimų, audito, saugumo ir sukčiavimo prevencijos, organizacijos juridinių teisių išsaugojimo ar gynimo arba kiti tikslai, atitinkantys racionalaus asmens lūkesčius konkrečiomis aplinkybėmis, kuriomis renkami duomenys.

([7]) Tokiais atvejais jeigu, atsižvelgiant į tapatybės nustatymo priemones, kurios, kaip pagrįstai galima tikėtis, veikiausiai bus naudojamos (be kita ko, atsižvelgiant į tapatybės nustatymo sąnaudas ir reikiamą laiką, taip pat į duomenų tvarkymo metu prieinamas technologijas), ir formą, kuria saugomi duomenys, organizacija galėtų pagrįstai nustatyti asmens tapatybę arba tai galėtų padaryti trečioji šalis, jeigu turėtų galimybę susipažinti su duomenimis, laikoma, kad asmens tapatybę galima nustatyti.

c. Jeigu asmuo kreipėsi dėl privalomo arbitražo pateikdamas atitinkamai organizacijai pranešimą, paisydamas procedūrų ir laikydamasis I priede nustatytų sąlygų, organizacijos privalo arbitražo tvarka nagrinėti reikalavimus ir vadovautis I priede nustatytomis sąlygomis.

d. Jeigu duomenys perduodami toliau, sistemoje dalyvaujanti organizacija atsako už asmeninės informacijos, kurią gavo pagal ES ir JAV DPS ir toliau perduoda trečiajai šaliai, kuri jos vardu veikia kaip atstovė, tvarkymą. Sistemoje dalyvaujanti organizacija pagal Principus lieka atsakinga, jeigu jos atstovas tokią asmeninę informaciją tvarko su Principais nesuderinamu būdu, nebent organizacija įrodo, kad nėra atsakinga už įvykį, dėl kurio padaryta žala.

e. Kai organizacijai taikoma dėl reikalavimų nesilaikymo priimta teismo nutartis arba dėl reikalavimų nesilaikymo priimtas Principuose ar būsimame Principų priede nurodytos JAV valstybinės įstaigos (pvz., FPK arba Transporto departamento) nutartis, ta organizacija viešai paskelbia visus atitinkamus su ES ir JAV DPS susijusius visų teismui arba JAV valstybinei įstaigai pateiktų atitikties arba vertinimo ataskaitų skirsnius, kiek tai atitinka konfidencialumo reikalavimus. Departamentas įsteigė specialų DAI kontaktinį centrą, į kurį galima kreiptis dėl visų problemų, susijusių su tuo, kaip sistemoje dalyvaujančios organizacijos laikosi reikalavimų. FPK ir Transporto departamentas pirmumo tvarka nagrinės Departamento ir ES valstybių narių valdžios institucijų perduotus klausimus dėl Principų nesilaikymo ir laiku bei laikydamiesi galiojančių konfidencialumo apribojimų su perduodančiosios valstybės valdžios institucijomis keisis informacija dėl perduotų klausimų.

III. **PAPILDOMI PRINCIPAI**

1. **Neskelbtini duomenys**

a. Nereikalaujama, kad organizacija gautų aiškų sutikimą (pasirinktą sutikimą) dėl neskelbtinų duomenų, jeigu:

i. duomenys tvarkomi dėl duomenų subjektui ar kitam asmeniui gyvybiškai svarbių interesų;

ii. duomenis tvarkyti būtina pareiškiant teisinius reikalavimus ar nustatant gynybos argumentus;

iii. duomenis tvarkyti reikia medicinos priežiūrai atlikti ar diagnozei nustatyti;

iv. duomenys tvarkomi vykdant fondo, asociacijos ar kitos ne pelno organizacijos, užsiimančios politine, filosofine, religine ar profesinių sąjungų veikla, teisėtą veiklą, jeigu tvarkymas susijęs tik su tos organizacijos nariais ar dėl jos tikslų reguliariai su ja ryšį palaikančiais asmenimis ir tokie duomenys be duomenų subjektų sutikimo nėra atskleidžiami trečiajai šaliai;

v. duomenis tvarkyti būtina organizacijos darbo teisės srities įsipareigojimams vykdyti arba

vi. duomenų tvarkymas susijęs su duomenimis, kuriuos asmuo aiškiai paskelbė viešai.

2. **Su žurnalistika susijusios išimtys**

a. Atsižvelgiant į JAV Konstitucijoje nustatytas spaudos laisvės apsaugos priemones, jeigu JAV Konstitucijos Pirmojoje pataisoje įtvirtintos laisvos spaudos teisės prieštarauja privatumo apsaugos interesams, JAV piliečių ir organizacijų veikloje interesai turi būti derinami pagal Pirmąją pataisą.

b. Asmeninei informacijai, kuri yra renkama skelbti, transliuoti ar perduoti kitomis viešo žurnalistinės medžiagos skelbimo formomis, nepriklausomai nuo to, ar yra panaudota, taip pat iš žurnalistikos archyvų platinamai anksčiau paskelbtoje medžiagoje rastai informacijai Principų reikalavimai netaikomi.

3. **Netiesioginė atsakomybė**

a. Interneto ar telekomunikacijų paslaugų teikėjai ir kitos organizacijos pagal Principus nėra atsakingi, jeigu kitos organizacijos vardu informaciją tik perduoda, nukreipia, perjungia ar saugo podėlyje. Pagal ES ir JAV DPS netiesioginės atsakomybės nesukuriama. Jeigu organizacija tik persiunčia trečiųjų šalių perduodamus duomenis ir nenustato tų asmens duomenų tvarkymo tikslų ir priemonių, ji nebūtų laikoma atsakinga.

4. **Išsamus patikrinimas ir auditas**

a. Vykdydami savo veiklą auditoriai ir investicijų bankininkai gali tvarkyti asmens duomenis be asmens sutikimo ar žinios. Tai leidžiama pagal pranešimo, pasirinkimo ir susipažinimo su duomenimis principus toliau aprašytomis aplinkybėmis.

b. Akcinėse bendrovėse ir uždarosiose akcinėse bendrovėse, įskaitant sistemoje dalyvaujančias organizacijas, reguliariai atliekamas auditas. Toks auditas, ypač kai nagrinėjami galimi pažeidimo atvejai, gali būti neveiksmingas, jeigu apie jį bus paskelbta iš anksto. Be to, sistemoje dalyvaujanti organizacija, įraukta į galimo bendrovių susijungimo arba perėmimo procesą, turės atlikti išsamų patikrinimą arba turės būti atliktas toks jos patikrinimas. Tokiais atvejais dažnai bus renkami ir tvarkomi asmens duomenys, pvz., informacija apie aukščiausius vadovus ar kitus svarbias pareigas einančius darbuotojus. Apie tai paskelbus iš anksto, gali būti pakenkta sandoriui ar netgi pažeista taikoma vertybinių popierių reguliavimo tvarka. Atliekant išsamų patikrinimą dalyvaujantys investicijų bankininkai ir advokatai arba auditą atliekantys auditoriai informaciją be asmens žinios gali tvarkyti tik tokiu mastu ir tol, kol tai būtina vykdant teisės aktų ar viešojo intereso reikalavimus ir kitomis aplinkybėmis, kuriomis taikant šiuos Principus būtų pažeisti teisėti organizacijos interesai. Tokie teisėti interesai, be kita ko, yra organizacijų teisinių prievolių vykdymo ir teisėtos apskaitos tvarkymo veiklos stebėsena ir būtinybė užtikrinti konfidencialumą, susiję su galimu įmonių įsigijimu, susijungimu, bendromis įmonėmis ar kitais panašiais investicijų bankininkų ir auditorių vykdomais sandoriais.

5. **Duomenų apsaugos institucijų vaidmuo**

a. Organizacijos vykdys savo įsipareigojimą bendradarbiauti su DAI, kaip aprašyta toliau. Pagal ES ir JAV DPS JAV organizacijos, gaunančios asmens duomenis iš ES, privalo įsipareigoti taikyti veiksmingus mechanizmus, kuriais užtikrinama, kad būtų laikomasi Principų. Konkrečiau, kaip nustatyta pagal teisių gynimo, vykdymo užtikrinimo ir atsakomybės principą, sistemoje dalyvaujančios organizacijos privalo: a) i) asmenims, su kuriais susiję duomenys, suteikti teisių gynimo priemonių; a) ii) nustatyti paskesnes procedūras, skirtas patikrinti, ar įmonių teiginiai ir pareiškimai apie jų taikomą privatumo užtikrinimo praktiką yra teisingi; a) iii) įsipareigoti spręsti problemas, kylančias dėl Principų nesilaikymo, ir nustatyti padarinius tokioms organizacijoms. Organizacija gali atitikti teisių gynimo, vykdymo užtikrinimo ir atsakomybės principo a punkto i ir iii papunkčiuose nustatytus reikalavimus, jeigu laikosi šiame skirsnyje nustatytų bendradarbiavimo su DAI reikalavimų.

b. Organizacija įsipareigoja bendradarbiauti su DAI Departamentui teikiamuose ES ir JAV DPS savarankiško sertifikavimo dokumentuose nurodydama (žr. papildomą savarankiško sertifikavimo principą), kad:

i. nusprendė laikytis teisių gynimo, vykdymo užtikrinimo ir atsakomybės principo a punkto i ir iii papunkčiuose nustatytų reikalavimų įsipareigodama bendradarbiauti su DAI;

ii. bendradarbiaus su DAI tiriant ir sprendžiant pagal Principus pateiktus skundus, taip pat

iii. laikysis visų DAI teikiamų rekomendacijų, kai, DAI manymu, organizacija turi imtis tam tikrų veiksmų, kad atitiktų Principus, įskaitant teisių gynimo ar kompensacines priemones, skirtas asmenims, patyrusiems poveikį dėl bet kokio Principų nesilaikymo, ir raštu DAI patvirtins, kad tokių veiksmų imtasi.

c. DAI kolegijų veikla

i. DAI bendradarbiaudamos teiks informaciją ir rekomendacijas tokiais būdais:

1. DAI rekomendacijos bus teikiamos per ES lygiu įkurtą neformalią DAI kolegiją, kuri, *inter alia*, padės užtikrinti darnų ir nuoseklų požiūrį;

2. ši kolegija teiks rekomendacijas atitinkamoms JAV organizacijoms dėl neišspręstų asmenų skundų dėl iš ES pagal ES ir JAV DPS perduotos asmeninės informacijos tvarkymo. Tokiomis rekomendacijomis bus siekiama užtikrinti, kad Principai būtų taikomi teisingai ir atitinkamam (-iems) asmeniui (-ims) būtų suteikiama teisių gynimo priemonių, kurias DAI laiko tinkamomis;

3. kolegija teiks tokias rekomendacijas reaguodama į atitinkamų organizacijų perduotus ir (arba) tiesiogiai iš asmenų gautus skundus dėl organizacijų, kurios ES ir JAV DPS tikslais įsipareigojo bendradarbiauti su DAI, ir kartu skatins ir, jei reikia, padės tokiems asmenims iš pradžių pasinaudoti vidinėmis skundų nagrinėjimo procedūromis, kurias gali pasiūlyti organizacija;

4. rekomendacijos bus skelbiamos tik po to, kai abiem ginčo šalims buvo suteikta pagrįsta galimybė pateikti pastabų ir visus pageidaujamus įrodymus. Kolegija stengsis rekomendacijas pateikti kuo greičiau, kiek įmanoma laikantis tinkamo proceso reikalavimų. Paprastai kolegija stengsis rekomendaciją pateikti per 60 dienų nuo skundo ar perduoto klausimo gavimo dienos, o jei įmanoma – greičiau;

5. kolegija viešai skelbs jai pateiktų skundų svarstymo rezultatus, jei manys, kad tai tikslinga;

6. kolegijos pateiktos rekomendacijos neužtraukia atsakomybės kolegijai ar pavienėms DAI.

ii. Kaip pažymėta pirmiau, šį ginčų sprendimo būdą pasirinkusios organizacijos privalo įsipareigoti laikytis DAI rekomendacijų. Jeigu organizacija per 25 dienas po rekomendacijų pateikimo jų neįvykdo ir nepateikia patenkinamo paaiškinimo dėl vėlavimo, kolegija praneš apie savo ketinimus šį klausimą perduoti FPK, Transporto departamentui ar kitai JAV federalinei ar valstijos įstaigai, kuriai įstatymais suteikti įgaliojimai imtis vykdymo užtikrinimo veiksmų apgaulės arba klaidinimo atvejais, arba priimti sprendimą, kad dėl rimtų bendradarbiavimo susitarimo pažeidimų susitarimas turi būti pripažintas niekiniu. Pastaruoju atveju kolegija informuos Departamentą, kad Duomenų privatumo sistemos sąrašas gali būti atitinkamai pakoreguotas. Už įsipareigojimo bendradarbiauti su DAI nevykdymą ir Principų nesilaikymą bus taikomos sankcijos kaip už apgaulingą veiklą pagal FPK akto 5 straipsnį (JAV kodekso 15 antraštinės dalies 45 straipsnį), JAV kodekso 49 antraštinės dalies 41712 straipsnį ar panašų įstatymą.

d. Organizacija, norinti, kad jai ES ir JAV DPS teikiami privalumai būtų taikomi ir darbo santykių aplinkybėmis iš ES perduodamiems žmogiškųjų išteklių duomenims, privalo įsipareigoti bendradarbiauti su DAI dėl tokių duomenų (žr. papildomą žmogiškųjų išteklių duomenų principą).

e. Šią galimybę pasirinkusios organizacijos turės mokėti metinį mokestį, kuris bus skirtas kolegijos veiklos išlaidoms padengti. Be to, jų gali būti paprašyta padengti visas būtinas vertimo išlaidas, patiriamas kolegijai nagrinėjant jai perduotus klausimus ar skundus. Mokesčio dydį nustatys Departamentas, pasikonsultavęs su Komisija. Mokestį gali rinkti trečioji šalis, kurią Departamentas pasirinks kaip šiam tikslui surinktų lėšų saugotoją. Departamentas glaudžiai bendradarbiaus su Komisija ir DAI, kad būtų nustatyta tinkama iš mokesčio surinktų lėšų paskirstymo tvarka, taip pat dėl kitų procedūrinių ir administracinių kolegijos veiklos aspektų. Departamentas ir Komisija gali susitarti pakeisti mokesčio rinkimo dažnumą.

6. **Savarankiškas sertifikavimas**

a. ES ir JAV DPS teikiami privalumai užtikrinami nuo tos dienos, kurią Departamentas įrašo organizaciją į Duomenų privatumo sistemos sąrašą. Departamentas organizaciją į Duomenų privatumo sistemos sąrašą įrašys tik nustatęs, kad organizacijos pradinio savarankiško sertifikavimo dokumentai yra išsamūs, ir išbrauks organizaciją iš to sąrašo, jeigu ji savo noru pasitrauks iš sistemos, neatliks metinio pakartotinio sertifikavimo arba jeigu ji nuolat nesilaiko Principų (žr. papildomą ginčų sprendimo ir vykdymo užtikrinimo principą).

b. Kad galėtų iš pradžių atlikti savarankišką sertifikavimą arba vėliau atlikti pakartotinį sertifikavimą dėl ES ir JAV DPS, organizacija turi kiekvieną kartą Departamentui pateikti organizacijos, kuri atitinkamai vykdydama savarankišką sertifikavimą arba pakartotinį sertifikavimą patvirtina, kad laikosi Principų, vardu vadovaujančio pareigūno parengtus dokumentus ([8]), kuriuose pateikiama bent ši informacija:

([8]) Dokumentus Departamento Duomenų privatumo sistemos interneto svetainėje turi pateikti organizacijoje dirbantis asmuo, įgaliotas organizacijos ir visų jos įtrauktų subjektų vardu teikti pareiškimus dėl Principų laikymosi.

i. savarankišką sertifikavimą arba pakartotinį sertifikavimą atliekančios JAV organizacijos pavadinimas, taip pat visų jos JAV subjektų arba JAV patronuojamųjų įmonių, kurie taip pat laikosi Principų ir kuriuos organizacija nori įtraukti, pavadinimai;

ii. organizacijos veiklos, susijusios su asmenine informacija, kuri būtų gaunama iš ES pagal ES ir JAV DPS, aprašymas;

iii. su tokia asmenine informacija susijusios atitinkamos organizacijos privatumo politikos aprašymas, įskaitant:

1. jeigu organizacija turi viešą interneto svetainę, – atitinkamą svetainės adresą, kuriuo skelbiama privatumo politika, arba, jeigu organizacija viešos interneto svetainės neturi, – vietą, kur visuomenė gali susipažinti su privatumo politika, taip pat

2. jos faktinio įgyvendinimo pradžios datą;

iv. organizacijoje veikianti kontaktinė tarnyba, kuri nagrinėja skundus, prašymus leisti susipažinti su duomenimis ir visus kitus dėl Principų kylančius klausimus ([9]), įskaitant:

1. atitinkamo (-ų) asmens (-ų) arba atitinkamos (-ų) kontaktinės (-ių) tarnybos (-ų) atstovo (-ų) vardą (-us), pavardę (-es), pareigas (jei taikoma), e. pašto adresą (-us) ir telefono numerį (-ius), taip pat

2. atitinkamą organizacijos JAV pašto adresą;

v. konkreti valstybinė įstaiga, turinti jurisdikciją nagrinėti visus skundus dėl organizacijos galimos nesąžiningos ar apgaulingos veiklos ir privatumo klausimus reglamentuojančių įstatymų ar teisės aktų pažeidimų (kuri yra įtraukta į Principų sąrašą arba būsimą Principų priedą);

vi. privatumo užtikrinimo programos, kurioje dalyvauja organizacija, pavadinimas;

vii. tikrinimo metodas (t. y. įsivertinimas arba išorinės reikalavimų laikymosi peržiūros, įskaitant tokias peržiūras atliekančią trečiąją šalį) ([10]), taip pat

viii. atitinkamas (-i) nepriklausomas (-i) teisių gynimo mechanizmas (-ai) su Principais susijusiems neišspręstiems skundams tirti ([11]).

c. Jeigu organizacija nori, kad jai ES ir JAV DPS teikiami privalumai būtų taikomi ir iš ES perduodamai žmogiškųjų išteklių informacijai, skirtai naudoti darbo santykių aplinkybėmis, ji gali tai daryti, jeigu Principų sąraše arba būsimame Principų priede nurodyta valstybinė įstaiga turi jurisdikciją nagrinėti organizacijai pareikštus reikalavimus dėl žmogiškųjų išteklių informacijos tvarkymo. Be to, organizacija privalo tai nurodyti savo pradinio savarankiško sertifikavimo dokumentuose, taip pat visuose pakartotinio sertifikavimo dokumentuose ir paskelbti savo įsipareigojimą bendradarbiauti su atitinkama (-omis) ES valdžios institucija (-omis) pagal papildomus žmogiškųjų išteklių duomenų ir duomenų apsaugos institucijų vaidmens principus (kaip taikoma) ir patvirtinti, kad laikysis tokių valdžios institucijų pateiktų rekomendacijų. Organizacija taip pat privalo pateikti Departamentui savo žmogiškųjų išteklių privatumo politikos kopiją ir informaciją, kur su privatumo politika gali susipažinti poveikį patyrę jos darbuotojai.

([9]) Pagrindinis organizacijos kontaktinis asmuo arba organizacijos vadovaujantis pareigūnas negali būti organizacijai nepriklausantis atstovas (pvz., išorės patarėjas ar išorės konsultantas).

([10]) Žr. papildomą patikrinimo principą.

([11]) Žr. papildomą ginčų sprendimo ir vykdymo užtikrinimo principą.

d. Departamentas tvarkys ir viešai skelbs Duomenų privatumo sistemos sąrašą, kuriame bus nurodomos organizacijos, pateikusios išsamius pradinio savarankiško sertifikavimo dokumentus, ir tą sąrašą atnaujins remdamasis išsamiais metinio pakartotinio sertifikavimo dokumentais, taip pat pagal papildomą ginčų sprendimo ir vykdymo užtikrinimo principą gautais pranešimais. Tokie pakartotinio sertifikavimo dokumentai turi būti teikiami ne rečiau kaip kartą per metus, antraip organizacija bus išbraukta iš Duomenų privatumo sistemos sąrašo ir nebegalės naudotis ES ir JAV DPS teikiamais privalumais. Visos į Duomenų privatumo sistemos sąrašą Departamento įtrauktos organizacijos privalo įdiegti atitinkamą privatumo politiką, kuri atitiktų pranešimo principą, ir tos privatumo politikos dokumentuose nurodyti, kad laikosi Principų ([12]). Jeigu organizacijos privatumo politika skelbiama internete, būtina pateikti saitą į Departamento Duomenų privatumo sistemos interneto svetainę, taip pat saitą į nepriklausomo teisių gynimo mechanizmo, kuris gali būti naudojamas su Principais susijusiems neišspręstiems skundams nemokamai nagrinėti, interneto svetainę arba skundo pateikimo formą.

e. Principai taikomi iš karto nuo savarankiško sertifikavimo momento. Sistemoje dalyvaujančios organizacijos, kurios anksčiau buvo atlikusios savarankišką sertifikavimą pagal ES ir JAV privatumo skydo sistemos principus, turės atnaujinti savo privatumo politiką, kad joje būtų nurodomi ES ir JAV duomenų privatumo sistemos principai. Tokios organizacijos šią nuorodą turi įtraukti kuo greičiau ir bet kuriuo atveju ne vėliau kaip per tris mėnesius nuo ES ir JAV duomenų privatumo sistemos principų įsigaliojimo dienos.

f. Organizacija privalo visus asmens duomenis, pagal ES ir JAV DPS gautus iš ES, tvarkyti pagal Principus. Įsipareigojimas laikytis Principų dėl asmens duomenų, gautų per laikotarpį, kurį organizacija naudojosi ES ir JAV DPS teikiamais privalumais, galioja neterminuotai; toks įsipareigojimas reiškia, kad organizacija tokiems duomenims ir toliau taikys Principus tol, kol saugo, naudoja ar atskleidžia tokius duomenis, net jei dėl bet kurios priežasties pasitraukia iš ES ir JAV DPS. Organizacija, norinti pasitraukti iš ES ir JAV DPS, apie tai turi iš anksto pranešti Departamentui. Tokiame pranešime taip pat turi būti nurodyta, ką organizacija darys su asmens duomenimis, kuriuos gavo pagal ES ir JAV DPS (t. y. duomenis išsaugos, grąžins ar ištrins, o jei išsaugos, kokiomis leidžiamomis priemonėmis užtikrins tų duomenų apsaugą). Iš ES ir JAV DPS pasitraukusi organizacija, kuri nori išsaugoti tokius duomenis, privalo kasmet Departamentui patvirtinti savo įsipareigojimą toliau duomenims taikyti Principus arba kitomis leidžiamomis priemonėmis (pvz., sudarydama sutartį, kuri visiškai atitinka Komisijos patvirtintose atitinkamose standartinėse sutarčių sąlygose nustatytus reikalavimus) užtikrinti „tinkamą“ duomenų apsaugą; priešingu atveju organizacija privalo informaciją grąžinti arba ištrinti ([13]). Pasitraukusi iš ES ir JAV DPS, organizacija privalo iš visų susijusių privatumo politikos dokumentų pašalinti bet kokias nuorodas į ES ir JAV DPS, iš kurių galima suprasti, kad organizacija toliau dalyvauja ES ir JAV DPS ir turi teisę naudotis jos teikiamais privalumais.

([12]) Pirmą kartą savarankišką sertifikavimą atliekanti organizacija galutiniuose privatumo politikos dokumentuose negali nurodyti, kad dalyvauja ES ir JAV DPS, kol gaus Departamento pranešimą, kad gali tai daryti. Teikdama pradinio savarankiško sertifikavimo dokumentus, organizacija turi Departamentui pateikti Principus atitinkantį privatumo politikos projektą. Nustatęs, kad organizacijos pradinio savarankiško sertifikavimo dokumentai apskritai yra išsamūs, Departamentas praneš organizacijai, kad ji turėtų baigti rengti (pvz., atitinkamais atvejais paskelbti) ES ir JAV DPS atitinkančią savo privatumo politiką. Baigusi rengti atitinkamą privatumo politiką, organizacija turi nedelsdama apie tai pranešti Departamentui, o Departamentas tada įtraukia organizaciją į Duomenų privatumo sistemos sąrašą.

([13]) Jeigu pasitraukdama iš sistemos organizacija renkasi išsaugoti asmens duomenis, kuriuos gavo pagal ES ir JAV DPS, ir kasmet Departamentui patvirtina, kad tokiems duomenims toliau taiko Principus, ta organizacija kartą per metus po pasitraukimo privalo Departamentui patvirtinti (t. y. išskyrus atvejus, kai organizacija užtikrina „tinkamą“ tokių duomenų apsaugą kitomis leidžiamomis priemonėmis ir tol, kol ji tai daro, arba grąžina ar ištrina visus tokius duomenis ir praneša Departamentui apie šį veiksmą), ką ji padarė su tais asmens duomenimis, ką ji darys su išsaugotais asmens duomenimis ir kas veiks kaip nuolatinis kontaktinis centras su Principais susijusiais klausimais.

g. Organizacija, kuri pasikeitus įmonės statusui, pvz., dėl susijungimo, perėmimo, bankroto ar likvidavimo, nustos egzistuoti kaip atskiras juridinis asmuo, privalo apie tai iš anksto pranešti Departamentui. Pranešime taip pat turėtų būti nurodyta, ar įmonės statusui pasikeitus atsiradęs subjektas i) toliau dalyvaus ES ir JAV DPS remdamasis esamu savarankišku sertifikavimu; ii) atliks savarankišką sertifikavimą kaip naujas ES ir JAV DPS dalyvis (pvz., kai naujas subjektas arba išlikęs subjektas dar nėra atlikęs savarankiško sertifikavimo, kuriuo remdamasis galėtų dalyvauti ES ir JAV DPS), arba iii) įdiegs kitas apsaugos priemones, pvz., rašytinį susitarimą, kuriuo bus užtikrinama, kad Principai ir toliau būtų taikomi visiems asmens duomenims, kuriuos organizacija gavo pagal ES ir JAV DPS ir išsaugos. Jeigu netaikomas nei i, nei ii, nei iii punktas, pagal ES ir JAV DPS gauti asmens duomenys turi būti nedelsiant grąžinti arba ištrinti.

h. Dėl bet kokių priežasčių pasitraukusi iš ES ir JAV DPS, organizacija privalo pašalinti visus pareiškimus, iš kurių galima suprasti, kad organizacija ir toliau dalyvauja ES ir JAV DPS arba turi teisę naudotis ES ir JAV DPS teikiamais privalumais. Jeigu naudojamas, ES ir JAV DPS sertifikavimo ženklas taip pat turi būti pašalintas. Už bet kokį visuomenės klaidinimą dėl organizacijos įsipareigojimo laikytis Principų FPK, Transporto departamentas ar kita atitinkama valdžios institucija gali taikyti sankcijas. Už klaidingą faktų pateikimą Departamentui gali būti taikomos sankcijos pagal Melagingų parodymų aktą (JAV kodekso 18 antraštinės dalies 1001 straipsnį).

7. **Patikrinimas**

a. Organizacijos privalo nustatyti paskesnes procedūras, skirtas patikrinti, ar jų teiginiai ir pareiškimai apie jų ES ir JAV DPS privatumo užtikrinimo praktiką yra teisingi ir ar ta privatumo užtikrinimo praktika įgyvendinama taip, kaip nurodoma, ir atitinka Principus.

b. Siekdama laikytis teisių gynimo, vykdymo užtikrinimo ir atsakomybės principo reikalavimų dėl tikrinimo, organizacija privalo tikrinti tokius teiginius ir pareiškimus atlikdama įsivertinimą arba išorinę reikalavimų laikymosi peržiūrą.

c. Jeigu organizacija pasirinko įsivertinimą, tokiu patikrinimu turi būti įrodyta, kad su iš ES gaunama asmenine informacija susijusi jos privatumo politika yra tiksli, išsami, lengvai prieinama, atitinka Principus ir yra visapusiškai įgyvendinama (t. y. jos laikomasi). Iš jo taip pat turi būti matyti, kad asmenys yra informuojami apie visas vidines skundų nagrinėjimo procedūras ir apie nepriklausomą (-us) teisių gynimo mechanizmą (-us), kuriuo (-iais) gali pasinaudoti teikdami skundus; kad yra parengta darbuotojų mokymo, kaip įgyvendinti politiką, tvarka ir drausminimo priemonės, kai tos politikos nesilaikoma; kad yra parengta vidaus tvarka, pagal kurią periodiškai objektyviai peržiūrima, kaip laikomasi nurodytų reikalavimų. Bent kartą per metus vadovaujantis pareigūnas ar kitas įgaliotas organizacijos atstovas privalo pasirašyti pareiškimą, kuriame patvirtinama, kad įsivertinimas atliktas; toks pareiškimas turi būti pateikiamas asmenų prašymu, atliekant tyrimą arba gavus skundą dėl reikalavimų nesilaikymo.

d. Jeigu organizacija pasirinko išorinę reikalavimų laikymosi peržiūrą, tokiu patikrinimu turi būti įrodyta, kad su iš ES gaunama asmenine informacija susijusi jos privatumo politika yra tiksli, išsami, lengvai prieinama, atitinka Principus ir yra visapusiškai įgyvendinama (t. y. jos laikomasi). Iš jo taip pat turi būti matyti, kad asmenys yra informuojami apie mechanizmą (-us), kuriuo (-iais) gali pasinaudoti teikdami skundus. Peržiūros gali būti atliekamos, be kita ko, tokiais būdais: prireikus vykdant auditą, rengiant atsitiktines peržiūras, taikant „spąstų“ metodą arba naudojant technologines priemones. Bent kartą per metus tikrintojas, vadovaujantis pareigūnas ar kitas įgaliotas organizacijos atstovas privalo pasirašyti pareiškimą, kuriame patvirtinama, kad išorinė reikalavimų laikymosi peržiūra atlikta; toks pareiškimas turi būti pateikiamas asmenų prašymu, atliekant tyrimą arba gavus skundą dėl reikalavimų nesilaikymo.

e. Organizacijos privalo tvarkyti savo ES ir JAV DPS privatumo užtikrinimo praktikos įgyvendinimo registrus ir pateikti juos už skundų nagrinėjimą atsakingai nepriklausomai ginčų sprendimo įstaigai arba agentūrai, kurios jurisdikcijai priklauso tirti nesąžiningą ir apgaulingą veiklą, kai to prašoma vykdant tyrimą ar gavus skundą dėl reikalavimų nesilaikymo. Organizacijos taip pat privalo greitai atsakyti į Departamento užklausas ir kitus prašymus pateikti informacijos, susijusios su tuo, kaip organizacija laikosi Principų.

8. **Susipažinimas su duomenimis**

a. Susipažinimo su duomenimis principo taikymas praktikoje

i. Pagal Principus teisė susipažinti su duomenimis yra esminis privatumo apsaugos aspektas. Visų pirma taip asmenys gali patikrinti, ar saugoma informacija apie juos yra tiksli. Pagal susipažinimo su duomenimis principą asmenys turi teisę:

1. gauti organizacijos patvirtinimą, ar ji tvarko su jais susijusius asmens duomenis ([14]);

2. gauti tokius duomenis, kad galėtų patikrinti, ar jie tikslūs ir tvarkomi teisėtai, taip pat

3. nurodyti ištaisyti, pakeisti arba ištrinti duomenis, jeigu jie netikslūs arba tvarkomi pažeidžiant Principus.

ii. Asmenys neprivalo pagrįsti prašymų leisti susipažinti su savo asmens duomenimis. Atsakydamos į asmenų prašymus leisti susipažinti su duomenimis, organizacijos pirmiausia turėtų įvertinti, dėl kokios (-ių) priežasties (-ių) tokie prašymai buvo pateikti. Pavyzdžiui, jei prašymas leisti susipažinti su duomenimis yra neaiškus ar didelės apimties, organizacija gali tai aptarti su asmeniu, kad geriau suprastų prašymo motyvus ir nustatytų pageidaujamą informaciją. Organizacija gali pasiteirauti, su kuriuo (-iais) organizacijos padaliniu (-iais) asmuo bendravo, arba apie informacijos, su kuria prašoma leisti susipažinti, pobūdį ar panaudojimą.

iii. Kadangi galimybė susipažinti su duomenimis yra esminė, organizacijos visada turėtų sąžiningai stengtis suteikti galimybę susipažinti su duomenimis. Pavyzdžiui, kai tam tikrą informaciją reikia apsaugoti ir ją galima lengvai atskirti nuo kitos asmeninės informacijos, su kuria prašoma leisti susipažinti, organizacija turėtų atskirti saugomą informaciją ir pateikti kitą informaciją. Jeigu organizacija nusprendžia, kad tam tikru konkrečiu atveju galimybė susipažinti su duomenimis turėtų būti ribojama, ji turėtų prašymą leisti susipažinti su duomenimis pateikusiam asmeniui paaiškinti tokio sprendimo priežastį ir nurodyti kontaktinį centrą, kuriam galima teikti paskesnes užklausas.

b. Galimybės susipažinti su duomenimis suteikimo našta arba išlaidos

i. Teisė susipažinti su asmens duomenimis gali būti ribojama išimtinėmis aplinkybėmis, kai būtų pažeistos teisėtos kitų asmenų teisės arba kai suteikiant galimybę susipažinti su duomenimis patiriama našta ar išlaidos atitinkamu atveju būtų neproporcingos, palyginti su rizika to asmens privatumui. Išlaidos ir našta yra svarbūs veiksniai ir į juos reikėtų atsižvelgti, tačiau jie nėra lemiami nustatant, ar suteikti galimybę susipažinti su duomenimis yra pagrįsta.

ii. Pavyzdžiui, jeigu asmeninė informacija naudojama priimant sprendimus, kurie asmeniui turės reikšmingą poveikį (pvz., dėl to būtų atsisakyta suteikti arba suteikta reikšmingos naudos, pvz., susijusios su draudimu, hipoteka ar darbu), organizacija, laikydamasi kitų šių papildomų principų nuostatų, turėtų atskleisti informaciją net jei ją pateikti gana sunku ar brangu. Jeigu prašoma asmeninė informacija nėra neskelbtina arba nėra naudojama priimant sprendimus, kurie asmeniui turės reikšmingą poveikį, tačiau yra lengvai prieinama ir ją pateikti nebrangu, organizacija turėtų suteikti galimybę susipažinti su tokia informacija.

c. Konfidenciali komercinė informacija

i. Konfidenciali komercinė informacija – informacija, kurią organizacija stengiasi apsaugoti, kad ji nebūtų atskleista, jeigu jos atskleidimas padėtų rinkos konkurentams. Organizacijos gali nesuteikti galimybės susipažinti su informacija arba apriboti tokią galimybę tiek, kiek suteikus galimybę susipažinti su visa informacija būtų atskleista jos pačios konfidenciali komercinė informacija, pvz., organizacijos padarytos rinkodaros išvados ar sudarytos klasifikacijos, arba kitų organizacijų konfidenciali komercinė informacija, kuriai taikomi sutartiniai įsipareigojimai dėl konfidencialumo.

([14]) Organizacija turėtų atsakyti į asmens prašymus nurodyti duomenų tvarkymo tikslus, atitinkamų asmens duomenų kategorijas ir gavėjus, kuriems atskleidžiami asmens duomenys, arba tokių gavėjų kategorijas.

ii. Jeigu konfidencialią komercinę informaciją galima lengvai atskirti nuo kitos asmeninės informacijos, su kuria prašoma leisti susipažinti, organizacija turėtų atskirti konfidencialią komercinę informaciją ir pateikti nekonfidencialią informaciją.

d. Duomenų bazių organizavimas

i. Galimybę susipažinti su duomenimis organizacija gali suteikti asmeniui atskleisdama susijusią asmeninę informaciją; tam asmeniui nebūtina prieiga prie organizacijos duomenų bazės.

ii. Prieiga turi būti suteikiama tik tokiu mastu, kokiu organizacija saugo asmeninę informaciją. Pačiu susipažinimo su duomenimis principu prievolė išsaugoti, tvarkyti, pertvarkyti ar restruktūrizuoti asmeninės informacijos bylas nenustatoma.

e. Galimi susipažinimo su duomenimis ribojimo atvejai

i. Kadangi organizacijos visada privalo sąžiningai stengtis suteikti asmenims galimybę susipažinti su jų asmens duomenimis, aplinkybių, kuriomis organizacijos gali riboti tokią galimybę, yra nedaug, o galimybė susipažinti su duomenimis gali būti ribojama tik dėl konkrečių priežasčių. Kaip nustatyta BDAR, organizacija galimybes susipažinti su informacija gali riboti tiek, kiek ją atskleidus veikiausiai kiltų sunkumų apsaugoti svarbius priešingus viešuosius interesus, pvz., nacionalinio saugumo, gynybos arba visuomenės saugumo. Be to, jeigu asmeninė informacija tvarkoma vien tyrimų ar statistikos tikslais, galimybės susipažinti su informacija galima nesuteikti. Galimybė susipažinti su duomenimis gali būti nesuteikiama arba ribojama ir dėl šių priežasčių:

1. tai trukdytų vykdyti teisės aktus ar užtikrinti jų vykdymą arba nagrinėti privačias bylas, be kita ko, užkirsti kelią pažeidimams, juos tirti ar nustatyti arba naudotis teise į teisingą bylos nagrinėjimą;

2. atskleidus informaciją būtų pažeistos kitų asmenų teisėtos teisės arba svarbūs interesai;

3. būtų pažeista teisinė ar kitokia teisė ar įsipareigojimas neatskleisti profesinės paslapties;

4. būtų pakenkta su darbuotojų saugumu susijusiems tyrimams arba skundų teikimo procedūrai, arba su personalo planavimu ir įmonių reorganizavimu susijusiems dalykams, arba

5. būtų pažeistas konfidencialumas, būtinas su patikimu valdymu susijusioms stebėsenos, priežiūros ar kontrolės funkcijoms arba vyksiančiose ar vykstančiose derybose, kuriose dalyvauja organizacija.

ii. Išimtį taikyti siekiančiai organizacijai tenka pareiga įrodyti jos būtinybę, taip pat asmenims turi būti nurodytos galimybių susipažinti su duomenimis ribojimo priežastys ir kontaktinis centras, kuriam galima teikti paskesnes užklausas.

f. Teisė gauti patvirtinimą ir mokestis galimybės susipažinti su duomenimis suteikimo išlaidoms kompensuoti

i. Asmuo turi teisę gauti patvirtinimą, ar ši organizacija turi su juo susijusių asmens duomenų. Asmuo taip pat turi teisę gauti su juo susijusius asmens duomenis. Organizacija už tai gali imti ne pernelyg didelį mokestį.

ii. Mokesčio ėmimas gali būti pagrįstas, pvz., kai prašymai leisti susipažinti su duomenimis yra akivaizdžiai pertekliniai, visų pirma dėl to, kad yra kartotiniai.

iii. Negalima neleisti susipažinti su duomenimis dėl su išlaidomis susijusių priežasčių, jeigu asmuo pasisiūlo apmokėti išlaidas.

g. Kartotiniai arba nepagrįsti prašymai leisti susipažinti su duomenimis

i. Organizacija gali nustatyti pagrįstas ribas, kiek kartų per tam tikrą laikotarpį patenkins konkretaus asmens prašymus leisti susipažinti su duomenimis. Nustatydama tokius apribojimus, organizacija turėtų atsižvelgti į tokius veiksnius kaip informacijos atnaujinimo dažnumą, duomenų naudojimo paskirtį ir informacijos pobūdį.

h. Apgaulingi prašymai leisti susipažinti su duomenimis

i. Organizacija neprivalo leisti susipažinti su duomenimis, jeigu jai pateikiama nepakankamai informacijos, kad ji galėtų patvirtinti prašymą pateikusio asmens tapatybę.

i. Atsakymų pateikimo terminas

i. Organizacijos į prašymus leisti susipažinti su informacija turėtų atsakyti per pagrįstą terminą, pagrįstu būdu ir asmeniui suprantama forma. Organizacija, kuri informaciją duomenų subjektams teikia reguliariai, asmens prašymą leisti susipažinti su duomenimis gali patenkinti, kai reguliariai atskleis duomenis, jeigu tai įvyks ne pernelyg vėlai.

9. **Žmogiškųjų išteklių duomenys**

a. ES ir JAV DPS taikymas

i. Jeigu ES veikianti organizacija savo darbuotojų (buvusių ar esamų) asmeninę informaciją, kuri buvo surinkta darbo santykių aplinkybėmis, perduoda ES ir JAV DPS dalyvaujančiai patronuojančiajai bendrovei, asocijuotajai įmonei ar neasocijuotam paslaugų teikėjui Jungtinėse Amerikos Valstijose, tokiems duomenims taikomi ES ir JAV DPS suteikiami privalumai. Tokiais atvejais informacija prieš perduodant renkama ir tvarkoma laikantis tos ES valstybės narės, kurioje buvo surinkta, nacionalinės teisės aktų, taigi reikės laikytis visų tuose teisės aktuose numatytų jos perdavimo sąlygų ar apribojimų.

ii. Principai galioja tik kai perduodami įrašai, iš kurių nustatoma arba gali būti nustatyta asmens tapatybė, arba kai susipažįstama su tokiais įrašais. Dėl statistinių ataskaitų, kurios grindžiamos apibendrintais įdarbinimo duomenimis ir kuriuose nėra asmens duomenų arba naudojami nuasmeninti duomenys, su privatumu susijusių klausimų nekyla.

b. Pranešimo ir pasirinkimo principų taikymas

i. JAV organizacija, pagal ES ir JAV DPS iš ES gavusi informacijos apie darbuotojus, gali ją atskleisti trečiosioms šalims arba naudoti įvairiems tikslams tik laikydamasi pranešimo ir pasirinkimo principų. Pavyzdžiui, jeigu organizacija ketina darbo santykių metu surinktą asmeninę informaciją naudoti su darbu nesusijusiais tikslais, pvz., rinkodaros pranešimuose, JAV organizacija prieš tai privalo suteikti susijusiems asmenims būtiną galimybę rinktis, nebent jie jau būtų leidę informaciją naudoti tokiais tikslais. Toks naudojimas negali būti nesuderinamas su tikslais, kuriais asmeninė informacija buvo surinkta arba vėliau asmuo ją leido naudoti. Be to, draudžiama dėl tokio pasirinkimo riboti galimybes įsidarbinti arba imtis kokių nors baudžiamųjų veiksmų prieš tokius darbuotojus.

ii. Pažymėtina, kad tam tikromis plačiai taikomomis duomenų perdavimo iš kai kurių ES valstybių narių sąlygomis gali būti neleidžiama naudoti tokios informacijos kitais tikslais net ir perdavus ją už ES ribų ir tokias sąlygas būtina vykdyti.

iii. Be to, darbdaviai turėtų dėti pagrįstas pastangas atsižvelgti į darbuotojų privatumo pageidavimus. Tai gali būti daroma, pvz., apribojant galimybę susipažinti su asmens duomenimis, kai kuriuos duomenis nuasmeninant arba priskiriant jiems kodus ar pseudonimus, kai tikrieji vardai atitinkamu valdymo tikslu nebūtini.

iv. Tokiu mastu ir tol, kol tai būtina, kad nebūtų sumažintos organizacijos galimybės paaukštinti pareigas, skirti į pareigas ar priimti kitus panašius darbo santykių sprendimus, organizacija pranešti ir suteikti galimybės rinktis neprivalo.

c. Susipažinimo su duomenimis principo taikymas

i. Pagal papildomą susipažinimo su duomenimis principą nurodomos priežastys, kuriomis gali būti pateisinamas atsisakymas suteikti prašomą galimybę susipažinti su duomenimis arba tokios galimybės ribojimas žmogiškųjų išteklių srityje. Be abejo, darbdaviai ES privalo laikytis vietos teisės aktų ir užtikrinti, kad ES darbuotojai galėtų susipažinti su tokia informacija, kaip reikalaujama jų šalių teisės aktuose, neatsižvelgiant į tai, kur tvarkomi ir saugomi duomenys. Pagal ES ir JAV DPS reikalaujama, kad tokius duomenis tvarkanti organizacija Jungtinėse Amerikos Valstijose bendradarbiautų suteikdama tokią galimybę susipažinti su duomenimis tiesiogiai arba per ES darbdavį.

d. Vykdymo užtikrinimas

i. Tiek, kiek asmeninė informacija naudojama tik darbo santykių aplinkybėmis, darbuotojo atžvilgiu pagrindinė atsakomybė už duomenis tenka ES veikiančiai organizacijai. Taigi Europos darbuotojams pasiskundus dėl jų duomenų apsaugos teisių pažeidimų ir esant nepatenkintiems vidinio patikrinimo, skundo nagrinėjimo ir apeliacijos procedūrų (arba bet kurių taikomų skundų teikimo procedūrų pagal sutartį su profesine sąjunga) rezultatais, tie skundai turėtų būti perduoti valstijos ar nacionalinei duomenų apsaugos ar darbo institucijai, kurios jurisdikcijai priklauso darbuotojų darbovietė. Tai apima atvejus, kai už įtariamą netinkamą jų asmeninės informacijos tvarkymą atsako JAV organizacija, gavusi tą informaciją iš darbdavio, o tai reiškia įtariamą Principų pažeidimą. Tai yra veiksmingiausias būdas spręsti klausimus dėl dažnai sutampančių teisių ir prievolių, nustatytų vietos darbo teisės aktais ir darbo sutartimis, taip pat duomenų apsaugos teisės aktais.

ii. Todėl ES ir JAV DPS dalyvaujanti JAV organizacija, naudojanti darbo santykių aplinkybėmis iš ES perduodamus ES žmogiškųjų išteklių duomenis ir norinti, kad perduodant tokius duomenis būtų taikoma ES ir JAV DPS, privalo įsipareigoti bendradarbiauti su kompetentingomis ES institucijomis joms vykdant tyrimus ir laikytis jų rekomendacijų.

e. Atskaitomybės už tolesnį duomenų perdavimą principo taikymas

i. Tenkinant sistemoje dalyvaujančios organizacijos atsitiktinius su darbu susijusius veiklos poreikius, kurie apima pagal ES ir JAV DPS perduotų asmens duomenų tvarkymą, pvz., dėl skrydžio ar viešbučio kambario užsakymo arba draudimo, nedidelio skaičiaus darbuotojų asmens duomenys gali būti perduodami duomenų valdytojams netaikant susipažinimo su duomenimis principo arba nesudarant sutarties su trečiąja šalimi duomenų valdytoja, kaip kitais atvejais reikalaujama pagal atskaitomybės už tolesnį duomenų perdavimą principą, su sąlyga, kad ta sistemoje dalyvaujanti organizacija laikėsi pranešimo ir pasirinkimo principų.

10. **Privalomos sutartys dėl tolesnio duomenų perdavimo**

a. Duomenų tvarkymo sutartys

i. Jeigu asmens duomenys iš ES į Jungtines Amerikos Valstijas perduodami tik tvarkymo tikslais, reikalaujama sudaryti sutartį nepaisant to, kad duomenų tvarkytojas dalyvauja ES ir JAV DPS.

ii. ES veikiantys duomenų valdytojai visada privalo sudaryti sutartį, kai duomenys perduodami vien tvarkyti, nesvarbu, ar duomenys tvarkomi ES, ar už jos ribų ir ar duomenų tvarkytojas dalyvauja ES ir JAV DPS. Sutartimi siekiama užtikrinti, kad duomenų tvarkytojas:

1. veiktų tik pagal duomenų valdytojo nurodymus;

2. pasirūpintų tinkamomis techninėmis ir organizacinėmis priemonėmis asmens duomenims apsaugoti, kad jie nebūtų atsitiktinai ar neteisėtai sunaikinti arba atsitiktinai prarasti, pakeisti, neteisėtai atskleisti arba neteisėtai su jais susipažinta, ir žinotų, ar duomenis leidžiama perduoti toliau, taip pat

3. atsižvelgdamas į duomenų tvarkymo pobūdį, padėtų duomenų valdytojui pateikti atsakymus asmenims, kurie naudojasi savo teisėmis pagal Principus.

iii. Kadangi sistemoje dalyvaujančios organizacijos užtikrina tinkamą apsaugą, su tokiomis organizacijomis sudarant sutartis vien dėl duomenų tvarkymo gauti išankstinio leidimo nereikia.

b. Duomenų perdavimas korporacijų ar subjektų kontroliuojamoje grupėje

i. Kai asmeninė informacija perduodama tarp dviejų duomenų valdytojų korporacijų ar subjektų kontroliuojamoje grupėje, ne visada reikalaujama sudaryti sutartį pagal atskaitomybės už tolesnį duomenų perdavimą principą. Korporacijų ar subjektų kontroliuojamoje grupėje veikiantys duomenų valdytojai taip perduoti duomenis gali remdamiesi kitomis priemonėmis, pvz., ES įmonėms privalomomis taisyklėmis arba kitomis grupėje taikomomis priemonėmis (pvz., reikalavimų laikymosi užtikrinimo ir kontrolės programomis), kuriomis užtikrinama nuolatinė asmeninės informacijos apsauga pagal Principus. Taip perduodant duomenis sistemoje dalyvaujanti organizacija lieka atsakinga už Principų laikymąsi.

c. Duomenų perdavimas tarp duomenų valdytojų

i. Jeigu duomenų valdytojai duomenis perduoda tarpusavyje, duomenis gaunantis duomenų valdytojas nebūtinai turi būti sistemoje dalyvaujanti organizacija arba turėti nepriklausomą teisių gynimo mechanizmą. Sistemoje dalyvaujanti organizacija privalo sudaryti sutartį su duomenis gaunančia trečiąja šalimi duomenų valdytoja, kuria užtikrinamas toks pat apsaugos lygis kaip ir pagal ES ir JAV DPS, bet nereikalaujama, kad ta trečioji šalis duomenų valdytoja būtų sistemoje dalyvaujanti organizacija arba turėtų nepriklausomą teisių gynimo mechanizmą, jeigu užtikrina galimybę naudotis lygiaverčiu mechanizmu.

11. **Ginčų sprendimas ir vykdymo užtikrinimas**

a. Pagal teisių gynimo, vykdymo užtikrinimo ir atsakomybės principą nustatomi ES ir JAV DPS įgyvendinimui užtikrinti taikomi reikalavimai. Šio principo a punkto ii papunktyje nustatytų reikalavimų vykdymo tvarka nustatoma pagal papildomą patikrinimo principą. Šis papildomas principas taikomas a punkto i ir iii papunkčiams, kuriuose reikalaujama užtikrinti nepriklausomus teisių gynimo mechanizmus. Tokie mechanizmai gali būti įvairūs, tačiau turi atitikti teisių gynimo, vykdymo užtikrinimo ir atsakomybės principo reikalavimus. Organizacijos reikalavimus įvykdo taip: i) laikydamosi privačiojo sektoriaus sukurtų privatumo užtikrinimo programų, kurių taisyklėse įtvirtinti Principai ir kuriose nustatyti veiksmingi pagal teisių gynimo, vykdymo užtikrinimo ir atsakomybės principą nurodyto tipo vykdymo užtikrinimo mechanizmai; ii) laikydamosi teisinių arba reguliuojamojo pobūdžio priežiūros institucijų reikalavimų, susijusių su asmenų skundų nagrinėjimu ir ginčų sprendimu, arba iii) įsipareigodamos bendradarbiauti su ES veikiančiomis DAI arba jų įgaliotais atstovais.

b. Šis sąrašas tik pavyzdinis ir nebaigtinis. Privačiajame sektoriuje gali būti sukurta papildomų mechanizmų, kuriais užtikrinamas vykdymas, jeigu jie atitinka teisių gynimo, vykdymo užtikrinimo ir atsakomybės principo ir papildomų principų reikalavimus. Pažymėtina, kad teisių gynimo, vykdymo užtikrinimo ir atsakomybės principo reikalavimai papildo reikalavimą, kad turi būti užtikrinamas savireguliavimo veiklos vykdymas pagal FPK akto 5 straipsnį (JAV kodekso 15 antraštinės dalies 45 straipsnį), kuriuo draudžiami nesąžiningi ir apgaulingi veiksmai, JAV kodekso 49 antraštinės dalies 41712 straipsnį, kuriuo vežėjui arba bilietų pardavėjui draudžiama vykdyti nesąžiningą ar apgaulingą veiklą oro transporto arba oro transporto paslaugų pardavimo srityse, arba kitą įstatymą ar teisės aktą, kuriuo draudžiami tokie veiksmai.

c. Siekdamos padėti užtikrinti, kad būtų laikomasi jų įsipareigojimų pagal ES ir JAV DPS, ir palengvinti programos administravimą, organizacijos, be kita ko, pagal jų nepriklausomus teisių gynimo mechanizmus, Departamentui paprašius privalo teikti su ES ir JAV DPS susijusią informaciją. Be to, organizacijos privalo operatyviai atsakyti į skundus dėl jų padarytų Principų pažeidimų, kuriuos per Departamentą perdavė DAI. Atsakyme reikėtų nurodyti, ar skundas turi pagrindą, ir, jei taip, kaip organizacija spręs tą problemą. Departamentas gautos informacijos konfidencialumą užtikrins pagal JAV teisę.

d. Teisių gynimo mechanizmai

i. Asmenys turėtų būti raginami prieš naudodamiesi nepriklausomais teisių gynimo mechanizmais pirmiau savo skundus pateikti atitinkamai organizacijai. Organizacijos privalo asmeniui pateikti atsakymą per 45 dienas nuo skundo gavimo. Ar teisių gynimo mechanizmas nepriklausomas, yra faktinis klausimas, į kurį galima atsakyti visų pirma įvertinus nešališkumą, skaidrią sudėtį ir finansavimą, taip pat įrodymais pagrįstą ankstesnę patirtį. Kaip reikalaujama pagal teisių gynimo, vykdymo užtikrinimo ir atsakomybės principą, teisių gynimo priemonės, kuriomis gali naudotis asmenys, turi būti lengvai prieinamos ir nemokamos. Nepriklausomos ginčų sprendimo įstaigos turėtų nagrinėti kiekvieną iš asmenų gautą skundą, nebent tokie skundai akivaizdžiai nepagrįsti ar nerimti. Taip neužkertamas kelias teisių gynimo mechanizmą teikiančiai nepriklausomai ginčų sprendimo įstaigai nustatyti tinkamumo reikalavimus, tačiau tokie reikalavimai turėtų būti skaidrūs ir pagrįsti (pvz., atmetant skundus, kuriems programa netaikoma arba jie turi būti nagrinėjami kitur) ir jais neturėtų būti sumažintas įsipareigojimas nagrinėti teisėtus skundus. Be to, teikiant skundą pagal teisių gynimo mechanizmus asmenims turėtų būti suteikta išsami ir lengvai prieinama informacija apie ginčų sprendimo tvarką. Teikiant tokią informaciją turėtų būti pranešama apie mechanizmo privatumo užtikrinimo praktiką, kuri atitinka Principus. Institucijos taip pat turėtų bendradarbiauti kurdamos tokias priemones kaip standartinės skundų formos, kad palengvintų skundų nagrinėjimo procesą.

ii. Nepriklausomų teisių gynimo mechanizmų viešose interneto svetainėse turi būti pateikta informacijos apie Principus ir paslaugas, jų teikiamas pagal ES ir JAV DPS. Ši informacija turi apimti: 1) informaciją apie nepriklausomiems teisių gynimo mechanizmams pagal Principus taikomus reikalavimus arba tokių reikalavimų nuorodą; 2) Departamento Duomenų privatumo sistemos interneto svetainės nuorodą; 3) paaiškinimą, kad jų ginčų sprendimo paslaugos pagal ES ir JAV DPS asmenims teikiamos nemokamai; 4) aprašymą, kaip galima pateikti su Principais susijusį skundą; 5) terminus, per kuriuos išnagrinėjami su Principais susiję skundai; 6) galimų taisomųjų priemonių aprašymą.

iii. Turi būti skelbiama nepriklausomų teisių gynimo mechanizmų metinė ataskaita, kurioje pateikiami apibendrinti jų teikiamų ginčų sprendimo paslaugų statistiniai duomenys. Metinėje ataskaitoje turi būti nurodyta: 1) bendras per ataskaitinius metus gautų su Principais susijusių skundų skaičius; 2) gautų skundų rūšys; 3) ginčų sprendimo kokybės užtikrinimo priemonės, pvz., skundų nagrinėjimo trukmė; 4) gautų skundų nagrinėjimo rezultatai, visų pirma taikytų teisių gynimo priemonių ar sankcijų skaičius ir rūšys.

iv. Kaip nustatyta I priede, asmuo gali kreiptis dėl arbitražo, kad, atsižvelgiant į neįvykdytus reikalavimus, būtų nustatyta, ar sistemoje dalyvaujanti organizacija pažeidė savo įsipareigojimus pagal Principus dėl to asmens ir ar toks pažeidimas tebėra visiškai arba iš dalies neištaisytas. Šia galimybe galima pasinaudoti tik nurodytais tikslais. Šia galimybe negalima naudotis, pvz., dėl Principų išimčių ([15]) arba dėl teiginių, susijusių su ES ir JAV DPS tinkamumu. Pagal šią arbitražo galimybę ES ir JAV duomenų privatumo sistemos kolegija (kurią sudaro vienas arba trys arbitrai, kaip susitarė šalys) turi įgaliojimus nustatyti konkrečiam asmeniui skirtas nepinigines lygiavertes teisių gynimo priemones (pvz., galimybę susipažinti su atitinkamais asmens duomenimis, juos ištaisyti, ištrinti ar grąžinti), kurios yra būtinos siekiant ištaisyti Principų pažeidimą tik to asmens atžvilgiu. Asmenys ir sistemoje dalyvaujančios organizacijos galės siekti, kad pagal Federalinį arbitražo aktą arbitražo sprendimai būtų peržiūrėti teisme ir vykdomi pagal JAV teisę.

e. Teisių gynimo priemonės ir sankcijos

i. Nepriklausomos ginčų sprendimo įstaigos nurodytomis teisių gynimo priemonėmis turėtų būti užtikrinama, kad organizacija, kiek įmanoma, panaikintų ar ištaisytų reikalavimų nesilaikymo padarinius, toliau tvarkytų duomenis laikydamasi Principų ir atitinkamais atvejais nutrauktų skundą pateikusio asmens duomenų tvarkymą. Sankcijos turi būti pakankamai griežtos, kad priverstų organizacijas laikytis Principų. Taikydamos skirtingo griežtumo sankcijas, ginčų sprendimo įstaigos galės tinkamai reaguoti į įvairaus sunkumo reikalavimų nesilaikymo atvejus. Taikant sankcijas, be kita ko, turėtų būti viešai skelbiamos

([15]) Principų apžvalga, 5 punktas.

išvados dėl reikalavimų nesilaikymo ir tam tikromis aplinkybėmis reikalaujama ištrinti duomenis ([16]). Kitos sankcijos galėtų būti ženklo galiojimo sustabdymas ir atėmimas, dėl reikalavimų nesilaikymo asmenims padarytos žalos atlyginimas ir nustatyti draudimai. Privačiojo sektoriaus nepriklausomos ginčų sprendimo įstaigos ir savireguliavimo įstaigos apie tai, kad sistemoje dalyvaujančios organizacijos nesilaiko jų nutarčių, privalo pranešti atitinkamai valdžios institucijai, kurios jurisdikcijai priklauso tie klausimai, arba teismams ir informuoti Departamentą.

f. FPK veikla

i. FPK įsipareigojo pirmumo tvarka peržiūrėti klausimus dėl įtariamo Principų nesilaikymo, kuriuos jai perdavė: i) privatumo savireguliavimo įstaigos ir kitos nepriklausomos ginčų sprendimo įstaigos, ii) ES valstybės narės ir iii) Departamentas, kad nustatytų, ar buvo pažeistas FPK akto 5 straipsnis, kuriuo prekybos srityje draudžiami nesąžiningi ar apgaulingi veiksmai ar veikla. Nusprendusi, jog yra priežasčių manyti, kad 5 straipsnis buvo pažeistas, FPK gali spręsti šį klausimą siekdama, kad būtų išduota administracinė nutartis nutraukti veiksmus, kuria uždraudžiama taikyti svarstomą praktiką, arba pateikdama skundą federaliniam apygardos teismui. Jeigu jis priima palankų sprendimą, galėtų būti paskelbta tokio pat poveikio federalinio teismo nutartis. Tai apima organizacijų, kurios jau nėra įtrauktos į Duomenų privatumo sistemos sąrašą arba niekada nebuvo atlikusios savarankiško sertifikavimo Departamente, neteisingus teiginius apie Principų laikymąsi arba dalyvavimą ES ir JAV DPS. FPK gali taikyti pinigines nuobaudas už administracinės nutarties nutraukti veiklą nesilaikymą ir vykdyti administracinį arba baudžiamąjį persekiojimą už federalinio teismo nutarties nevykdymą. FPK informuos Departamentą apie visus tokius veiksmus, kurių imasi. Departamentas ragina kitas valdžios institucijas jam pranešti, kaip galiausiai išspręsti tokie joms perduoti klausimai, arba apie kitas nutartis dėl Principų laikymosi.

g. Nuolatinis reikalavimų nesilaikymas

i. Jeigu organizacija nuolat nesilaiko Principų, ji netenka teisės naudotis ES ir JAV DPS. Nuolat Principų nesilaikančias organizacijas Departamentas išbrauks iš Duomenų privatumo sistemos sąrašo ir jos privalės grąžinti arba ištrinti pagal ES ir JAV DPS gautą asmeninę informaciją.

ii. Nuolatiniu reikalavimų nesilaikymu laikoma padėtis, kai Departamente savarankišką sertifikavimą atlikusi organizacija atsisako vykdyti galutinį bet kurios privatumo savireguliavimo įstaigos, nepriklausomos ginčų sprendimo įstaigos ar valdžios institucijos sprendimą, arba kai tokia įstaiga ar institucija, įskaitant Departamentą, nustato, kad organizacija taip dažnai nesilaiko Principų, kad jos pasižadėjimas jų laikytis jau yra neįtikimas. Jeigu tokį sprendimą priima ne Departamentas, organizacija privalo nedelsdama apie tai pranešti Departamentui. To nepadarius, gali būti taikomos sankcijos pagal Melagingų parodymų aktą (JAV kodekso 18 antraštinės dalies 1001 straipsnį). Pasitraukusi iš privačiojo sektoriaus privatumo savireguliavimo programos arba nepriklausomo ginčų sprendimo mechanizmo organizacija neatleidžiama nuo prievolės laikytis Principų ir tai būtų laikoma nuolatiniu reikalavimų nesilaikymu.

iii. Departamentas dėl nuolatinio reikalavimų nesilaikymo organizaciją iš Duomenų privatumo sistemos sąrašo išbrauks, be kita ko, reaguodamas į visus iš pačios organizacijos, privatumo savireguliavimo įstaigos, kitos nepriklausomos ginčų sprendimo įstaigos arba valdžios institucijos gautus pranešimus apie tokių reikalavimų nesilaikymą, tačiau tik pirmiau prieš 30 dienų organizacijai įteikęs pranešimą ir suteikęs galimybę pateikti atsakymą ([17]). Taigi iš Departamento tvarkomo Duomenų privatumo sistemos sąrašo bus aišku, kurios organizacijos gali naudotis ES ir JAV DPS teikiamais privalumais, o kurios – ne.

iv. Organizacija, teikdama prašymą dalyvauti savireguliavimo įstaigos veikloje, kad galėtų vėl naudotis ES ir JAV DPS, privalo tai institucijai pateikti visą informaciją apie savo ankstesnį dalyvavimą ES ir JAV DPS.

([16]) Nepriklausomos ginčų sprendimo įstaigos gali pasirinkti, kokiomis aplinkybėmis taikys tokias sankcijas. Sprendžiant, ar reikėtų reikalauti ištrinti duomenis, reikia atsižvelgti į tai, ar atitinkami duomenys neskelbtini, taip pat į tai, ar organizacija rinko, naudojo ar atskleidė informaciją akivaizdžiai nepaisydama Principų.

([17]) Departamentas pranešime nurodo, per kiek laiko (visada mažiau nei 30 dienų) organizacija turi atsakyti į pranešimą.

12. **Pasirinkimas. Atsisakymo sutikti laikas**

a. Apskritai pasirinkimo principu siekiama užtikrinti, kad asmeninė informacija būtų naudojama ir atskleidžiama taip, kaip to tikisi ir pasirenka pats asmuo. Todėl asmuo turėtų turėti galimybę bet kuriuo metu atsisakyti sutikti, kad jo asmeninė informacija būtų tvarkoma tiesioginės rinkodaros tikslais, laikydamasis organizacijos nustatytų pagrįstų terminų, kurių, pvz., organizacijai pakaktų atsisakymui sutikti įgyvendinti. Organizacija taip pat gali reikalauti pateikti pakankamai informacijos atsisakymo sutikti reikalaujančio asmens tapatybei patvirtinti. Jungtinėse Amerikos Valstijose asmenys šia pasirinkimo galimybe gali pasinaudoti naudodamiesi centrine atsisakymo programa. Bet kuriuo atveju asmeniui turi būti suteiktas lengvai prieinamas ir suprantamas mechanizmas, kad jis galėtų pasinaudoti šia galimybe.

b. Be to, organizacija gali naudoti informaciją tam tikrais tiesioginės rinkodaros tikslais, kai suteikti asmeniui galimybę atsisakyti sutikti prieš panaudojant informaciją praktiškai neįmanoma, jeigu organizacija suteikia asmeniui galimybę iškart (o pareikalavus – bet kuriuo metu) atsisakyti (nemokamai) gauti paskesnius tiesioginės rinkodaros pranešimus ir įvykdo to asmens pageidavimą.

13. **Kelionių informacija**

a. Oro vežėjo keleivio rezervavimo duomenys ir kita kelionės informacija, pvz., keleivio lojalumo arba viešbučio rezervavimo informacija ir informacija apie specialius keleivio poreikius, pvz., dėl religinius reikalavimus atitinkančio maisto arba fizinės pagalbos, ne ES esančioms organizacijoms gali būti perduodami keleriopomis skirtingomis aplinkybėmis. Pagal BDAR, nesant sprendimo dėl tinkamumo, asmens duomenys gali būti perduodami trečiajai valstybei, jeigu pagal BDAR 46 straipsnį yra numatytos tinkamos duomenų apsaugos priemonės, arba, tam tikrais atvejais, jeigu tenkinama viena iš BDAR 49 straipsnio sąlygų (pvz., jeigu duomenų subjektas aiškiai sutiko, kad duomenys būtų perduoti). Prie ES ir JAV DPS prisijungusios JAV organizacijos užtikrina tinkamą asmens duomenų apsaugą, todėl gali gauti iš ES perduodamus duomenis pagal BDAR 45 straipsnį neprivalėdamos nustatyti duomenų perdavimo apsaugos priemonės pagal BDAR 46 straipsnį arba laikytis BDAR 49 straipsnyje nustatytų sąlygų. Kadangi ES ir JAV DPS neskelbtinai informacijai taikomos specialios taisyklės, tokia informacija (kurią gali reikėti rinkti, nes, pvz., klientui reikia fizinės pagalbos) gali būti įtraukiama perduodant duomenis sistemoje dalyvaujančioms organizacijoms. Tačiau informaciją perduodanti organizacija visais atvejais privalo laikytis ES valstybės narės, kurioje veikia, teisės aktų, kuriuose, *inter alia*, gali būti nustatytos specialios neskelbtinų duomenų tvarkymo sąlygos.

14. **Vaistai ir medicinos reikmenys**

a. ES ar valstybių narių teisės aktų arba Principų taikymas

i. Renkant ir tvarkant asmens duomenis prieš juos perduodant į Jungtines Amerikos Valstijas galioja ES ar valstybės narės teisės aktai. Perdavus duomenis į Jungtines Amerikos Valstijas, galioja Principai. Farmaciniams tyrimams ir kitais tikslais naudojami duomenys, jei įmanoma, turėtų būti nuasmeninti.

b. Būsimi moksliniai tyrimai

i. Vykdant konkrečius medicinos ar farmacinius tyrimus gauti asmens duomenys dažnai yra labai vertingi būsimiems moksliniams tyrimams. Jeigu atliekant mokslinį tyrimą surinkti asmens duomenys perduodami ES ir JAV DPS dalyvaujančiai JAV organizacijai, ta organizacija gali tuos duomenis naudoti naujai mokslinių tyrimų veiklai, jeigu iš pradžių tinkamai pranešė duomenų subjektui ir suteikė jam galimybę rinktis. Tokiame pranešime turėtų būti pateikta informacijos apie bet kokį būsimą konkretų duomenų panaudojimą, pvz., periodinę stebėseną, susijusius tyrimus ar rinkodarą.

ii. Suprantama, kad visų būsimų duomenų panaudojimo atvejų nurodyti neįmanoma, nes naujai naudoti duomenis moksliniams tyrimams gali prireikti dėl pradiniais duomenimis grindžiamų naujų įžvalgų, naujų medicinos atradimų ir pažangos, taip pat visuomenės sveikatos ir reglamentavimo pokyčių. Todėl, jei įmanoma, pranešime turi būti paaiškinta, kad asmens duomenys gali būti naudojami nenumatytai būsimų medicinos ir farmacinių tyrimų veiklai. Jeigu asmens duomenis ketinama naudoti tikslu (-ais), neatitinkančiu (-iais) bendrojo (-ųjų) mokslinių tyrimų tikslo (-ų), kuriuo (-iais) duomenys iš pradžių buvo surinkti arba vėliau asmuo leido juos naudoti, sutikimą būtina gauti iš naujo.

c. Pasitraukimas iš klinikinio tyrimo

i. Dalyviai bet kuriuo metu gali nuspręsti arba jų gali būti paprašyta nebedalyvauti klinikiniame tyrime. Visi iki pasitraukimo surinkti asmens duomenys gali būti toliau tvarkomi kartu su kitais klinikinio tyrimo metu surinktais duomenimis, jei dalyviui apie tai buvo aiškiai pranešta tuomet, kai jis sutiko dalyvauti.

d. Duomenų perdavimas reguliavimo ir priežiūros tikslais

i. Vaistus ir medicinos priemones gaminančioms bendrovėms leidžiama ES vykdytų klinikinių tyrimų metu gautus asmens duomenis reguliavimo ir priežiūros tikslais pateikti Jungtinėse Amerikos Valstijose veikiančioms reguliavimo institucijoms. Panašiai duomenis leidžiama perduoti kitoms šalims, kurios nėra reguliavimo institucijos, pvz., bendrovės padaliniams 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 galimybės susipažinti su informacija apie kiekvieno dalyvio gydymą. Suteikus tokią galimybę kiltų pavojus, kad tyrimai ir jų rezultatai bus nepatikimi. Tokių klinikinių tyrimų (vadinamųjų aklųjų tyrimų) dalyviams neturi būti suteikiama galimybė susipažinti su duomenimis apie jų gydymą, kol vyksta tyrimas, jeigu šis apribojimas buvo paaiškintas dalyviui įsitraukiant į tyrimą, o tokios informacijos atskleidimas pakenktų mokslinio tyrimo vientisumui.

ii. Sutinkant dalyvauti tyrime tokiomis sąlygomis pagrįstai atsisakoma teisės susipažinti su duomenimis. Baigus tyrimą ir išanalizavus rezultatus dalyviams turėtų būti suteikiama galimybė susipažinti su jų duomenimis, jei jie to prašo. Pirmiausia jie to turėtų prašyti klinikinio tyrimo metu juos gydžiusio gydytojo ar kito sveikatos priežiūros paslaugų teikėjo arba po to – paramą teikusios organizacijos.

f. Produkto saugos ir veiksmingumo stebėsena

i. Vaistus ar medicinos priemones gaminanti bendrovė, vykdydama jos produktų saugos ir veiksmingumo stebėsenos veiklą, be kita ko, rengdama pranešimus apie nepageidaujamus reiškinius ir stebėdama tam tikrus vaistus vartojančius arba medicinos priemones naudojančius pacientus ar subjektus, neprivalo taikyti pranešimo, pasirinkimo, atskaitomybės už tolesnį duomenų perdavimą ir susipažinimo su duomenimis principų tiek, kiek laikantis Principų nepavyksta laikytis reguliavimo reikalavimų. Tai pasakytina ir apie sveikatos priežiūros teikėjų paslaugų ataskaitas vaistus ir medicinos priemones gaminančioms bendrovėms, ir apie vaistus ir medicinos reikmenis gaminančių bendrovių ataskaitas valdžios institucijoms, kaip antai Maisto ir vaistų administracijai.

g. Raktu užkoduoti duomenys

i. Dažniausiai pagrindinis tyrėjas iš pat pradžių užkoduoja duomenis unikaliu kodo raktu, kad nebūtų atskleista atskirų duomenų subjektų tapatybė. Tokį tyrimą remiančios farmacijos bendrovės kodo rakto negauna. Unikalų kodo raktą turi tik tyrėjas, kad tam tikromis aplinkybėmis galėtų nustatyti tyrimų subjekto tapatybę (pvz., jei reikia tęstinės medicinos priežiūros). Taip užkoduotų duomenų, kurie pagal ES teisę yra ES asmens duomenys, perdavimui iš ES į Jungtines Amerikos Valstijas Principai būtų taikomi.

15. **Vieši archyvai ir viešai prieinama informacija**

a. Organizacija privalo iš viešai prieinamų šaltinių gautiems asmens duomenims taikyti saugumo, duomenų vientisumo ir tikslo apribojimo, taip pat teisių gynimo, vykdymo užtikrinimo ir atsakomybės principus. Šie Principai taip pat taikomi iš viešų archyvų (t. y. iš bet kurio lygio valstybinių agentūrų ar įstaigų saugomų archyvų, kurie apskritai prieinami visuomenei) surinktiems asmens duomenims.

b. Pranešimo, pasirinkimo ar atskaitomybės už tolesnį duomenų perdavimą principų viešų archyvų informacijai taikyti nebūtina, jei ji nėra sujungta su neviešų archyvų informacija ir yra paisoma atitinkamoje jurisdikcijoje nustatytų susipažinimo su duomenimis sąlygų. Taip pat paprastai nebūtina taikyti pranešimo, pasirinkimo ar atskaitomybės už tolesnį duomenų perdavimą principų viešai prieinamai informacijai, nebent Europos siuntėjas nurodo, kad tokiai informacijai taikomi apribojimai, dėl kurių naudodama duomenis tokiu tikslu, kokiu ketina juos naudoti, organizacija privalo taikyti Principus. Organizacijos neatsako už tai, kaip tokią informaciją naudos ją iš paskelbtos medžiagos gavę subjektai.

c. Jeigu nustatoma, kad organizacija pažeisdama Principus sąmoningai viešai paskelbė asmeninę informaciją taip, kad ji ar kiti iš tokios išimties galėtų turėti naudos, ji netenka teisės naudotis ES ir JAV DPS teikiamais privalumais.

d. Susipažinimo su duomenimis principo iš viešų archyvų gautai informacijai taikyti nebūtina, jeigu ji nesujungta su kita asmenine informacija (išskyrus nedidelius kiekius, naudojamus viešuose archyvuose pateikiamai informacijai indeksuoti arba tvarkyti), tačiau turi būti paisoma atitinkamoje jurisdikcijoje nustatytų susipažinimo su duomenimis sąlygų. Priešingai, kai viešų archyvų informacija yra sujungta su kita neviešų archyvų informacija (kitokia, nei nurodyta pirmiau), organizacija privalo leisti susipažinti su visa tokia informacija, jeigu jai netaikomos kitos leidžiamos išimtys.

e. Kaip ir dėl viešų archyvų informacijos, nebūtina suteikti galimybės susipažinti su informacija, kuri ir taip viešai prieinama plačiajai visuomenei, jeigu tokia informacija nesujungta su viešai neprieinama informacija. Viešai prieinama informacija prekiaujančios organizacijos atsakydamos į prašymus leisti susipažinti su informacija gali taikyti įprastai organizacijos taikomą mokestį. Kita vertus, asmenys gali siekti susipažinti su informacija apie save per organizaciją, kuri iš pradžių sukaupė tuos duomenis.

16. **Valdžios institucijų prašymai leisti susipažinti su duomenimis**

a. Siekiant užtikrinti valdžios institucijų teisėtų prašymų leisti susipažinti su asmenine informacija skaidrumą, sistemoje dalyvaujančios organizacijos gali savo noru periodiškai teikti skaidrumo ataskaitas, kuriose būtų nurodomas joms teisėsaugos arba nacionalinio saugumo tikslais valdžios institucijų pateiktų prašymų leisti susipažinti su asmenine informacija skaičius, kiek pagal taikomą teisę leidžiama atskleisti tokią informaciją.

b. Sistemoje dalyvaujančių organizacijų tokiose ataskaitose pateikta informacija kartu su žvalgybos bendruomenės paskelbta informacija ir kita informacija gali būti naudojama atliekant periodinę ES ir JAV DPS veikimo pagal Principus bendrą metinę peržiūrą.

c. Tai, kad nepateikta pranešimo pagal pranešimo principo a punkto xii papunktį, nepanaikina ir nesumažina organizacijos galimybių atsakyti į bet kurį teisėtą prašymą.

I PRIEDAS. ARBITRAŽO MODELIS

Šiame I priede nurodomos sąlygos, kuriomis ES ir JAV DPS dalyvaujančios organizacijos įpareigojamos pagal teisių gynimo, vykdymo užtikrinimo ir atsakomybės principą nagrinėti reikalavimus arbitražo tvarka. Toliau aprašyta privalomo arbitražo galimybė galioja tam tikriems neįvykdytiems reikalavimams, susijusiems su duomenimis, kuriems taikoma ES ir JAV DPS. Suteikiant šią galimybę siekiama sukurti operatyvų, nepriklausomą ir sąžiningą mechanizmą, kurį asmenys galėtų rinktis, kad išspręstų įtariamus Principų pažeidimus, kurie nebuvo išspręsti taikant bet kurį kitą ES ir JAV DPS mechanizmą.

A. **Taikymo sritis**

Asmuo gali pasinaudoti šia arbitražo galimybe, kad, atsižvelgiant į neįvykdytus reikalavimus, būtų nustatyta, ar sistemoje dalyvaujanti organizacija pažeidė savo įsipareigojimus pagal Principus dėl to asmens ir ar toks pažeidimas tebėra visiškai arba iš dalies neištaisytas. Šia galimybe galima pasinaudoti tik nurodytais tikslais. Šia galimybe negalima naudotis, pvz., dėl Principų išimčių ([1]) arba dėl teiginių, susijusių su ES ir JAV DPS tinkamumu.

B. **Galimos teisių gynimo priemonės**

Pagal šią arbitražo galimybę ES ir JAV duomenų privatumo sistemos kolegija (arbitražo kolegija, kurią sudaro vienas arba trys arbitrai, kaip susitarė šalys) turi įgaliojimus nustatyti konkrečiam asmeniui skirtas nepinigines lygiavertes teisių gynimo priemones (pvz., galimybę susipažinti su atitinkamais asmens duomenimis, juos ištaisyti, ištrinti ar grąžinti), kurios yra būtinos siekiant ištaisyti Principų pažeidimą tik to asmens atžvilgiu. Tai vieninteliai ES ir JAV duomenų privatumo sistemos kolegijos įgaliojimai, susiję su teisių gynimo priemonėmis. Svarstydama teisių gynimo priemones, ES ir JAV duomenų privatumo sistemos kolegija privalo atsižvelgti į kitas teisių gynimo priemones, kurios jau buvo taikomos naudojantis kitais mechanizmais pagal ES ir JAV DPS. Žalos, išlaidų, mokesčių ar kitų teisių gynimo priemonių taikymo atlyginimas negalimas. Kiekviena šalis padengia savo advokato mokesčius.

C. **Iki arbitražo įvykdytini reikalavimai**

Asmuo, nusprendęs pasinaudoti šia arbitražo galimybe, prieš perduodamas reikalavimą arbitražui privalo atlikti šiuos veiksmus: 1) pareikšti reikalavimą dėl įtariamo pažeidimo tiesiogiai organizacijai ir suteikti jai galimybę išspręsti klausimą per papildomo ginčų sprendimo ir vykdymo užtikrinimo principo d punkto i papunktyje nustatytą terminą; 2) nemokamai pasinaudoti nepriklausomu teisių gynimo mechanizmu pagal Principus; 3) per asmens DAI klausimą nemokamai perduoti Departamentui ir suteikti jam galimybę pasistengti išspręsti tą klausimą per Departamento Tarptautinės prekybos administracijos rašte nustatytus terminus.

Šia arbitražo galimybe naudotis negalima, jeigu tas pats asmens reikalavimas dėl įtariamo Principų pažeidimo 1) buvo anksčiau nagrinėtas privalomo arbitražo tvarka; 2) dėl jo buvo priimtas galutinis teismo sprendimas byloje, kurioje asmuo dalyvavo kaip bylos šalis, arba 3) šalys jį išsprendė anksčiau. Be to, šia galimybe naudotis negalima, jeigu DAI 1) turi įgaliojimų pagal papildomą duomenų apsaugos institucijų vaidmens principą arba papildomą žmogiškųjų išteklių duomenų principą, arba 2) turi įgaliojimus pašalinti įtariamą pažeidimą tiesiogiai organizacijoje. Dėl DAI įgaliojimų nagrinėti tą patį ES duomenų valdytojui pareikštą reikalavimą savaime neišnyksta galimybė pasinaudoti šia arbitražo galimybe prieš kitą juridinį asmenį, kuriam šie DAI įgaliojimai netaikomi.

D. **Privalomas sprendimų pobūdis**

Asmuo sprendimą naudotis šia privalomo arbitražo galimybe priima visiškai savanoriškai. Arbitražo sprendimai bus privalomi visoms arbitražo šalims. Pradėjus procedūrą, asmuo netenka galimybės dėl to paties įtariamo pažeidimo ginti savo teisių kitur, nebent nepinigine lygiaverte teisių gynimo priemone įtariamas pažeidimas nėra visiškai ištaisomas – tokiu atveju tai, kad asmuo kreipėsi dėl arbitražo, netrukdys pateikti reikalavimo atlyginti žalą, kurį apskritai galima pateikti teisme.

([1]) Principų apžvalga, 5 punktas.

E. **Peržiūra ir vykdymo užtikrinimas**

Asmenys ir sistemoje dalyvaujančios organizacijos galės siekti, kad pagal Federalinį arbitražo aktą arbitražo sprendimai būtų peržiūrėti teisme ir vykdomi pagal JAV teisę ([2]). Visos tokios bylos turi būti keliamos federaliniame apygardos teisme, kurio teritorinei jurisdikcijai priklauso dalyvaujančios organizacijos pagrindinė verslo vieta.

Ši arbitražo galimybė skirta spręsti asmenų ginčams, o arbitražo sprendimais nesiekiama sukurti atgrasančio ar privalomo precedento su kitomis šalimis susijusiose bylose, įskaitant būsimą arbitražą arba ES ir JAV teismų ar FPK procedūras.

F. **Arbitražo kolegija**

ES ir JAV duomenų privatumo sistemos kolegijos arbitrus šalys pasirinks iš toliau nurodyto arbitrų sąrašo.

Laikydamiesi taikomų teisės aktų, Departamentas ir Komisija sudarys sąrašą, į kurį įtrauks bent 10 arbitrų, atrinktų atsižvelgiant į jų nepriklausomumą, sąžiningumą ir patirtį. Šiam procesui taikomos toliau išdėstytos nuostatos.

Arbitrai:

1) bus įtraukti į sąrašą trejus metus, jeigu nesusiklostys išimtinės aplinkybės arba nebus išbraukti dėl svarios priežasties; šį laikotarpį Departamentas, iš anksto pranešęs Komisijai, gali pratęsti dar trejiems metams;

2) nesivadovauja jokios šalies, sistemoje dalyvaujančios organizacijos, JAV, ES ar bet kurios ES valstybės narės, kitos valstybinės institucijos, valdžios institucijos arba vykdymo užtikrinimo institucijos nurodymais ir nėra su jomis susiję; taip pat

3) turi turėti teisę verstis advokato praktika Jungtinėse Amerikos Valstijose, taip pat būti JAV privatumo teisės ekspertai ir turėti žinių apie ES duomenų apsaugos teisę.

([2]) 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 teismą, turintį jurisdikciją pagal šį skyrių, kad būtų priimta nutartis, kuria patvirtinamas sprendimas bet kurios kitos arbitražo šalies atžvilgiu. Teismas sprendimą patvirtina, jeigu nenustato vieno iš minėtoje [Niujorko] konvencijoje nurodytų pagrindų atsisakyti pripažinti ar vykdyti sprendimą arba sprendimo pripažinimą ar vykdymą atidėti“ (ten pat, 207 straipsnis). 2 skyriuje taip pat nustatyta, kad „Jungtinių Amerikos Valstijų apygardos teismai <...> turi pirmosios instancijos jurisdikciją nagrinėti <...> ieškinį ar bylą [pagal Niujorko konvenciją], nepaisant ginčo sumos“ (ten pat, 203 straipsnis).
Be to, 2 skyriuje nustatyta, kad „1 skyrius taikomas pagal šį skyrių pateiktiems ieškiniams ir iškeltoms byloms tiek, kiek tas skyrius neprieštarauja šiam skyriui arba Jungtinių Amerikos Valstijų ratifikuotai [Niujorko] Konvencijai“ (ten pat, 208 straipsnis). 1 skyriuje nustatyta, kad „[r]ašytinė <...> sutarties, kuria patvirtinamas su prekyba susijęs sandoris, nuostata, kuria siekiama arbitražo tvarka išspręsti ginčą, vėliau kilusį dėl tokios sutarties ar sandorio arba atsisakymo vykdyti visą tokią sutartį ar sandorį arba jo (-s) dalį, arba raštiškas susitarimas iš tokios sutarties, sandorio arba atsisakymo kilusį tebevykstantį ginčą perduoti spręsti arbitražo tvarka, yra galiojantys, neatšaukiami ir vykdytini, išskyrus atvejus, kai teisės aktuose arba lygiaverčiuose dokumentuose nustatyta pagrindų atšaukti tokią sutartį“ (ten pat, 2 straipsnis). 1 skyriuje taip pat nustatyta, kad „bet kuri arbitražo šalis gali kreiptis į nurodytą teismą ir prašyti priimti nutartį, kuria būtų patvirtintas arbitražo sprendimas, o tokį prašymą gavęs teismas privalo priimti tokią nutartį, išskyrus atvejus, kai sprendimas panaikinamas, pakeičiamas arba ištaisomas, kaip nustatyta [FAA] 10 ir 11 straipsniuose“ (ten pat, 9 straipsnis).

G. **Arbitražo procedūros**

Departamentas ir Komisija, laikydamiesi taikomų teisės aktų, susitarė priimti arbitražo taisykles, kuriomis reglamentuojamas procesas ES ir JAV duomenų privatumo sistemos kolegijoje ([3]). Jeigu procesą reglamentuojančias taisykles reikėtų pakeisti, Departamentas ir Komisija susitars atitinkamai iš dalies pakeisti tas taisykles arba priims kitokį galiojančių ir nusistovėjusių JAV arbitražo procedūrų rinkinį, atsižvelgdami į kiekvieną iš toliau nurodytų aplinkybių.

1. Jeigu įvykdyti pirmiau nurodyti iki arbitražo procedūros įvykdytini reikalavimai, asmuo gali inicijuoti privalomą arbitražą įteikdamas pranešimą organizacijai. Pranešime glaustai išdėstomos priemonės, kurių pagal C dalį buvo imtasi siekiant patenkinti reikalavimą, apibūdinamas įtariamas pažeidimas ir asmens nuožiūra pateikiami patvirtinamieji dokumentai, medžiaga ir (arba) su reikalavimu dėl įtariamo pažeidimo susijusių teisės aktų aiškinimas.

2. Bus parengtos procedūros, kuriomis siekiama užtikrinti, kad su tuo pačiu įtariamu pažeidimu susijusios asmens teisės nebūtų ginamos dvejopomis teisių gynimo priemonėmis arba procedūromis.

3. Lygiagrečiai su arbitražo procedūra gali vykti procesas FPK.

4. Tokiose arbitražo procedūrose negali dalyvauti JAV, ES ar bet kurios ES valstybės narės arba bet kurios kitos valstybinės institucijos, valdžios institucijos arba vykdymo užtikrinimo institucijos atstovai, jeigu ES asmens prašymu DAI gali padėti tik parengti pranešimą, tačiau DAI negali gauti galimybės susipažinti su nustatytais faktais ar su tomis arbitražo procedūromis susijusia bet kokia kita medžiaga.

5. Arbitražas vyks Jungtinėse Amerikos Valstijose, o asmuo gali nuspręsti dalyvauti naudodamasis vaizdo konferencijos ar telefonijos priemonėmis, kurios jam suteikiamos nemokamai. Dalyvauti asmeniškai nereikalaujama.

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 posėdyje paslaugos ir arbitražo medžiagos vertimo raštu paslaugos, nebent ES ir JAV duomenų privatumo sistemos kolegija nustatytų, kad konkrečios arbitražo procedūros aplinkybėmis dėl to susidarytų nepagrįstų ar neproporcingų išlaidų.

7. Arbitrai jiems pateiktą medžiagą traktuoja kaip konfidencialią ir naudoja tik tiek, kiek ji susijusi su arbitražu.

8. Prireikus gali būti leidžiama susipažinti su faktais apie konkretų asmenį, o tokią informaciją šalys traktuos kaip konfidencialią ir naudos tik tiek, kiek ji susijusi su arbitražu.

9. Arbitražo procedūros turėtų būti baigiamos per 90 dienų nuo pranešimo įteikimo atitinkamai organizacijai dienos, nebent šalys susitarė kitaip.

([3]) Arbitražui pagal Principų I priedą administruoti ir Principų I priede nurodytam arbitražo fondui valdyti Departamentas pasirinko Tarptautinį ginčų sprendimo centrą (ICDR) – Amerikos arbitražo asociacijos (AAA) tarptautinį padalinį (toliau kartu – ICDR-AAA). 2017 m. rugsėjo 15 d. Departamentas ir Komisija susitarė priimti arbitražo taisykles, kuriomis būtų reglamentuojamas Principų I priede aprašytas privalomo arbitražo procesas, taip pat arbitrų elgesio kodeksą, kuris atitiktų visuotinai pripažintus prekybos arbitrų etikos standartus ir Principų I priedą. Departamentas ir Komisija susitarė pritaikyti arbitražo taisykles ir elgesio kodeksą, kad būtų atsižvelgta į atnaujintas ES ir JAV DPS nuostatas, o Departamentas bendradarbiaudamas su ICDR-AAA užtikrins, kad šie atnaujinimai būtų įdiegti.

H. **Išlaidos**

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

Departamentas, laikydamasis taikomų teisės aktų, sudarys palankesnes sąlygas išlaikyti fondą, į kurį sistemoje dalyvaujančios organizacijos turės mokėti įnašus, kurie iš dalies atitiks organizacijos dydį ir iš kurių bus padengiamos arbitražo išlaidos, įskaitant arbitrų atlygį, neviršijant maksimalių sumų (viršutinių ribų). Fondą valdys trečioji šalis; ji Departamentui reguliariai teiks fondo veiklos ataskaitas. Bendradarbiaudamas su ta trečiąja šalimi, Departamentas periodiškai tikrins, kaip veikia fondas, įskaitant tai, ar reikia patikslinti įnašų ar arbitražo išlaidų viršutinių ribų dydį, ir, be kita ko, atsižvelgs į arbitražo procesų skaičių, išlaidas ir trukmę stengdamasis, kad sistemoje dalyvaujančioms organizacijoms nebūtų užkrauta pernelyg didelė finansinė našta. Departamentas praneš Komisijai apie kartu su trečiąja šalimi atliktų tokių peržiūrų rezultatus ir iš anksto informuos Komisiją apie bet kokius įnašų sumos pakeitimus. Advokatų atlygiui ši nuostata netaikoma ir tokios išlaidos iš bet kurio pagal šią nuostatą įsteigto fondo nedengiamos.

II PRIEDAS

JUNGTINIŲ VALSTIJŲ PREKYBOS DEPARTAMENTAS
Prekybos sekretorius
Vašingtonas, DC 20230

2023 m. liepos 6 d.

Didier Reyndersui
Už teisingumą atsakingam Komisijos nariui
Europos Komisija
Rue de la Loi / Westraat 200
1049 Briuselis
Belgija

Gerbiamas Komisijos nary D. Reyndersai,

Jungtinių Amerikos Valstijų vardu perduodu ES ir JAV duomenų privatumo sistemos medžiagos rinkinį, kuris kartu su Vykdomuoju potvarkiu Nr. 14086 dėl Jungtinių Amerikos Valstijų signalų žvalgybos veiklos apsaugos priemonių griežtinimo ir Federalinių reglamentų kodekso 28 antraštinės dalies 201 dalimi, kuria iš dalies keičiant Teisingumo departamento reglamentus įsteigiamas Duomenų apsaugos apeliacinis teismas, atspindi reikšmingas ir išsamias derybas dėl privatumo ir piliečių laisvių apsaugos stiprinimo. Šių derybų rezultatas – naujos apsaugos priemonės, kuriomis siekiama užtikrinti, kad JAV signalų žvalgybos veikla būtų būtina ir proporcinga siekiant nustatytų nacionalinio saugumo tikslų, irnaujas mechanizmas, pagal kurį Europos Sąjungos (ES) asmenys galėtų ginti savo teises, jei mano, kad jų atžvilgiu neteisėtai vykdoma signalų žvalgybos veikla, – abi šios priemonės kartu užtikrins ES asmens duomenų privatumą. Remiantis ES ir JAV duomenų privatumo sistema bus plėtojama įtrauki ir konkurencinga skaitmeninė ekonomika. Kartu turėtume didžiuotis toje sistemoje įdiegtais patobulinimais, kurie sustiprins privatumo apsaugą visame pasaulyje. Šiuo dokumentų rinkiniu, kartu su Vykdomuoju potvarkiu, reglamentais ir kita iš viešų šaltinių prieinama informacija, Europos Komisija gali itin tvirtai remtis priimdama naują išvadą dėl tinkamumo ([1]).

Pridedama ši medžiaga:

— ES ir JAV duomenų privatumo sistemos principai, įskaitant papildomus principus (toliau kartu – Principai), ir Principų I priedas (t. y. priedas, kuriame nustatytos sąlygos, kuriomis Duomenų privatumo sistemos organizacijos privalo arbitražo tvarka spręsti su tam tikrais neįvykdytais reikalavimais susijusius klausimus dėl asmens duomenų, kuriems taikomi Principai);

— Duomenų privatumo sistemos programą administruojančios Departamento Tarptautinės prekybos administracijos raštas, kuriame aprašomi mūsų Departamento prisiimti įsipareigojimai užtikrinti veiksmingą ES ir JAV duomenų privatumo sistemos veikimą;

— Federalinės prekybos komisijos raštas, kuriame aprašoma, kaip ji užtikrins, kad būtų laikomasi Principų;

— Transporto departamento raštas, kuriame aprašoma, kaip jis užtikrins, kad būtų laikomasi Principų;

— Nacionalinės žvalgybos direktoriaus tarnybos parengtas raštas dėl JAV nacionalinio saugumo institucijoms taikomų apsaugos priemonių ir apribojimų, taip pat

— Teisingumo departamento parengtas raštas dėl JAV vyriausybei taikomų apsaugos priemonių ir apribojimų leidžiant susipažinti su duomenimis teisėsaugos ir viešojo intereso tikslais.

([1]) Kadangi Komisijos sprendimas dėl ES ir JAV duomenų privatumo sistemos užtikrinamos apsaugos tinkamumo taip pat taikomas Islandijai, Lichtenšteinui ir Norvegijai, ES ir JAV duomenų privatumo sistemos dokumentų rinkinys bus taikomas tiek Europos Sąjungai, tiek šioms trims šalims.

Visas ES ir JAV duomenų privatumo sistemos dokumentų rinkinys bus skelbiamas Departamento Duomenų privatumo sistemos interneto svetainėje, o Principai ir Principų I priedas įsigalios Europos Komisijos sprendimo dėl tinkamumo įsigaliojimo dieną.

Patikinu, kad Jungtinės Amerikos Valstijos šiuos įsipareigojimus vertina rimtai. Džiaugiamės galėdami su Jumis bendradarbiauti diegiant ES ir JAV duomenų privatumo sistemą ir kartu pereiti į kitą šio proceso etapą.

Pagarbiai

Gina M. RAIMONDO

III PRIEDAS

UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

2022 m. gruodžio 12 d.

Didier Reyndersui
Už teisingumą atsakingam Komisijos nariui
Europos Komisija
Rue de la Loi / Westraat 200
1049 Briuselis
Belgija

Gerbiamas Komisijos nary D. Reyndersai,

džiaugiuosi galėdama Tarptautinės prekybos administracijos (toliau – TPA) vardu pristatyti Prekybos departamento (toliau – Departamentas) prisiimtus įsipareigojimus užtikrinti asmens duomenų apsaugą administruojant ir prižiūrint Duomenų privatumo sistemos programą. Tai, kad galiausiai buvo sukurta ES ir JAV duomenų privatumo sistema (toliau – ES ir JAV DPS), yra svarbus pasiekimas privatumo srityje ir įmonėms abiejuose Atlanto vandenyno krantuose, nes taip ES asmenys galės tvirčiau pasitikėti, kad jų duomenys bus apsaugoti ir kad jie turės teisinių teisių gynimo priemonių su jų duomenimis susijusiems susirūpinimą keliantiems klausimams spręsti, o tūkstančiams įmonių bus sudarytos sąlygos toliau investuoti ir kitaip verstis prekyba ir komercine veikla per Atlanto vandenyną atitinkamai nešant naudą mūsų ekonomikai ir piliečiams. ES ir JAV DPS sukurta daug metų sunkiai dirbus ir bendradarbiavus su Jumis ir Jūsų kolegomis Europos Komisijoje (toliau – Komisija). Tikimės ir toliau bendradarbiauti su Komisija, kad šis bendro darbo rezultatas veiktų tinkamai.

ES ir JAV DPS asmenims ir įmonėms bus išties naudinga. Pirma, šioje sistemoje nustatytas svarbus į Jungtines Amerikos Valstijas perduodamų ES asmenų duomenų privatumo apsaugos priemonių rinkinys. Pagal jį reikalaujama, kad sistemoje dalyvaujančios JAV organizacijos parengtų atitinkamą privatumo politiką; viešai įsipareigotų laikytis ES ir JAV duomenų privatumo sistemos principų, įskaitant papildomus principus (toliau kartu – Principai), ir Principų I priedo (t. y. priedo, kuriame nustatytos sąlygos, kuriomis ES ir JAV DPS organizacijos privalo arbitražo tvarka spręsti su tam tikrais neįvykdytais reikalavimais susijusius klausimus dėl asmens duomenų, kuriems taikomi Principai), kad įsipareigojimas taptų vykdytinas pagal JAV teisę ([1]); kasmet vykdydamos pakartotinį sertifikavimą Departamentui patvirtintų, kad laikosi reikalavimų; ES asmenims užtikrintų nemokamą ir nepriklausomą ginčų sprendimą; kad joms galiotų Principų dokumente nurodytos JAV valstybinės įstaigos (pvz., Federalinės prekybos komisijos (FPK) ir Transporto departamento) arba būsimame Principų priede nurodytos valstybinės įstaigos tyrimo ir vykdymo užtikrinimo įgaliojimai. Nors organizacija sprendimą atlikti savarankišką sertifikavimą priima savo noru, kai organizacija viešai įsipareigoja dalyvauti ES ir JAV DPS, jos įsipareigojimo vykdymą pagal JAV teisę užtikrina FPK, Transporto departamentas arba kita JAV valstybinė įstaiga, priklausomai nuo to, kurios įstaigos jurisdikcijai priklauso sistemoje dalyvaujanti organizacija. Antra, pagal ES ir JAV DPS įmonės Jungtinėse Amerikos Valstijose, įskaitant Jungtinėse Amerikos Valstijose įsikūrusias Europos įmonių patronuojamąsias įmones, galės iš Europos Sąjungos gauti asmens duomenis, kad būtų sudarytos palankesnės sąlygos

([1]) Organizacijos, kurios atlikdamos savarankišką sertifikavimą yra patvirtinusios savo įsipareigojimą laikytis ES ir JAV privatumo skydo sistemos principų ir nori naudotis dalyvavimo ES ir JAV DPS teikiamais privalumais, privalo laikytis ES ir JAV duomenų privatumo sistemos principų. Šis įsipareigojimas laikytis ES ir JAV duomenų privatumo sistemos principų kuo greičiau ir bet kuriuo atveju ne vėliau kaip per tris mėnesius nuo ES ir JAV duomenų privatumo sistemos principų įsigaliojimo dienos turi būti įtrauktas į tokių sistemoje dalyvaujančių organizacijų privatumo politiką. (Žr. papildomo savarankiško sertifikavimo principo e punktą).

duomenų srautams, kuriais remiasi transatlantinė prekyba. Duomenų srautai tarp Jungtinių Amerikos Valstijų ir Europos Sąjungos yra didžiausi pasaulyje, be to, jais grindžiami 7,1 trln. JAV dolerių vertės JAV ir ES ekonominiai santykiai, kuriais remiasi milijonai darbo vietų abiejuose Atlanto krantuose. Transatlantiniais duomenų srautais naudojasi visų pramonės sektorių įmonės, įskaitant didžiausias „Fortune 500“ bendroves, taip pat daug mažųjų ir vidutinių įmonių. Dėl transatlantinių duomenų srautų JAV organizacijos gali tvarkyti duomenis, kurių reikia asmenims Europoje siūlant prekes, paslaugas ir galimybes įsidarbinti.

Siekdamas veiksmingai administruoti ir prižiūrėti Duomenų privatumo sistemos programą, Departamentas yra įsipareigojęs glaudžiai ir našiai bendradarbiauti su kolegomis iš ES. Šis įsipareigojimas vykdomas Departamente kuriant ir nuolat tobulinant įvairius išteklius, skirtus padėti organizacijoms vykdyti savarankiško sertifikavimo procesą, sukuriant interneto svetainę, kurioje suinteresuotiesiems subjektams būtų teikiama tikslinė informacija, bendradarbiaujant su Komisija ir Europos duomenų apsaugos institucijomis (DAI), kad būtų parengtos gairės, kuriose paaiškinami svarbūs ES ir JAV DPS elementai, vykdant informavimo veiklą, kuria siekiama sudaryti palankesnes sąlygas geriau suprasti organizacijų duomenų apsaugos prievoles, ir prižiūrinti bei stebint, kaip organizacijos laikosi programos reikalavimų.

Mums toliau bendradarbiaujant su gerbiamais ES kolegomis Departamentas galės užtikrinti, kad ES ir JAV DPS veiktų veiksmingai. Jungtinių Amerikos Valstijų vyriausybė jau seniai bendradarbiaudama su Komisija skatina laikytis bendrų duomenų apsaugos principų, stengiasi sumažinti atitinkamų mūsų teisinių požiūrių skirtumus ir kartu skatina prekybą ir ekonomikos augimą Europos Sąjungoje ir Jungtinėse Amerikos Valstijose. Manome, kad dėl ES ir JAV DPS, kaip šio bendradarbiavimo pavyzdžio, Komisija galės priimti naują sprendimą dėl tinkamumo, kuriuo organizacijoms bus leidžiama naudojantis ES ir JAV DPS perduoti asmens duomenims iš Europos Sąjungos į Jungtines Amerikos Valstijas laikantis ES teisės.

Prekybos departamento vykdomas Duomenų privatumo sistemos programos administravimas ir priežiūra

Departamentas yra tvirtai įsipareigojęs veiksmingai administruoti ir prižiūrėti Duomenų privatumo sistemos programą ir dės deramas pastangas bei skirs pakankamai išteklių tokiam rezultatui užtikrinti. Departamentas tvarkys ir viešai skelbs patikimą sąrašą, į kurį bus įtrauktos JAV organizacijos, kurios atliko savarankišką sertifikavimą ir Departamentui patvirtino savo įsipareigojimą laikytis Principų (toliau – Duomenų privatumo sistemos sąrašas), ir tą sąrašą atnaujins remdamasis sistemoje dalyvaujančių organizacijų kasmet teikiamais pakartotinio sertifikavimo dokumentais ir pašalindamas organizacijas, kai jos savo noru pasitrauks iš sistemos, neatliks metinio pakartotinio sertifikavimo pagal Departamento procedūras arba bus nustatyta, kad jos nuolat nesilaiko reikalavimų. Departamentas taip pat tvarkys ir viešai skelbs patikimą registrą, kuriame bus nurodytos iš Duomenų privatumo sistemos sąrašo pašalintos JAV organizacijos, ir nurodys kiekvienos organizacijos pašalinimo priežastį. Su nurodytaisiais patikimais sąrašu ir registru visuomenė galės susipažinti Departamento Duomenų privatumo sistemos svetainėje. Duomenų privatumo sistemos interneto svetainėje gerai matomoje vietoje bus pateiktas paaiškinimas, kad iš Duomenų privatumo sistemos sąrašo išbraukta organizacija privalo liautis teigusi, kad dalyvauja ES ir JAV DPS arba atitinka jos reikalavimus ir kad gali gauti asmeninę informaciją pagal ES ir JAV DPS. Vis dėlto tokia organizacija privalo ir toliau taikyti Principus asmeninei informacijai, kurią gavo dalyvaudama ES ir JAV DPS tol, kol saugo tokią informaciją. Departamentas, vykdydamas savo bendrą nuolatinį įsipareigojimą veiksmingai administruoti ir prižiūrėti Duomenų privatumo sistemos programą, visų pirma įsipareigoja vykdyti toliau nurodytus veiksmus.

Tikrinti, kaip laikomasi savarankiško sertifikavimo reikalavimų

— Prieš baigdamas organizacijos pradinį savarankišką sertifikavimą arba metinį pakartotinį sertifikavimą (toliau kartu – savarankiškas sertifikavimas) ir organizaciją įtraukdamas į Duomenų privatumo sistemos sąrašą arba neišbraukdamas iš jo, Departamentas patikrins, ar organizacija laikosi bent atitinkamų papildomo savarankiško sertifikavimo principo reikalavimų dėl informacijos, kurią organizacija privalo pateikti Departamentui teikiamuose savarankiško sertifikavimo dokumentuose, ir ar laiku nustatė atitinkamą privatumo politiką, pagal kurią asmenys informuojami apie visus 13 pagal pranešimo principą nurodytų elementų. Departamentas patikrins, ar organizacija:

— nurodė organizaciją, kuri teikia savo savarankiško sertifikavimo dokumentus, taip pat visus savarankišką sertifikavimą atliekančios organizacijos JAV subjektus arba JAV patronuojamąsias įmones, kurie taip pat laikosi Principų ir kuriems, organizacijos pageidavimu, taip pat būtų taikomas savarankiškas sertifikavimas;

— pateikė reikalaujamą organizacijos kontaktinę informaciją (pvz., savarankišką sertifikavimą atliekančioje organizacijoje dirbančio (-ių) už skundų, prašymų susipažinti su duomenimis ir kitų su ES ir JAV DPS susijusių klausimų nagrinėjimą atsakingo (-ų) konkretaus (-ių) asmens (-ų) ir (arba) tarnybos (-ų) kontaktinę informaciją);

— apibūdino tikslą (-us), kuriuo (-iais) organizacija rinks ir naudos iš Europos Sąjungos gaunamą asmeninę informaciją;

— nurodė, kokia asmeninė informacija būtų gaunama iš Europos Sąjungos pagal ES ir JAV DPS, taigi tokiai informacijai būtų taikomas jos savarankiškas sertifikavimas;

— jeigu organizacija turi viešą interneto svetainę, nurodė svetainės adresą, kuriuo toje interneto svetainėje galima lengvai susipažinti su atitinkama privatumo politika, arba, jeigu organizacija viešos interneto svetainės neturi, Departamentui pateikė atitinkamos privatumo politikos dokumentų kopiją ir nurodė, kur su ta privatumo politika galėtų susipažinti poveikį patyrę asmenys (t. y. poveikį patyrę darbuotojai, jeigu atitinkama privatumo politika yra žmogiškųjų išteklių privatumo politika, arba visuomenė, jeigu atitinkama privatumo politika nėra žmogiškųjų išteklių privatumo politika);

— į savo atitinkamą privatumo politiką (t. y. iš pradžių tik į privatumo politikos projektą, pateikiamą kartu su dokumentais, jeigu dokumentai teikiami vykdant pradinį savarankišką sertifikavimą, arba į galutinius ir, kai taikoma, paskelbtus privatumo politikos dokumentus) laiku įtraukė pareiškimą, kad laikosi Principų, ir saitą į Departamento Duomenų privatumo sistemos interneto svetainę arba tos interneto svetainės adresą (pvz., pradžios tinklalapio arba Duomenų privatumo sistemos sąrašo tinklalapio);

— į savo atitinkamą privatumo politiką laiku įtraukė visus kitus 12 pagal pranešimo principą nurodytų elementų (pvz., galimybę poveikį patyrusiam ES asmeniui tam tikromis sąlygomis kreiptis dėl privalomo arbitražo, reikalavimą atskleisti asmeninę informaciją tenkinant teisėtus valdžios institucijų prašymus, be kita ko, laikantis nacionalinio saugumo arba teisėsaugos reikalavimų, ir savo atsakomybę toliau perduodant duomenis trečiosioms šalims);

— nurodė konkrečią valstybinę įstaigą, turinčią jurisdikciją nagrinėti visus skundus dėl organizacijos galimos nesąžiningos ar apgaulingos veiklos ir privatumo klausimus reglamentuojančių įstatymų ar teisės aktų pažeidimų (kai šie teisės aktai ar reglamentai yra įtraukti į Principus arba būsimą Principų priedą);

— nurodė privatumo užtikrinimo programas, kurioje dalyvauja organizacija;

— nurodė, ar siekiant patikrinti, kaip laikomasi Principų, taikomas metodas (t. y. paskesnės procedūros, kurias organizacija turi nustatyti), yra įsivertinimas (t. y. vidinis patikrinimas), ar išorinė reikalavimų laikymosi peržiūra (t. y. trečiosios šalies atliekamas patikrinimas), o jeigu nurodė, kad atitinkamas metodas yra išorinė reikalavimų laikymosi peržiūra, taip pat nurodė tą peržiūrą atlikusią trečiąją šalį;

— nurodė atitinkamą nepriklausomą teisių gynimo mechanizmą, kuris gali būti naudojamas pagal Principus pateiktiems skundams nagrinėti ir tam, kad poveikį patyrusiam asmeniui būtų suteikta tinkama nemokama teisių gynimo priemonė.

— Jeigu organizacija pasirinko nepriklausomą teisių gynimo mechanizmą, kurį teikia privačiojo sektoriaus alternatyvaus ginčų sprendimo įstaiga, ji į savo atitinkamos privatumo politikos dokumentus įtraukė saitą į atitinkamą to mechanizmo, kuris gali būti taikomas pagal Principus pateiktiems neišspręstiems skundams nagrinėti, interneto svetainę arba skundo pateikimo formą arba nurodė tos interneto svetainės ar formos adresą.

— Jeigu organizacija privalo (t. y. dėl žmogiškųjų išteklių duomenų, perduodamų iš Europos Sąjungos darbo santykių aplinkybėmis) arba nusprendė bendradarbiauti su atitinkamomis DAI nagrinėjant ir sprendžiant pagal Principus pateiktus skundus, ji pareiškė esanti įsipareigojusi bendradarbiauti su DAI ir laikytis susijusių jų rekomendacijų imtis konkrečių veiksmų, kad būtų laikomasi Principų.

— Departamentas taip pat patikrins, ar organizacijos pateikti savarankiško sertifikavimo dokumentai atitinka susijusią jos privatumo politiką. Jeigu savarankišką sertifikavimą vykdanti organizacija nori įtraukti savo JAV subjektą arba JAV patronuojamąją įmonę, kuris (-i) taiko atskirą atitinkamą privatumo politiką, Departamentas taip pat peržiūrės atitinkamą tokių įtraukiamų subjektų arba patronuojamųjų įmonių privatumo politiką siekdamas užtikrinti, kad į ją būtų įtraukti visi pagal pranešimo principą reikalaujami elementai.

— Departamentas, bendradarbiaudamas su valstybinėmis įstaigomis (pvz., FPK ir Transporto departamentu) patikrins, ar organizacijos priklauso jų savarankiško sertifikavimo dokumentuose nurodytos atitinkamos valstybinės įstaigos jurisdikcijai, jeigu Departamentas turi priežasčių abejoti, kad jos priklauso tai jurisdikcijai.

— Departamentas, bendradarbiaudamas su privačiojo sektoriaus alternatyvaus ginčų sprendimo įstaigomis, patikrins, ar organizacijos yra aktyviai užsiregistravusios naudotis jų savarankiško sertifikavimo dokumentuose nurodytu nepriklausomu teisių gynimo mechanizmu, taip pat bendradarbiaudamas su tomis institucijomis patikrins, ar organizacijos yra aktyviai užsiregistravusios, kad būtų atlikta jų savarankiško sertifikavimo dokumentuose nurodyta išorinė reikalavimų laikymosi peržiūra, jeigu tokios institucijos gali teikti abiejų rūšių paslaugas.

— Departamentas, bendradarbiaudamas su Departamento pasirinkta trečiąja šalimi, kuri veiks kaip iš DAI kolegijos mokesčio (t. y. metinio mokesčio, skirto DAI kolegijos veiklos išlaidoms padengti) surinktų lėšų saugotoja, patikrins, ar organizacijos, kaip atitinkamą nepriklausomą teisių gynimo mechanizmą nurodžiusios DAI, sumokėjo tą mokestį už atitinkamus metus.

— Departamentas, bendradarbiaudamas su Departamento pasirinkta trečiąja šalimi, kuri pagal Principų I priedą administruos arbitražą ir valdys Principų I priede nurodytą arbitražo fondą, patikrins, ar organizacijos sumokėjo įnašus į tą arbitražo fondą.

— Jeigu peržiūrėdamas organizacijų pateiktus savarankiško sertifikavimo dokumentus nustato problemų, Departamentas organizacijas informuos, kad per Departamento nustatytą atitinkamą terminą jos turi išspręsti visas tas problemas ([2]). Departamentas taip pat jas informuos, kad per Departamento nustatytus terminus nepateikus atsakymo arba dėl kitų priežasčių pagal Departamento procedūras nebaigus savarankiško sertifikavimo, bus laikoma, kad to savarankiško sertifikavimo proceso atsisakoma ir kad dėl bet kokio klaidingo faktų pateikimo apie organizacijos dalyvavimą ES ir JAV DPS ar šios sistemos reikalavimų laikymąsi FPK, Transporto departamentas ar kita atitinkama valstybinė įstaiga gali imtis vykdymo užtikrinimo veiksmų. Departamentas organizacijas informuos naudodamasis organizacijų Departamentui nurodytomis ryšių palaikymo priemonėmis.

Sudaryti palankesnes sąlygas bendradarbiauti su alternatyvaus ginčų sprendimo įstaigomis, teikiančiomis su Principais susijusias paslaugas

— Departamentas, bendradarbiaudamas su privačiojo sektoriaus alternatyvaus ginčų sprendimo įstaigomis, teikiančiomis nepriklausomus teisių gynimo mechanizmus, kuriais galima naudotis nagrinėjant neišspręstus pagal Principus pateiktus skundus, patikrins, ar jos atitinka bent pagal papildomą ginčų sprendimo ir vykdymo užtikrinimo principą nustatytus reikalavimus. Departamentas patikrins, ar jos:

  — savo viešose interneto svetainėse pateikia informacijos apie Principus ir pagal ES ir JAV DPS savo teikiamas paslaugas, kuri turi apimti: 1) informaciją apie nepriklausomiems teisių gynimo mechanizmams pagal Principus taikomus reikalavimus arba saitą į tokius reikalavimus; 2) saitą į Departamento Duomenų privatumo sistemos interneto svetainę; 3) paaiškinimą, kad jų ginčų sprendimo paslaugos pagal ES ir JAV DPS asmenims teikiamos nemokamai; 4) aprašymą, kaip galima pateikti su Principais susijusį skundą; 5) terminus, per kuriuos išnagrinėjami su Principais susiję skundai; 6) galimų taisomųjų priemonių aprašymą. Departamentas institucijoms laiku praneš apie esminius Departamento vykdomos Duomenų privatumo sistemos programos priežiūros ir administravimo pakeitimus, kai tokie pakeitimai netrukus bus padaryti arba jau yra padaryti ir yra susiję su institucijų vaidmeniu pagal ES ir JAV DPS;

([2]) Pavyzdžiui, numatoma, kad vykdydamos pakartotinį sertifikavimą organizacijos visas tokias problemas išspręs per 45 dienas, nebent Departamentas nustato kitą tinkamą terminą.

— skelbia metinę ataskaitą, kurioje pateikiami apibendrinti statistiniai duomenys apie jų teikiamas ginčų sprendimo paslaugas ir turi būti nurodyta: 1) bendras per ataskaitinius metus gautų su Principais susijusių skundų skaičius; 2) gautų skundų rūšys; 3) ginčų sprendimo kokybės užtikrinimo priemonės, pvz., skundų nagrinėjimo trukmė; 4) gautų skundų nagrinėjimo rezultatai, visų pirma taikytų teisių gynimo priemonių ar sankcijų skaičius ir rūšys. Departamentas institucijoms teiks konkrečias papildomas gaires, kokią informaciją jos turėtų pateikti tose metinėse ataskaitose, ir išsamiau apibūdins tuos reikalavimus (pvz., išvardys konkrečius kriterijus, kuriuos turi atitikti skundas, kad teikiant metinę ataskaitą jį būtų galima laikyti susijusiu su Principais), taip pat nustatys kitų rūšių informaciją, kurią reikėtų pateikti (pvz., jeigu institucija taip pat teikia su Principais susijusią tikrinimo paslaugą, aprašymą, kaip institucija vengia bet kokių faktinių ar galimų interesų konfliktų tais atvejais, kai organizacijai teikia ir tikrinimo paslaugas, ir ginčų sprendimo paslaugas). Departamento teikiamose papildomose gairėse taip pat bus nurodyta data, iki kurios turėtų būti paskelbtos institucijų metinės ataskaitos už atitinkamą ataskaitinį laikotarpį.

Dirbti su organizacijomis, kurios nori būti arba yra išbrauktos iš Duomenų privatumo sistemos sąrašo

— Jeigu organizacija nori pasitraukti iš ES ir JAV DPS, Departamentas pareikalaus, kad organizacija iš susijusios privatumo politikos pašalintų visas nuorodas į ES ir JAV DPS, iš kurių galima suprasti, kad organizacija toliau dalyvauja ES ir JAV DPS ir gali gauti asmens duomenis pagal ES ir JAV DPS (žr. Departamento įsipareigojimo vykdyti neteisingų teiginių apie dalyvavimą paiešką aprašymą). Departamentas taip pat pareikalaus, kad organizacija užpildytų ir pateiktų Departamentui atitinkamą klausimyną, kad būtų galima patikrinti:

  — ar ji nori pasitraukti;

  — ką ji darys su asmens duomenimis, kuriuos gavo pagal ES ir JAV DPS, kol dalyvavo šioje sistemoje: a) saugos tokius duomenis, tokiems duomenims toliau taikys Principus ir kasmet Departamentui patvirtins savo įsipareigojimą tokiems duomenims taikyti Principus; b) saugos tokius duomenis ir užtikrins „tinkamą“ tokių duomenų apsaugą kitomis leidžiamomis priemonėmis ar c) iki nurodytos datos grąžins arba ištrins visus tokius duomenis; taip pat

  — kas organizacijoje veiks kaip nuolatinis kontaktinis centras su Principais susijusiais klausimais.

— Jeigu organizacija pasirinko a punkte nurodytą galimybę, Departamentas taip pat pareikalaus, kad ji užpildytų ir kasmet po pasitraukimo (t. y. kol sueis pirmi metai po pasitraukimo, taip pat kol sueis kiekvieni vėlesni metai, nebent organizacija užtikrina „tinkamą“ tokių duomenų apsaugą kitomis leidžiamomis priemonėmis ir tol, kol ji tai daro, arba grąžina ar ištrina visus tokius duomenis ir praneša Departamentui apie šį veiksmą) Departamentui pateiktų atitinkamą klausimyną, kad būtų galima patikrinti, ką ji padarė su tais asmens duomenimis, ką ji darys su išsaugotais asmens duomenimis ir kas organizacijoje veiks kaip nuolatinis kontaktinis centras su Principais susijusiais klausimais.

— Jeigu organizacija leido pasibaigti jos savarankiško sertifikavimo galiojimui (t. y. kasmet atlikdama pakartotinį sertifikavimą nepatvirtino, kad laikosi Principų, ir nebuvo išbraukta iš Duomenų privatumo sistemos sąrašo dėl bet kurios kitos priežasties, pvz., pasitraukimo), Departamentas nurodys jai užpildyti ir Departamentui pateikti atitinkamą klausimyną, kad būtų galima patikrinti, ar ji nori pasitraukti iš sistemos, ar atlikti pakartotinį sertifikavimą:

  — jeigu organizacija nori pasitraukti, papildomai patikrinti, ką ji darys su asmens duomenimis, kuriuos gavo pagal ES ir JAV DPS, kol dalyvavo šioje sistemoje (žr. ankstesnį aprašymą, ką organizacija privalo patikrinti, jeigu nori pasitraukti iš sistemos);

  — jeigu organizacija ketina atlikti pakartotinį sertifikavimą, papildomai patikrinti, ar baigus galioti sertifikavimo statusui ji taikė Principus pagal ES ir JAV DPS gautiems asmens duomenims, ir išsiaiškinti, kokių priemonių imsis, kad išspręstų neišspręstus klausimus, dėl kurių uždelsė atlikti pakartotinį sertifikavimą.

— Jeigu organizacija išbraukiama iš Duomenų privatumo sistemos sąrašo dėl bet kurios iš šių priežasčių: a) ji pasitraukė iš ES ir JAV DPS, b) ji neatliko metinio pakartotinio sertifikavimo ir nepatvirtino, kad laikosi Principų (t. y. pradėjo metinio pakartotinio sertifikavimo procesą, bet jo laiku neužbaigė, arba to proceso net nepradėjo), arba c) ji nuolat nesilaiko reikalavimų, Departamentas organizacijos savarankiško sertifikavimo dokumentuose nurodytam (-iems) kontaktiniam (-iams) asmeniui (-ims) nusiųs pranešimą, kuriame nurodys išbraukimo priežastį ir paaiškins, kad organizacija privalo liautis tiesiogiai ar numanomai teigusi, kad dalyvauja ES ir JAV DPS arba atitinka jos reikalavimus ir gali gauti asmens duomenis pagal ES ir JAV DPS. Pranešime, kuriame taip pat gali būti pateikiama išbraukimo priežastį atitinkančio kito turinio, bus nurodyta, kad kai organizacijų, kurios klaidingai nurodo faktus apie dalyvavimą ES ir JAV DPS arba jos reikalavimų laikymąsi, be kita ko, teigdamos, kad dalyvauja ES ir JAV DPS po to, kai buvo išbrauktos iš Duomenų privatumo sistemos sąrašo, atžvilgiu FPK, Transporto departamentas ar kita atitinkama valstybinė įstaiga gali imtis vykdymo užtikrinimo veiksmų.

Atlikti neteisingų teiginių apie dalyvavimą paiešką ir šalinti tokius teiginius

— Reguliariai, kai organizacija: a) nustoja dalyvauti ES ir JAV DPS, b) neatlieka metinio pakartotinio sertifikavimo ir nepatvirtina, kad laikosi Principų (t. y. pradeda metinio pakartotinio sertifikavimo procesą, bet jo laiku neužbaigia, arba to proceso net nepradeda), c) kaip dalyvė pašalinama iš ES ir JAV DPS visų pirma dėl „nuolatinio reikalavimų nesilaikymo“ arba d) neatlieka pradinio savarankiško sertifikavimo ir nepatvirtina, kad laikosi Principų (t. y. pradeda pradinio savarankiško sertifikavimo procesą, bet jo laiku neužbaigia), Departamentas nuolat *ex officio* imsis veiksmų, kad patikrintų, ar organizacijos atitinkamos paskelbtos privatumo politikos dokumentuose nėra nuorodų į ES ir JAV DPS, iš kurių būtų galima suprasti, kad organizacija dalyvauja ES ir JAV DPS ir gali gauti asmens duomenis pagal ES ir JAV DPS. Radęs tokių nuorodų, Departamentas informuos organizaciją, kad prireikus perduos šį klausimą atitinkamai agentūrai, kad ši imtųsi galimų vykdymo užtikrinimo veiksmų, jeigu organizacija ir toliau klaidingai nurodys dalyvaujanti ES ir JAV DPS. Departamentas organizaciją informuos naudodamasis organizacijos Departamentui nurodytomis ryšių palaikymo priemonėmis arba, prireikus, kitomis tinkamomis priemonėmis. Jeigu organizacija Departamento nustatyta tvarka nepašalina nuorodų ir atlikdama savarankišką sertifikavimą nepatvirtina, kad laikosi reikalavimų pagal ES ir JAV DPS, Departamentas *ex officio* perduoda klausimą FPK, Transporto departamentui ar kitai atitinkamai vykdymo užtikrinimo agentūrai arba imasi kitų tinkamų veiksmų siekdamas užtikrinti, kad ES ir JAV DPS sertifikavimo ženklas būtų naudojamas tinkamai;

— Departamentas imsis kitų priemonių, kad nustatytų neteisingus teiginius apie dalyvavimą ES ir JAV DPS ir netinkamą ES ir JAV DPS sertifikavimo ženklo naudojimą, be kita ko, organizacijų, kurios, priešingai nei pirmiau aprašytos organizacijos, niekada net nebuvo pradėjusios savarankiško sertifikavimo proceso (pvz., atliks atitinkamas paieškas internete, kad nustatytų nuorodas į ES ir JAV DPS organizacijų privatumo politikoje). Jeigu vykdydamas tokią veiklą nustato neteisingus teiginius apie dalyvavimą ES ir JAV DPS ir netinkamą ES ir JAV DPS sertifikavimo ženklo naudojimą, Departamentas informuos organizaciją, kad prireikus perduos šį klausimą atitinkamai agentūrai, kad ši imtųsi galimų vykdymo užtikrinimo veiksmų, jeigu organizacija ir toliau klaidingai pateiks informaciją apie savo dalyvavimą ES ir JAV DPS. Departamentas organizaciją informuos naudodamasis organizacijos Departamentui nurodytomis ryšių palaikymo priemonėmis, jeigu yra, arba, prireikus, kitomis tinkamomis priemonėmis. Jeigu organizacija Departamento nustatyta tvarka nepašalina nuorodų ir atlikdama savarankišką sertifikavimą nepatvirtina, kad laikosi reikalavimų pagal ES ir JAV DPS, Departamentas *ex officio* perduoda klausimą FPK, Transporto departamentui ar kitai atitinkamai vykdymo užtikrinimo agentūrai arba imasi kitų tinkamų veiksmų siekdamas užtikrinti, kad ES ir JAV DPS sertifikavimo ženklas būtų naudojamas tinkamai;

— Departamentas nedelsdamas peržiūrės ir nagrinės Departamento gautus konkrečius ir pagrįstus skundus dėl neteisingų teiginių apie dalyvavimą ES ir JAV DPS (pvz., skundus, gautus iš DAI, pagal privačiojo sektoriaus alternatyvaus ginčų sprendimo įstaigų teikiamus nepriklausomus teisių gynimo mechanizmus, gautus iš duomenų subjektų, ES ir JAV įmonių ir kitokių trečiųjų šalių); taip pat

— Departamentas gali imtis kitų tinkamų taisomųjų veiksmų. Už klaidingą faktų pateikimą Departamentui gali būti taikomos sankcijos pagal Melagingų parodymų aktą (JAV kodekso 18 antraštinės dalies 1001 straipsnį).

Periodiškai *ex officio* atlikti Duomenų privatumo sistemos programos reikalavimų laikymosi peržiūras ir vertinimus

— Departamentas nuolat stengsis stebėti, kaip veiksmingai ES ir JAV DPS organizacijos laikosi reikalavimų, kad nustatytų problemas, dėl kurių gali reikėti imtis paskesnių veiksmų. Visų pirma Departamentas *ex officio* atliks įprastas atsitiktine tvarka atrinktų ES ir JAV DPS organizacijų patikras vietoje, taip pat tam tikrų ES ir JAV DPS organizacijų *ad hoc* patikras vietoje, kai bus nustatyta su reikalavimų laikymusi susijusių galimų trūkumų (pvz., su reikalavimų laikymusi susijusių galimų trūkumų, apie kuriuos Departamentui pranešė trečiosios šalys), kad patikrintų: a) ar veikia kontaktinis (-iai) centras (-ai), atsakingas (-i) už skundų, prašymų leisti susipažinti su duomenimis ir kitų su ES ir JAV DPS susijusių klausimų nagrinėjimą; b) jei taikoma, ar visuomenė gali lengvai susipažinti su visuomenei skirta organizacijos privatumo politika tiek organizacijos viešoje interneto svetainėje, tiek naudojantis saitu į Duomenų privatumo sistemos sąrašą; c) ar organizacijos privatumo politika ir toliau atitinka pagal Principus aprašytus savarankiško sertifikavimo reikalavimus; d) ar galima naudotis organizacijos nustatytu nepriklausomu teisių gynimo mechanizmu pagal ES ir JAV DPS pateiktiems skundams nagrinėti. Departamentas taip pat aktyviai stebės naujienas, ieškodamas pranešimų, kuriuose pateikiama patikimų įrodymų, kad ES ir JAV DPS organizacijos nesilaiko reikalavimų;

— atlikdamas reikalavimų laikymosi peržiūrą, Departamentas reikalaus, kad ES ir JAV DPS organizacija užpildytų ir pateiktų Departamentui išsamų klausimyną, kai: a) Departamentas gavo konkrečių pagrįstų skundų dėl to, kaip organizacija laikosi Principų, b) organizacija nepateikė tinkamo atsakymo į Departamento užklausas dėl informacijos, susijusios su ES ir JAV DPS, arba c) yra patikimų įrodymų, kad organizacija nesilaiko savo įsipareigojimų pagal ES ir JAV DPS. Departamentui išsiuntus tokį išsamų klausimyną organizacijai, o organizacijai tinkamai neatsakius į tą klausimyną, Departamentas informuos organizaciją, kad prireikus perduos šį klausimą atitinkamai agentūrai, kad ši imtųsi galimų vykdymo užtikrinimo veiksmų, jeigu Departamentas iš organizacijos laiku negaus tinkamo atsakymo. Departamentas organizaciją informuos naudodamasis organizacijos Departamentui nurodytomis ryšių palaikymo priemonėmis arba, prireikus, kitomis tinkamomis priemonėmis. Jeigu organizacija laiku nepateikia tinkamo atsakymo, Departamentas *ex officio* perduoda klausimą FPK, Transporto departamentui ar kitai atitinkamai vykdymo užtikrinimo agentūrai arba imasi kitų tinkamų veiksmų reikalavimų laikymuisi užtikrinti. Departamentas dėl tokių reikalavimų laikymosi peržiūrų prireikus konsultuojasi su kompetentingomis duomenų apsaugos institucijomis, taip pat

— Departamentas periodiškai vertins Duomenų privatumo sistemos programos administravimą ir priežiūrą siekdamas užtikrinti, kad jo stebėsenos pastangos, įskaitant pastangas, kurių imamasi naudojantis paieškos priemonėmis (pvz., tikrinant, ar nėra neveikiančių nuorodų į ES ir JAV DPS organizacijų privatumo politikos dokumentus), būtų tinkamos esamiems klausimams ir bet kokiems kylantiems naujiems klausimams spręsti.

Pritaikyti Duomenų privatumo sistemos interneto svetainę prie tikslinės auditorijos poreikių

Departamentas Duomenų privatumo sistemos interneto svetainę pritaikys taip, kad ji visų pirma būtų skirta šioms tikslinėms grupėms: ES asmenims, ES įmonėms, JAV įmonėms ir DAI. Pateikus tiesiogiai ES asmenims ir ES įmonėms skirtą medžiagą įvairiais aspektais bus lengviau užtikrinti skaidrumą. Interneto svetainėje ES asmenims bus tiksliai paaiškinama: 1) pagal ES ir JAV DPS ES asmenims suteikiamos teisės; 2) teisių gynimo mechanizmai, kuriais gali naudotis ES asmenys, jeigu mano, kad organizacija pažeidė savo įsipareigojimą laikytis Principų; 3) kaip rasti informacijos, susijusios su organizacijos ES ir JAV DPS savarankišku sertifikavimu. ES įmonėms interneto svetainėje bus lengviau patikrinti: 1) ar organizacija dalyvauja ES ir JAV DPS; 2) informacijos, kuriai taikomas organizacijos ES ir JAV DPS savarankiškas sertifikavimas, rūšį; 3) atitinkamai informacijai taikomą privatumo politiką; 4) metodą, kurį organizacija taiko siekdama patikrinti, kaip laikosi Principų. Interneto svetainėje JAV įmonėms bus tiksliai paaiškinama: 1) dalyvavimo ES ir JAV DPS nauda; 2) kaip prisijungti prie ES ir JAV DPS, taip pat kaip atlikti pakartotinį sertifikavimą arba pasitraukti iš ES ir JAV DPS; 3) kaip Jungtinės Amerikos Valstijos administruoja ES ir JAV DPS ir užtikrina vykdymą. Įtraukus tiesiogiai DAI skirtą medžiagą (pvz., informaciją apie Departamento specialiai DAI skirtą kontaktinį centrą ir saitą į FPK interneto svetainėje pateikiamą su Principais susijusį turinį) bus lengviau bendradarbiauti ir užtikrinti skaidrumą. Departamentas taip pat *ad hoc* pagrindu bendradarbiaudamas su Komisija ir Europos duomenų apsaugos valdyba (EDAV) parengs papildomos teminės medžiagos (pvz., atsakymus į dažnai užduodamus klausimus), kuri bus naudojama Duomenų privatumo sistemos interneto svetainėje, kur tokia informacija palengvintų veiksmingą Duomenų privatumo sistemos programos administravimą ir priežiūrą.

Sudaryti palankesnes sąlygas bendradarbiauti su DAI

Siekdamas sukurti daugiau galimybių bendradarbiauti su DAI, Departamentas įsteigs specialų kontaktinį centrą, kuris veiks kaip ryšių palaikymo su DAI institucija. Jeigu DAI mano, kad ES ir JAV DPS organizacija nesilaiko Principų, be kita ko, remdamasi iš ES asmens gautu skundu, ji turi galimybę kreiptis į specialų Departamento kontaktinį centrą, kad perduotų organizaciją tolesnei peržiūrai. Departamentas stengsis kuo labiau palengvinti skundų dėl ES ir JAV DPS organizacijos sprendimą. Per 90 dienų nuo skundo gavimo dienos Departamentas pateiks DAI naujausią informaciją. Specialiam kontaktiniam centrui taip pat bus perduodami klausimai dėl organizacijų, kurios neteisingai teigia, kad dalyvauja ES ir JAV DPS. Specialus kontaktinis centras seks visų iš DAI Departamento gautų klausimų nagrinėjimą, o Departamentas atlikęs toliau aprašytą bendrą peržiūrą pateiks ataskaitą, kurioje bus pristatyta apibendrinta kasmet gaunamų skundų analizė. Specialus kontaktinis centras padės DAI ieškoti informacijos, susijusios su konkrečios organizacijos savarankišku sertifikavimu arba ankstesniu dalyvavimu ES ir JAV DPS, be to, specialus kontaktinis centras atsakys į DAI užklausas dėl konkrečių ES ir JAV DPS reikalavimų įgyvendinimo. Departamentas taip pat bendradarbiaus su Komisija ir EDAV dėl procedūrinių ir administracinių DAI kolegijos klausimų, įskaitant tinkamų iš DAI kolegijos mokesčio surinktų lėšų paskirstymo procedūrų nustatymą. Manome, kad Komisija bendradarbiaus su Departamentu, kad būtų lengviau išspręsti visus su šiomis procedūromis susijusius klausimus. Be to, Departamentas teiks DAI medžiagą apie ES ir JAV DPS, kad ji būtų skelbiama pačių DAI interneto svetainėse siekiant didesnio skaidrumo ES asmenų ir ES įmonių atžvilgiu. Didesnis informuotumas apie ES ir JAV DPS ir pagal ją atsiradusias teises bei pareigas turėtų padėti lengviau nustatyti kylančias problemas ir tinkamai jas išspręsti.

Vykdyti savo įsipareigojimus pagal Principų I priedą

Departamentas vykdys savo įsipareigojimus pagal Principų I priedą, be kita ko, tvarkys sąrašą, į kurį bus įtraukti arbitrai, kartu su Komisija atrinkti atsižvelgiant į jų nepriklausomumą, sąžiningumą ir patirtį, taip pat prireikus rems trečiąją šalį, kurią Departamentas pasirinko pagal Principų I priedą administruoti arbitražui ir valdyti Principų I priede nurodytam arbitražo fondui ([3]). Departamentas, bendradarbiaudamas su trečiąja šalimi, be kita ko, patikrins, ar ta trečioji šalis turi interneto svetainę, kurioje pateikiamos arbitražo proceso gairės, į kurias įtraukiama: 1) informacija, kaip pradėti procesą ir pateikti dokumentus; 2) Departamento tvarkomas arbitrų sąrašas ir informacija, kaip iš to sąrašo pasirinkti arbitrus; 3) Departamento ir Komisijos priimtos pagrindinės arbitražo procedūros ir arbitrų elgesio kodeksas ([4]); 4) informacija apie arbitražo mokesčių surinkimą ir mokėjimą. Be to, bendradarbiaudamas su ta trečiąja šalimi, Departamentas periodiškai tikrins, kaip veikia arbitražo fondas, įskaitant tai, ar reikia patikslinti įnašų ar arbitražo išlaidų viršutinių ribų dydį (t. y. didžiausias sumas), ir, be kita ko, atsižvelgs į arbitražo procedūrų skaičių, išlaidas ir trukmę stengdamasis, kad ES ir JAV DPS organizacijoms nebūtų užkrauta pernelyg didelė finansinė našta. Departamentas praneš Komisijai apie kartu su trečiąja šalimi atliktų tokių peržiūrų rezultatus ir iš anksto informuos Komisiją apie bet kokius įnašų sumos pakeitimus.

Vykdyti bendras ES ir JAV DPS veikimo peržiūras

Departamentas ir, prireikus, kitos agentūros reguliariai rengs susitikimus su Komisija, suinteresuotomis DAI ir atitinkamais EDAV atstovais, o Departamentas juose teiks naujausią informaciją apie ES ir JAV DPS. Tokiuose susitikimuose bus aptariami esami klausimai, susiję su Duomenų privatumo sistemos programos veikimu, įgyvendinimu, priežiūra ir vykdymo užtikrinimu. Susitikimuose prireikus gali būti aptariamos susijusios temos, pvz., kiti duomenų perdavimo mechanizmai, kuriems taikomos pagal ES ir JAV DPS nustatytos apsaugos priemonės.

([3]) Arbitražui pagal Principų I priedą administruoti ir Principų I priede nurodytam arbitražo fondui valdyti Departamentas pasirinko Tarptautinį ginčų sprendimo centrą (ICDR) – Amerikos arbitražo asociacijos (AAA) tarptautinį padalinį (toliau kartu – ICDR-AAA).

([4]) 2017 m. rugsėjo 15 d. Departamentas ir Komisija susitarė priimti arbitražo taisykles, kuriomis būtų reglamentuojamas Principų I priede aprašytas privalomo arbitražo procesas, taip pat arbitrų elgesio kodeksą, kuris atitiktų visuotinai pripažintus prekybos arbitrų etikos standartus ir Principų I priedą. Departamentas ir Komisija susitarė pritaikyti arbitražo taisykles ir elgesio kodeksą, kad būtų atsižvelgta į atnaujintas ES ir JAV DPS nuostatas, o Departamentas bendradarbiaudamas su ICDR-AAA užtikrins, kad šie atnaujinimai būtų įdiegti.

Atnaujinti teisės aktus

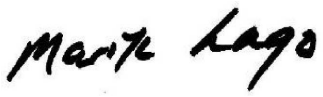
Departamentas pagrįstai stengsis informuoti Komisiją apie ES ir JAV DPS aktualius esminius Jungtinių Amerikos Valstijų teisės pakeitimus duomenų privatumo apsaugos srityje ir susijusius su JAV valdžios institucijų galimybėms susipažinti su asmens duomenimis ir vėliau juos naudoti taikomais apribojimais ir apsaugos priemonėmis.

JAV vyriausybės galimybės susipažinti su asmens duomenimis

Jungtinės Amerikos Valstijos paskelbė Vykdomąjį potvarkį Nr. 14086 dėl Jungtinių Amerikos Valstijų signalų žvalgybos veiklos apsaugos priemonių griežtinimo ir Federalinių reglamentų kodekso 28 antraštinės dalies 201 dalį, kuria iš dalies keičiant Teisingumo departamento reglamentus įsteigiamas Duomenų apsaugos apeliacinis teismas (DPRC), – taip užtikrinama griežta asmens duomenų apsauga, susijusi su valdžios institucijų galimybe susipažinti su duomenimis nacionalinio saugumo tikslais. Užtikrinant apsaugą, be kita ko: griežtinamos privatumo ir piliečių laisvių apsaugos priemonės stengiantis užtikrinti, kad JAV signalų žvalgybos veikla būtų būtina ir proporcinga siekiant nustatytų nacionalinio saugumo tikslų; sukuriamas nepriklausomais ir privalomais įgaliojimais grindžiamas naujas teisių gynimo mechanizmas; stiprinama esama griežta kelių lygmenų JAV signalų žvalgybos veiklos priežiūra. Naudodamiesi šiomis apsaugos priemonėmis, ES asmenys gali ginti savo teises pagal naują kelių lygmenų teisių gynimo mechanizmą, apimantį nepriklausomą DPRC, kurį sudarytų ne iš JAV vyriausybės atrinkti asmenys, kurie turėtų visus įgaliojimus nagrinėti ieškinius ir prireikus imtis tiesioginių taisomųjų priemonių. Departamentas tvarkys registrą, į kurį įtraukiami ES asmenys, pagal Vykdomąjį potvarkį Nr. 14086 ir Federalinių reglamentų kodekso 28 antraštinės dalies 201 dalį pateikę reikalavimus atitinkantį skundą. Praėjus penkeriems metams nuo šio rašto datos ir vėliau kas penkerius metus Departamentas kreipsis į atitinkamas agentūras, kad patikrintų, ar su reikalavimus atitinkančių skundų peržiūra arba su DPRC pateiktų peržiūros prašymų peržiūra susijusi informacija yra išslaptinta. Jeigu tokia informacija išslaptinta, Departamentas, bendradarbiaudamas su atitinkama DAI, informuos ES asmenį. Šiais patobulinimais patvirtinama, kad į Jungtines Amerikos Valstijas perduodami ES asmens duomenys bus tvarkomi laikantis ES teisinių reikalavimų dėl valdžios institucijų galimybių susipažinti su duomenimis.

Remdamiesi Principais, Vykdomuoju potvarkiu Nr. 14086, Federalinių reglamentų kodekso 28 antraštinės dalies 201 dalimi ir pridedamais raštais bei medžiaga, įskaitant Departamento įsipareigojimus dėl Duomenų privatumo sistemos programos administravimo ir priežiūros, tikimės Komisijos patvirtinimo, kad ES ir JAV DPS užtikrinama ES teisės reikalavimus atitinkanti tinkama apsauga ir kad duomenys iš Europos Sąjungos toliau bus perduodami ES ir JAV DPS dalyvaujančioms organizacijoms. Taip pat tikimės, kad šių susitarimų nuostatomis bus sudarytos dar palankesnės sąlygos perduoti duomenis JAV organizacijoms remiantis ES standartinėmis sutarčių sąlygomis arba ES įmonėms privalomomis taisyklėmis.

Pagarbiai



Marisa LAGO

IV PRIEDAS

JUNGTINĖS AMERIKOS VALSTIJOS
Federalinės prekybos komisija
VAŠINGTONAS, DC 20580

Pirmininkės tarnyba

2023 m. birželio 9 d.

Didier Reyndersui
Už teisingumą atsakingam Komisijos nariui
Europos Komisija
Rue de la Loi / Wetstraat 200
1049 Briuselis
Belgija

Gerbiamas Komisijos nary D. Reyndersai,

Jungtinių Amerikos Valstijų Federalinė prekybos komisija (FPK) mielai naudojasi galimybe aptarti su ES ir JAV duomenų privatumo sistemos (toliau – ES ir JAV DPS) Principais susijusį savo vykdymo užtikrinimo vaidmenį. FPK jau seniai yra įsipareigojusi užtikrinti vartotojų ir privatumo apsaugą tarpvalstybiniu mastu, taip pat esame įsipareigoję užtikrinti, kad būtų įtvirtinti prekybos sektoriui aktualūs šios sistemos aspektai. FPK tokį vaidmenį atlieka nuo 2000 m. pagal JAV ir ES saugaus uosto sistemą, o pastaruoju metu – nuo 2016 m. pagal ES ir JAV privatumo skydo sistemą ([1]). 2020 m. liepos 16 d. Europos Sąjungos Teisingumo Teismas (ESTT) dėl problemų, nesusijusių su komerciniais principais, kuriuose siekė įtvirtinti FPK, Europos Komisijos sprendimą dėl tinkamumo, kuriuo grindžiama ES ir JAV privatumo skydo sistema, paskelbė negaliojančiu. Nuo to laiko JAV ir Europos Komisija derėjosi dėl ES ir JAV duomenų privatumo sistemos atsižvelgdamos į tą ESTT sprendimą.

Šiuo raštu patvirtinu FPK įsipareigojimą uoliai užtikrinti, kad būtų laikomasi ES ir JAV DPS principų. Visų pirma patvirtiname savo įsipareigojimą trijose pagrindinėse srityse: 1) teikti pirmumą perduotiems klausimams ir juos nagrinėti; 2) prašyti priimti nutartis ir jas stebėti; 3) bendradarbiauti su ES duomenų apsaugos institucijomis (DAI) užtikrinant vykdymą.

I. **Įvadas**

a. **FPK vykdomas privatumo užtikrinimas ir politinis darbas**

FPK turi plačius civilinius vykdymo užtikrinimo įgaliojimus skatinti vartotojų apsaugą ir konkurenciją prekybos srityje. Įgyvendindama vartotojų apsaugos įgaliojimus, FPK užtikrina įvairių teisės aktų vykdymą, kad apsaugotų vartotojų ir jų duomenų privatumą ir užtikrintų jų saugumą. Pagrindiniu teisės aktu, kurio vykdymą užtikrina FPK, – FPK aktu –

([1]) Pirmininkės Edithos Ramirez raštas už teisingumą, vartotojų reikalus ir lyčių lygybę atsakingai Europos Komisijos narei Věrai Jourovái, kuriame nurodoma, kaip Federalinė prekybos komisija įgyvendina naująją ES ir JAV privatumo skydo sistemą (2016 m. vasario 29 d.), *pateikiamas adresu* https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. FPK anksčiau taip pat buvo įsipareigojusi vykdyti JAV ir ES saugaus uosto programą. FPK pirmininko Roberto Pitofsky'io raštas Europos Komisijos Vidaus rinkos GD direktoriui Johnui Moggui (2000 m. liepos 14 d.), *pateikiamas adresu* https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission. Šiuo raštu pakeičiami tie ankstesni įsipareigojimai.

draudžiami „nesąžiningi“ ar „apgaulingi“ veiksmai ar veikla prekybos srityje arba darantys poveikį prekybai ([2]). FPK taip pat užtikrina tikslinių įstatymų vykdymą, kad apsaugotų su sveikata, įsiskolinimais ir kitais finansiniais dalykais susijusią informaciją, taip pat vaikų informaciją internete, ir yra priėmusi kiekvieno iš šių įstatymų įgyvendinimo reglamentus ([3]).

Neseniai FPK taip pat ėmėsi įvairių iniciatyvų, kuriomis suintensyvinamas mūsų darbas privatumo srityje. 2022 m. rugpjūčio mėn. FPK paskelbė, kad svarsto taisykles, kaip kovoti su žalingu komerciniu stebėjimu ir nerūpestingu požiūriu į duomenų saugumą ([4]). Projekto tikslas – sukaupti patikimų viešų duomenų, kad būtų aišku, ar FPK turėtų nustatyti taisykles, kuriomis būtų sprendžiami komercinio stebėjimo ir duomenų saugumo užtikrinimo praktikos klausimai, ir kokios turėtų būti tos taisyklės. Džiaugėmės gavę ES suinteresuotųjų subjektų pastabų dėl šios ir kitų iniciatyvų.

Mūsų konferencijose „PrivacyCon“ toliau dalyvauja pirmaujantys tyrėjai, kad aptartų naujausius mokslinius tyrimus ir tendencijas, susijusias su vartotojų privatumu ir duomenų saugumu. Taip pat subūrę augančią technologų ir tarpdalykių tyrėjų komandą pasistengėme, kad mūsų agentūra gebėtų neatsilikti nuo technologijų pažangos, kuria grindžiama didelė dalis mūsų darbo privatumo srityje. Kaip žinote, taip pat paskelbėme apie bendrą dialogą su Jumis ir Jūsų kolegomis Europos Komisijoje, kuriame, be kita ko, sprendžiami tokie su privatumu susiję klausimai kaip manipuliatyvūs dizaino sprendimai ir verslo modeliai, kuriems būdingas visuotinis duomenų rinkimas ([5]). Be to, neseniai pateikėme ataskaitą Kongresui, kurioje įspėjome apie žalą, susijusią su dirbtinio intelekto (DI) naudojimu siekiant pašalinti Kongreso nustatytą žalą internete. Toje ataskaitoje išreikštas susirūpinimas dėl netikslumo, šališkumo, diskriminacijos ir perteklinio komercinio stebėjimo ([6]).

b. **ES vartotojams naudingos JAV teisinės apsaugos priemonės**

ES ir JAV DPS veikia platesnėje JAV privatumo srityje, kurioje įvairiais būdais užtikrinama ir ES vartotojų apsauga. FPK akte nustatytu nesąžiningų ar apgaulingų veiksmų ar veiklos draudimu siekiama apsaugoti ne tik JAV vartotojus nuo JAV bendrovių, nes jis taikomas veiklai, kuri 1) sukelia arba veikiausiai sukels pagrįstai numatomą žalą Jungtinėse Amerikos Valstijose, arba 2) yra susijusi su faktiniu elgesiu Jungtinėse Amerikos Valstijose. Be to, siekdama apsaugoti užsienio vartotojus, FPK gali naudoti visas teisių gynimo priemones, kurios yra prieinamos šalies vartotojams ([7]).

FPK taip pat užtikrina, kad būtų vykdomi ir kiti tiksliniai teisės aktai, kuriais užtikrinama ne vien JAV vartotojų apsauga, pvz., Vaikų privatumo internete apsaugos aktas (COPPA). COPPA, be kita ko, reikalaujama, kad vaikams skirtų interneto svetainių ir internetinių paslaugų arba visai visuomenei skirtų interneto svetainių, kuriose sąmoningai renkama asmeninė informacija iš jaunesnių nei 13 metų vaikų, valdytojai pateiktų įspėjimą tėvams ir gautų patikrinamą tėvų sutikimą. Reikalaujama, kad JAV veikiančios interneto svetainės ir paslaugos, kurioms taikomas COPPA ir kuriose renkama

([2]) JAV kodekso 15 antraštinės dalies 45 straipsnio a dalis. FPK neturi jurisdikcijos baudžiamosios teisėsaugos ar nacionalinio saugumo klausimais. FPK taip pat negali daryti įtakos daugumai kitų vyriausybės veiksmų. Be to, FPK jurisdikcijai komercinės veiklos srityje taikomos išimtys, be kita ko, susijusios su bankais, oro vežėjais, draudimo bendrovėmis ir bendra telekomunikacijų paslaugų teikėjų vežimo veikla. FPK jurisdikcijai taip pat nepriklauso dauguma ne pelno organizacijų, tačiau jos jurisdikcijai priklauso fiktyvūs labdaros fondai ar kitos ne pelno organizacijos, kurios iš tiesų siekia pelno. FPK jurisdikcijai taip pat priklauso ne pelno organizacijos, kurios siekia pelno savo nariams, be kita ko, tokiems nariams teikdamos reikšmingą ekonominę naudą. Kai kuriais atvejais FPK jurisdikcija sutampa su kitų teisėsaugos agentūrų jurisdikcija. Užmezgėme tvirtus darbinius ryšius su federalinėmis ir valstijų valdžios institucijomis ir glaudžiai su jomis bendradarbiaujame koordinuodami tyrimus arba, prireikus, perduodami bylas.

([3]) *Žr.* FPK, skirsnis „Privatumas ir saugumas“, https://www.ftc.gov/business-guidance/privacy-security.

([4]) *Žr.* Fed. prekybos komisijos pranešimą spaudai apie tai, kad FPK svarsto taisykles, kaip kovoti su komerciniu stebėjimu ir nerūpestingu požiūriu į duomenų saugumą (2022 m. rugpjūčio 11 d.), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

([5]) *Žr.* už teisingumą atsakingo Europos Komisijos nario Didier Reynderso ir Jungtinių Amerikos Valstijų Federalinės prekybos komisijos pirmininkės Linos Khan bendrą pranešimą spaudai (2022 m. kovo 30 d.), https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

([6]) *Žr.* FPK ataskaitą, kurioje įspėjama dėl dirbtinio intelekto naudojimo kovojant su problemomis internete (2022 m. birželio 16 d.), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.

([7]) JAV kodekso 15 antraštinės dalies 45 straipsnio a dalies 4 punkto B papunktis. Be to, „nesąžiningi ar apgaulingi veiksmai ar veikla“ apima tokius su užsienio prekyba susijusius veiksmus ar veiklą, kurie i) sukelia arba veikiausiai sukels pagrįstai numatomą žalą Jungtinėse Amerikos Valstijose arba ii) yra susiję su faktiniu elgesiu Jungtinėse Amerikos Valstijose. JAV kodekso 15 antraštinės dalies 45 straipsnio a dalies 4 punkto A papunktis.

asmeninė informacija iš užsienio vaikų, atitiktų COPPA. Užsienyje veikiančios interneto svetainės ir internetinės paslaugos taip pat turi atitikti COPPA, jeigu yra skirtos Jungtinių Amerikos Valstijų vaikams arba jose sąmoningai renkama asmeninė informacija iš Jungtinių Amerikos Valstijų vaikų. Be to, ES vartotojams taip pat gali būti naudingi ne tik JAV federaliniai įstatymai, kurių vykdymą užtikrina FPK, bet ir kiti federaliniai ir valstijų teisės aktai dėl vartotojų apsaugos, duomenų saugumo pažeidimų ir privatumo.

c. **FPK vykdymo užtikrinimo veikla**

FPK iškėlė bylų pagal JAV ir ES saugaus uosto ir ES ir JAV privatumo skydo sistemas ir toliau užtikrino ES ir JAV privatumo skydo taikymą net ir po to, kai ESTT sprendimą dėl tinkamumo, kuriuo grindžiama ES ir JAV privatumo skydo sistema, paskelbė negaliojančiu ([8]). Keliuose naujausiuose FPK pateiktuose skunduose, be kita ko, bylose prieš „Twitter“ ([9]), „CafePress“ ([10]) ir „Flo“ ([11]), teigiama, kad įmonės pažeidė ES ir JAV privatumo skydo nuostatas. Vykdydama „Twitter“ skirtus vykdymo užtikrinimo veiksmus, FPK iš „Twitter“ gavo 150 mln. JAV dolerių už ankstesnės FPK nutarties pažeidimą, kuris turėjo poveikio daugiau kaip 140 mln. klientų, taip pat už ES ir JAV privatumo skydo 5 principo (duomenų vientisumo ir tikslo apribojimo) pažeidimą. Be to, agentūros nutartyje reikalaujama, kad „Twitter“ leistų naudotojams naudoti saugius daugiaveiksnio tapatumo nustatymo metodus, pagal kuriuos naudotojai neprivalo nurodyti savo telefono numerio.

„CafePress“ byloje FPK pareiškė, kad bendrovė neužtikrino neskelbtinos vartotojų informacijos saugumo, nuslėpė didelį duomenų saugumo pažeidimą ir pažeidė ES ir JAV privatumo skydo 2 principą (pasirinkimo), 4 principą (saugumo) ir 6 principą (susipažinimo su duomenimis). FPK nutartyje reikalaujama, kad bendrovė netinkamas tapatumo nustatymo priemones pakeistų daugiaveiksniu tapatumo nustatymu, gerokai sumažintų renkamų ir saugomų duomenų kiekį, užšifruotų socialinio draudimo numerius ir pasirūpintų, kad trečioji šalis įvertintų savo informacijos saugumo programas, taip pat FPK pateiktų kopiją, kurią galima skelbti.

„Flo“ byloje FPK pareiškė, kad vaisingumo stebėjimo programėlė atskleidė naudotojų sveikatos informaciją trečiųjų šalių duomenų analizės paslaugų teikėjams, nors buvo įsipareigojusi užtikrinti tokios informacijos privatumą. FPK skunde konkrečiai atkreipiamas dėmesys į bendrovės santykius su ES vartotojais ir į tai, kad „Flo“ pažeidė ES ir JAV privatumo skydo 1 principą (pranešimo), 2 principą (pasirinkimo), 3 principą (atskaitomybės už tolesnį duomenų perdavimą) ir 5 principą (duomenų vientisumo ir tikslo apribojimo). Be kita ko, agentūros nutartyje reikalaujama, kad „Flo“ praneštų poveikį patyrusiems naudotojams apie jų asmeninės informacijos atskleidimą ir nurodytų naudotojų sveikatos informaciją gavusiai bet kuriai trečiajai šaliai tuos duomenis sunaikinti. Svarbu, kad pagal FPK nutartis saugomi visi pasaulio vartotojai, kurie palaiko ryšį su JAV įmone, o ne vien skundą pateikę vartotojai.

Daugelis ankstesnių JAV ir ES saugaus uosto ir ES ir JAV privatumo skydo vykdymo užtikrinimo bylų buvo susijusios su organizacijomis, kurios atliko pradinį savarankišką sertifikavimą Prekybos departamente, bet neišlaikė metinio savarankiško sertifikavimo, nors ir toliau teigė, kad dalyvauja sistemoje. Kitos bylos buvo susijusios su organizacijų, kurios niekada nebuvo atlikusios pradinio savarankiško sertifikavimo Prekybos departamente, neteisingais teiginiais apie dalyvavimą sistemoje. Ateityje numatome proaktyviai užtikrindami vykdymą susitelkti į tokio tipo esminius ES ir JAV DPS principų pažeidimus, kokie nurodomi, pvz., „Twitter“, „CafePress“ ir „Flo“ bylose. Kol kas Prekybos departamentas administruos ir prižiūrės savarankiško sertifikavimo procesą, tvarkys patikimą ES ir JAV DPS dalyvių sąrašą ir spręs kitus su teiginiais apie dalyvavimą programoje susijusius klausimus ([12]). Svarbu, kad organizacijų, kurios teigia dalyvaujančios ES ir JAV DPS, atžvilgiu gali būti imamasi reikšmingų ES ir JAV DPS principų laikymosi užtikrinimo veiksmų, net jei jos neatlieka arba nepratęsia savarankiško sertifikavimo per Prekybos departamentą.

([8]) FPK saugaus uosto ir privatumo skydo bylų sąrašas pateikiamas A priedėlyje.

([9]) Žr. Fed. prekybos komisijos pranešimą spaudai apie FPK skirtą baudą „Twitter“, apgaulingai naudojusiam paskyros saugumo duomenis tikslinėms reklamoms parduoti (2022 m. gegužės 25 d.), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

([10]) Žr. pranešimą apie FPK veiksmus prieš „CafePress“ dėl mėginimo nuslėpti duomenų saugumo pažeidimą (2022 m. kovo 15 d.), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

([11]) Žr. Fed. prekybos komisijos pranešimą spaudai apie FPK priimtą galutinę nutartį dėl „Flo Health“ – vaisingumo stebėjimo programėlės, kuri dalijosi neskelbtinais duomenimis su „Facebook“, „Google“ ir kt. (2021 m. birželio 22 d.), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

([12]) Už tarptautinę prekybą atsakingos prekybos sekretorės pavaduotojos Marisos Lago raštas už teisingumą atsakingam Europos Komisijos nariui Didier Reyndersui (2022 m. gruodžio 12 d.).

II. **Pirmumas perduodamiems klausimams ir tyrimai**

Kaip ir pagal JAV ir ES saugaus uosto sistemą ir ES ir JAV privatumo skydo sistemą, FPK įsipareigoja pirmumo tvarka svarstyti Prekybos departamento ir ES valstybių narių perduotus su ES ir JAV DPS principais susijusius klausimus. Taip pat pirmumo tvarka nagrinėsime privatumo savireguliavimo organizacijų ir kitų nepriklausomų ginčų sprendimo įstaigų perduotus klausimus dėl ES ir JAV DPS principų nesilaikymo.

Kad būtų lengviau pagal ES ir JAV DPS perduoti klausimą iš ES valstybių narių, FPK nustatė standartizuotą klausimų perdavimo procesą ir ES valstybėms narėms pateikė rekomendacijų, kokių rūšių informacija būtų naudingiausia FPK tiriant perduotą klausimą. Be kita ko, FPK paskyrė kontaktinę agentūrą, kuriai ES valstybės narės galės perduoti klausimus. Naudingiausia, kai perduodančioji institucija atlieka pirminį įtariamo pažeidimo tyrimą ir gali bendradarbiauti su tyrimą atliekančia FPK.

Gavusi tokį Prekybos departamento, ES valstybės narės, savireguliavimo organizacijos ar kitų nepriklausomų ginčų sprendimo įstaigų perduotą klausimą, FPK gali imtis įvairių veiksmų iškeltiems klausimams spręsti. Pavyzdžiui, galime peržiūrėti organizacijos privatumo politiką, tiesiogiai iš organizacijos arba iš trečiųjų šalių gauti papildomos informacijos, imtis paskesnių veiksmų su klausimą perdavusiu subjektu, įvertinti, ar yra pažeidimų modelis arba poveikį patyrė daug vartotojų, nustatyti, ar perduotas klausimas susijęs su Prekybos departamento kompetencijai priklausančiais klausimais, įvertinti, ar būtų naudinga papildomai informuoti rinkos dalyvius, ir, prireikus, pradėti vykdymo užtikrinimo procesą.

FPK ne tik pirmumo tvarka nagrinės Prekybos departamento, ES valstybių narių ir privatumo savireguliavimo organizacijų ar kitų nepriklausomų ginčų sprendimo įstaigų perduotus su ES ir JAV DPS principais susijusius klausimus, ([13]) bet ir prireikus savo iniciatyva toliau tirs reikšmingus ES ir JAV DPS principų pažeidimus, naudodama įvairias priemones. Vykdydama FPK programą, pagal kurią nagrinėjami su komercinėmis organizacijomis susiję privatumo ir saugumo klausimai, ši agentūra reguliariai tikrino, ar atitinkamas subjektas padarė su ES ir JAV privatumo skydu susijusių pareiškimų. Jeigu subjektas padarė tokių pareiškimų ir atlikus tyrimą buvo nustatyta akivaizdžių ES ir JAV privatumo skydo principų pažeidimų, FPK į savo vykdymo užtikrinimo veiksmus įtraukė įtarimus dėl ES ir JAV privatumo skydo pažeidimų. Toliau laikysimės šio proaktyvaus požiūrio, dabar remdamiesi ES ir JAV DPS principais.

III. **Prašymas priimti nutartis ir jų stebėjimas**

FPK taip pat patvirtina savo įsipareigojimą prašyti priimti vykdomąsias nutartis ir stebėti, kaip jos vykdomos, siekdama užtikrinti, kad būtų laikomasi ES ir JAV DPS principų. Laikytis ES ir JAV DPS principų reikalausime taikydami įvairias tinkamas draudžiamąsias nuostatas, išdėstytas būsimose FPK nutartyse dėl ES ir JAV DPS principų. Už FPK administracinių nutarčių pažeidimus gali būti skiriama piniginė nuobauda iki 501,20 JAV dolerių už pažeidimą arba 501,20 JAV dolerių už dieną, jeigu pažeidimas tęsiamas ([14]), taigi jeigu atitinkama praktika turėjo poveikio daugeliui vartotojų, gali susidaryti milijonus dolerių siekianti suma. Į kiekvieną susitarimo nutartį taip pat įtraukiamos nuostatos dėl ataskaitų teikimo ir reikalavimų laikymosi. Subjektai, kuriems skirta nutartis, nurodytą skaičių metų privalo saugoti dokumentus, kuriais įrodoma, kad jie laikėsi reikalavimų. Nutartys taip pat turi būti įteikiamos darbuotojams, atsakingiems už nutarčių laikymosi užtikrinimą.

FPK sistemingai stebi, kaip laikomasi galiojančių nutarčių dėl ES ir JAV privatumo skydo principų, taip pat visų kitų jos nutarčių, ir prireikus imasi veiksmų, kad užtikrintų jų vykdymą ([15]). Svarbu, kad pagal FPK nutartis toliau bus saugomi visi pasaulio vartotojai, kurie palaiko ryšį su įmone, o ne vien skundą pateikę vartotojai. Galiausiai FPK tvarkys internetinį sąrašą, į kurį bus įtraukiamos bendrovės, kurioms taikomos nutartys, išduotos siekiant užtikrinti, kad būtų laikomasi ES ir JAV DPS principų ([16]).

([13]) Nors FPK nesprendžia atskirų vartotojų skundų ir jiems netarpininkauja, FPK patvirtina, kad teiks pirmumą ES DAI perduotiems su ES ir JAV DPS principais susijusiems klusimams. Be to, remdamasi skundais savo Vartotojų kontrolinėje duomenų bazėje, kuria gali naudotis daug kitų teisėsaugos institucijų, FPK nustato tendencijas, vykdymo užtikrinimo prioritetus ir galimus tyrimų objektus. Norėdami pateikti skundą FPK, ES asmenys gali naudotis ta pačia skundų teikimo sistema, kaip ir JAV vartotojai, kuri yra pasiekiama adresu https://reportfraud.ftc.gov/. Tačiau atskirus su ES ir JAV DPS principais susijusius skundus ES asmenims gali būti naudingiausia pateikti savo valstybės narės DAI arba nepriklausomai ginčų sprendimo įstaigai.

([14]) JAV kodekso 15 antraštinės dalies 45 straipsnio m dalis, Federalinių reglamentų kodekso 16 antraštinės dalies 1.98 straipsnis. Ši suma periodiškai koreguojama atsižvelgiant į infliaciją.

([15]) Praėjusiais metais FPK balsavo už tai, kad pakartotiniams pažeidėjams taikomas tyrimo procesas būtų supaprastintas. *Žr.* pranešimą apie FPK leidžiamus su pagrindiniais vykdymo užtikrinimo prioritetais susijusius tyrimus (2021 m. liepos 1 d.), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.

([16]) *Cf.* FPK, privatumo skydas, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. **Bendradarbiavimas su ES DAI vykdymo užtikrinimo srityje**

FPK pripažįsta svarbų ES DAI vaidmenį, kurį jos gali atlikti užtikrindamos, kad būtų laikomasi ES ir JAV DPS principų, ir skatina aktyviau konsultuotis ir glaudžiau bendradarbiauti užtikrinant vykdymą. Iš tiesų, vis svarbesnis tampa koordinuotas požiūris į iššūkius, kylančius dėl dabartinių skaitmeninės rinkos pokyčių ir dideliais duomenų kiekiais grindžiamų verslo modelių. FPK su klausimus perdavusiomis vykdymo užtikrinimo institucijomis informacija apie perduotus klausimus, be kita ko, informacija apie perduoto klausimo nagrinėjimo statusą, keisis laikydamasi konfidencialumo teisės aktų ir apribojimų. Kiek įmanoma atsižvelgiant į perduotų klausimų skaičių ir rūšį, teikiant informaciją bus įtraukiamas perduotų klausimų vertinimas, be kita ko, apibūdinami reikšmingi iškelti klausimai ir visi veiksmai, kurių savo jurisdikcijoje ėmėsi FPK, kad ištaisytų teisės aktų pažeidimus. FPK klausimą perdavusiai institucijai taip pat teiks grįžtamąją informaciją apie gautų klausimų rūšis, kad veiksmai, kuriais siekiama spręsti neteisėto elgesio problemą, būtų veiksmingesni. Jeigu klausimą perdavusi vykdymo užtikrinimo institucija siekia gauti informacijos apie konkretaus perduoto klausimo nagrinėjimo statusą, kad pradėtų savo vykdymo užtikrinimo procesą, FPK, atsižvelgdama į nagrinėjamų klausimų skaičių ir laikydamasi konfidencialumo ir kitų teisinių reikalavimų, pateiks atsakymą tai institucijai.

FPK taip pat glaudžiai dirbs su ES DAI, kad padėtų užtikrinti vykdymą. Atitinkamais atvejais, be kita ko, galėtų būti dalijamasi informacija ir padedama vykdyti tyrimus pagal JAV saugaus tinklo aktą, kuriuo FPK leidžiama teikti pagalbą užsienio teisėsaugos agentūroms, kai pastarosios užtikrina, kad būtų vykdomi teisės aktai, kuriais draudžiama praktika, iš esmės panaši į praktiką, draudžiamą pagal teisės aktus, kurių vykdymą užtikrina FPK ([17]). Teikdama tokią pagalbą, FPK gali dalytis informacija, susijusia su FPK atliekamu tyrimu, savo tyrimą atliekančios ES DAI vardu priimti privalomus procesinius dokumentus ir prašyti išklausyti žodinių liudytojų ar atsakovų parodymų, susijusių su DAI vykdymo užtikrinimo procesu, laikydamasi JAV saugaus tinklo akte nustatytų reikalavimų. FPK reguliariai naudojasi šiais įgaliojimais, kad padėtų kitoms įvairių pasaulio šalių institucijoms nagrinėti privatumo ir vartotojų apsaugos sričių bylas.

FPK ne tik konsultuosis su klausimą perdavusiomis ES DAI dėl konkrečių dalykų, bet ir dalyvaudama reguliariuose susitikimuose su paskirtais Europos duomenų apsaugos valdybos (EDAV) atstovais aptars, kaip apskritai gerinti bendradarbiavimą vykdymo užtikrinimo srityje. FPK kartu su Prekybos departamentu, Europos Komisija ir EDAV atstovais taip pat dalyvaus periodinėje ES ir JAV DPS peržiūroje, kad aptartų jos įgyvendinimo klausimus. FPK taip pat ragina kurti priemones, kurios paskatins vykdymo užtikrinimo srityje aktyviau bendradarbiauti su ES DAI, taip pat kitomis privatumo užtikrinimo institucijomis visame pasaulyje. FPK su malonumu patvirtina savo įsipareigojimą užtikrinti, kad būtų įtvirtinti prekybos sektoriui aktualūs ES ir JAV DPS aspektai. Partnerystę su ES kolegomis laikome itin svarbia mūsų ir jūsų piliečių privatumo apsaugos užtikrinimo dalimi.

Pagarbiai

Lina M. KHAN
Federalinės prekybos komisijos pirmininkė

([17]) Nustatydama, ar pasinaudoti JAV saugaus tinklo aktu suteikiamais įgaliojimais, FPK, *inter alia*, nagrinėja: „A) ar prašančioji agentūra sutiko teikti arba teiks tarpusavio pagalbą Komisijai; B) ar įvykdžius prašymą būtų pakenkta Jungtinių Amerikos Valstijų viešiesiems interesams; C) ar prašančiosios agentūros tyrimas arba vykdymo užtikrinimo procesas yra susiję su veiksmais ar praktika, dėl kurių daug asmenų patiria arba veikiausiai patirs žalą.“ JAV kodekso 15 antraštinės dalies 46 straipsnio j dalies 3 punktas. Konkurencijos teisės aktų vykdymo užtikrinimui šie įgaliojimai netaikomi.

A priedėlis

Privatumo skydo ir saugaus uosto vykdymo užtikrinimas

	Registro / FPK bylos Nr.	Byla	Nuoroda
1	FPK byla Nr. 2023062 Byla Nr. 3:22-cv-03070 (N. D. Cal.)	JAV / **„Twitter, Inc.“**	Twitter
2	FPK byla Nr. 192 3209	„Residual Pumpkin Entity, LLC“, ankstesniu prekybiniu pavadinimu **„CafePress“**, ir „PlanetArt, LLC“, prekybiniu pavadinimu **„CafePress“**, byloje	CafePress
3	FPK byla Nr. 192 3133 Registro Nr. C-4747	**„Flo Health, Inc.“** byloje	Flo Health
4	FPK byla Nr. 192 3050 Registro Nr. C-4723	**„Ortho-Clinical Diagnostics, Inc.“** byloje	Ortho-Clinical
5	FPK byla Nr. 192 3092 Registro Nr. C-4709	**„T&M Protection, LLC“** byloje	T&M Protection
6	FPK byla Nr. 192 3084 Registro Nr. C-4704	**„TDARX, Inc.“** byloje	TDARX
7	FPK byla Nr. 192 3093 Registro Nr. C-4706	**„Global Data Vault, LLC“** byloje	Global Data
8	FPK byla Nr. 192 3078 Registro Nr. C-4703	**„Incentive Services, Inc.“** byloje	Incentive Services
9	FPK byla Nr. 192 3090 Registro Nr. C-4705	**„Click Labs, Inc.“** byloje	Click Labs
10	FPK byla Nr. 182 3192 Registro Nr. C-4697	**„Medable, Inc.“** byloje	Medable
11	FPK byla Nr. 182 3189 Registro Nr. 9386	„NTT Global Data Centers Americas, Inc.“, kuri yra įmonės **„RagingWire Data Centers, Inc.“** teisių perėmėja, byloje	RagingWire
12	FPK byla Nr. 182 3196 Registro Nr. C-4702	**„Thru, Inc.“** byloje	Thru
13	FPK byla Nr. 182 3188 Registro Nr. C-4698	**„DCR Workforce, Inc.“** byloje	DCR Workforce
14	FPK byla Nr. 182 3194 Registro Nr. C-4700	**„LotaData“, Inc.“** byloje	LotaData
15	FPK byla Nr. 182 3195 Registro Nr. C-4701	**„EmpiriStat, Inc.“** byloje	EmpiriStat

16	FPK byla Nr. 182 3193 Registro Nr. C-4699	„214 Technologies, Inc.“, prekybiniu pavadinimu **„Trueface.ai“**, byloje	Trueface.ai
17	FPK byla Nr. 182 3107 Registro Nr. 9383	**„Cambridge Analytica, LLC“** byloje	Cambridge Analytica
18	FPK byla Nr. 182 3152 Registro Nr. C-4685	**„SecureTest, Inc.“** byloje	SecurTest
19	FPK byla Nr. 182 3144 Registro Nr. C-4664	**„VenPath, Inc.“** byloje	VenPath
20	FPK byla Nr. 182 3154 Registro Nr. C-4666	**„SmartStart Employment Screening, Inc“** byloje	SmartStart
21	FPK byla Nr. 182 3143 Registro Nr. C-4663	**„mResourceLLC“,** prekybiniu pavadinimu „Loop Works LLC“, byloje	mResource
22	FPK byla Nr. 182 3150 Registro Nr. C-4665	**„Idmission LLC“** byloje	IDmission
23	FPK byla Nr. 182 3100 Registro Nr. C-4659	**„ReadyTech Corporation“** byloje	ReadyTech
24	FPK byla Nr. 172 3173 Registro Nr. C-4630	**„Decusoft, LLC“** byloje	Decusoft
25	FPK byla Nr. 172 3171 Registro Nr. C-4628	**„Tru Communication, Inc.“** byloje	Tru
26	FPK byla Nr. 172 3172 Registro Nr. C-4629	**„Md7, LLC“** byloje	Md7
30	FPK byla Nr. 152 3198 Registro Nr. C-4543	**„Jhayrmaine Daniels“** (prekybiniu pavadinimu **„California Skate-Line“**) byloje	Jhayrmaine Daniels
31	FPK byla Nr. 152 3190 Registro Nr. C-4545	**„Dale Jarrett Racing Adventure, Inc.“** byloje	Dale Jarrett
32	FPK byla Nr. 152 3141 Registro Nr. C-4540	**„Golf Connect, LLC“** byloje	Golf Connect
33	FPK byla Nr. 152 3202 Registro Nr. C-4546	**„Inbox Group, LLC“** byloje	Inbox Group
34	Bylos Nr. 152 3187 Registro Nr. C-4542	**„IOActive, Inc“** byloje	IOActive
35	FPK byla Nr. 152 3140 Registro Nr. C-4549	**„Jubilant Clinsys, Inc.“** byloje	Jubilant
36	FPK byla Nr. 152 3199 Registro Nr. C-4547	**„Just Bagels Manufacturing, Inc.“** byloje	Just Bagels

37	FPK byla Nr. 152 3138 Registro Nr. C-4548	**„NAICS Association, LLC“** byloje	NAICS
38	FPK byla Nr. 152 3201 Registro Nr. C-4544	**„One Industries Corp.“** byloje	One Industries
39	FPK byla Nr. 152 3137 Registro Nr. C-4550	**„Pinger, Inc.“** byloje	Pinger
40	FPK byla Nr. 152 3193 Registro Nr. C-4552	**„SteriMed Medical Waste Solutions**“ byloje	SteriMed
41	FPK byla Nr. 152 3184 Registro Nr. C-4541	**„Contract Logix, LLC“** byloje	Contract Logix
42	FPK byla Nr. 152 3185 Registro Nr. C-4551	**„Forensics Consulting Solutions, LLC“** byloje	Forensics Consulting
43	FPK byla Nr. 152 3051 Registro Nr. C-4526	**„American Int'l Mailing, Inc.“** byloje	AIM
44	FPK byla Nr. 152 3015 Registro Nr. C-4525	**„TES Franchising, LLC“** byloje	TES
45	FPK byla Nr. 142 3036 Registro Nr. C-4459	**„American Apparel, Inc.“** byloje	American Apparel
46	FPK byla Nr. 142 3026 Registro Nr. C-4469	**„Fantage.com, Inc.“** byloje	Fantage
47	FPK byla Nr. 142 3017 Registro Nr. C-4461	**„Apperian, Inc.“** byloje	Apperian
48	FPK byla Nr. 142 3018 Registro Nr. C-4462	**„Atlanta Falcons Football Club, LLC“** byloje	Atlanta Falcons
49	FPK byla Nr. 142 3019 Registro Nr. C-4463	**„Baker Tilly Virchow Krause, LLP“** byloje	Baker Tilly
50	FPK byla Nr. 142 3020 Registro Nr. C-4464	**„BitTorrent, Inc.“** byloje	BitTorrent
51	FPK byla Nr. 142 3022 Registro Nr. C-4465	**„Charles River Laboratories, Int'l“** byloje	Charles River
52	FPK byla Nr. 142 3023 Registro Nr. C-4466	**„DataMotion, Inc.“** byloje	DataMotion
53	FPK byla Nr. 142 3024 Registro Nr. C-4467	**„DDC Laboratories, Inc.“**, prekybiniu pavadinimu „DNA Diagnostics Center“, byloje	DDC
54	FPK byla Nr. 142 3028 Registro Nr. C-4470	**„Level 3 Communications, LLC“** byloje	Level 3

55	FPK byla Nr. 142 3025 Registro Nr. C-4468	**„PDB Sports, Ltd.**“, prekybiniu pavadinimu „Denver Broncos Football Club, LLP“, byloje	Broncos
56	FPK byla Nr. 142 3030 Registro Nr. C-4471	**„Reynolds Consumer Products, Inc.“** byloje	Reynolds
57	FPK byla Nr. 142 3031 Registro Nr. C-4472	**„Receivable Management Services Corporation“** byloje	Receivable Mgmt
58	FPK byla Nr. 142 3032 Registro Nr. C-4473	**„Tennessee Football, Inc.“** byloje	Tennessee Football
59	FPK byla Nr. 102 3058 Registro Nr. C-4369	**„Myspace LLC“** byloje	Myspace
60	FPK byla Nr. 092 3184 Registro Nr. C-4365	**„Facebook, Inc.“** byloje	Facebook
61	FPK byla Nr. 092 3081 Civilinė byla Nr. 09-CV-5276 (C. D. Cal.)	FPK / Javian Karnani ir **„Balls of Kryptonite, LLC“**, prekybiniu pavadinimu „Bite Size Deals, LLC“, ir „Best Priced Brands, LLC“	Balls of Kryptonite
62	FPK byla Nr. 102 3136 Registro Nr. C-4336	**„Google, Inc.“** byloje	Google
63	FPK byla Nr. 092 3137 Registro Nr. C-4282	**„World Innovators, Inc.“** byloje	World Innovators
64	FPK byla Nr. 092 3141 Registro Nr. C-4271	**„Progressive Gaitways LLC“** byloje	Progressive Gaitways
65	FPK byla Nr. 092 3139 Registro Nr. C-4270	**„Onyx Graphics, Inc.“** byloje	Onyx Graphics
66	FPK byla Nr. 092 3138 Registro Nr. C-4269	**„ExpatEdge Partners, LLC“** byloje	ExpatEdge
67	FPK byla Nr. 092 3140 Registro Nr. C-4281	**„Directors Desk LLC“** byloje	Directors Desk
68	FPK byla Nr. 092 3142 Registro Nr. C-4272	**„Collectify LLC“** byloje	Collectify

V PRIEDAS

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

2023 m. liepos 6 d.

Komisijos nariui Didier Reyndersui
Europos Komisija
Rue de la Loi / Wetstraat 200
1049 Briuselis
Belgija

Gerbiamas Komisijos nary D. Reyndersai,

Jungtinių Amerikos Valstijų transporto departamentas (toliau – Departamentas arba Transporto departamentas) mielai naudojasi galimybe apibūdinti savo vaidmenį užtikrinant, kad būtų laikomasi ES ir JAV duomenų privatumo sistemos (toliau – ES ir JAV DPS) principų. ES ir JAV DPS atliks esminį vaidmenį apsaugant asmens duomenis, teikiamus sudarant prekybos sandorius vis glaudesniais tarpusavio ryšiais susijusiame pasaulyje. Ši sistema sudarys sąlygas įmonėms vykdyti svarbias operacijas globalios ekonomikos sąlygomis ir kartu padės užtikrinti, kad ES vartotojai toliau galėtų naudotis svarbiomis privatumo užtikrinimo priemonėmis.

Transporto departamentas savo įsipareigojimą užtikrinti JAV ir ES saugaus uosto sistemos įgyvendinimą pirmą kartą viešai pareiškė prieš 22 metus Europos Komisijai išsiųstame rašte; tie įsipareigojimai buvo pakartoti ir išplėsti 2016 m. rašte dėl ES ir JAV privatumo skydo sistemos. Transporto departamentas tuose raštuose įsipareigojo uoliai užtikrinti, kad būtų laikomasi JAV ir ES saugaus uosto privatumo principų, o vėliau – ES ir JAV privatumo skydo principų. Transporto departamentas išplečia tą įsipareigojimą, kad jis apimtų ES ir JAV DPS principus, ir šiuo raštu įtvirtina tą įsipareigojimą.

Visų pirma Transporto departamentas patvirtina savo įsipareigojimą šiose pagrindinėse srityse: 1) teikti pirmumą įtariamų ES ir JAV DPS principų pažeidimų tyrimams; 2) imtis tinkamų vykdymo užtikrinimo veiksmų prieš subjektus, kurie neteisingai ar melagingai teigia dalyvaujantys ES ir JAV DPS; 3) stebėti ir skelbti vykdomąsias nutartis dėl ES ir JAV DPS principų pažeidimų. Informuojame apie kiekvieną iš šių įsipareigojimų ir nurodydami reikiamas aplinkybes pateikiame pagrindinius faktus, susijusius su Transporto departamento vaidmeniu užtikrinant vartotojų privatumo apsaugą ir ES ir JAV DPS principų laikymąsi.

1. **Pagrindiniai faktai**

A. Transporto departamento įgaliojimai privatumo srityje

Departamentas tvirtai įsipareigojo užtikrinti informacijos, kurią vartotojai teikia

oro vežėjams ir bilietų pardavėjams, apsaugą. Transporto departamento įgaliojimai imtis veiksmų šioje srityje nustatyti JAV kodekso 49 antraštinės dalies 41712 straipsnyje, kuriuo vežėjui ar bilietų pardavėjui draudžiama vykdyti „nesąžiningą ar apgaulingą veiklą“ oro transporto arba oro transporto paslaugų pardavimo srityse. 41712 straipsnis

suformuluotas pagal Federalinės prekybos komisijos (FPK) akto 5 straipsnį (JAV kodekso 15 antraštinės dalies 45 straipsnis). Neseniai Transporto departamentas paskelbė reglamentus, kuriuose apibrėžiama nesąžininga ir apgaulinga veikla, remiantis tiek Transporto departamento, tiek FPK precedentais (Federalinių reglamentų kodekso 14 antraštinės dalies 399.79 straipsnis). Konkrečiai, veikla yra „nesąžininga“, jeigu sukelia arba veikiausiai sukels didelę žalą, kurios pagrįstai negalima išvengti, ir tos žalos neatsveria

nauda vartotojams ar konkurencijai. Veikla vartotojų atžvilgiu yra „apgaulinga“, jeigu dėl esminių dalykų veikiausiai klaidins vartotoją, racionaliai veikiantį atitinkamomis aplinkybėmis. Dalykas yra esminis, jeigu veikiausiai turės įtakos vartotojo elgesiui ar sprendimui dėl prekės ar paslaugos. Be šių bendrųjų principų, Transporto departamentas konkrečiai aiškina, kad 41712 straipsniu vežėjams ir bilietų pardavėjams draudžiama: 1) pažeisti jo privatumo politikos nuostatas; 2) pažeisti bet kurią Departamento priimtą taisyklę, kurioje konkreti privatumo užtikrinimo veikla įvardijama kaip nesąžininga ar apgaulinga, arba 3) pažeisti Vaikų privatumo internete apsaugos aktą (COPPA) arba FPK taisykles, kuriomis įgyvendinamas COPPA, arba 4) dalyvaujant ES ir JAV DPS nesilaikyti ES ir JAV DPS principų. ([1]).

Kaip pirmiau nurodyta, pagal federalinę teisę DOT turi išimtinius 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 transporto paslaugų pardavėjui viešai įsipareigojus taikyti ES ir JAV DPS principus, Departamentas gali naudotis 41712 straipsnyje nustatytais įgaliojimais, kad užtikrintų tų principų laikymąsi. Todėl kai keleivis pateikia informacijos vežėjui arba bilietų pardavėjui, kuris įsipareigojo laikytis ES ir JAV DPS principų, kiekvienas atvejis, kai vežėjas arba bilietų pardavėjas tų principų nesilaikys, bus laikomas 41712 straipsnio pažeidimu.

B. Vykdymo užtikrinimo praktika

Pagal JAV kodekso 49 antraštinės dalies 41712 straipsnį bylas tiria ir baudžiamąjį persekiojimą vykdo Departamento Aviacijos vartotojų apsaugos tarnyba (OACP) ([2]). Ji užtikrina, kad būtų laikomasi 41712 straipsnyje nustatyto draudimo vykdyti nesąžiningą ir apgaulingą veiklą, visų pirma vesdama derybas, ruošdama nutartis nutraukti veiksmus ir rengdama nutartis, kuriomis nustatomos piniginės nuobaudos. Tarnyba apie galimus pažeidimus dažniausiai sužino iš jai pateiktų asmenų, kelionių agentų, oro vežėjų ir JAV bei užsienio valstybinių agentūrų skundų. Su privatumu susijusį skundą dėl oro vežėjų ir bilietų pardavėjų vartotojai gali pateikti Transporto departamento interneto svetainėje ([3]).

Jeigu pagrįsto ir tinkamo susitarimo byloje nepasiekiama, OACP turi įgaliojimus pradėti vykdymo užtikrinimo procesą, kuriame, be kita ko, Transporto departamento administracinės teisės teisėjas išklausytų parodymus. Administracinės teisės teisėjas turi įgaliojimus priimti nutartis nutraukti veiksmus ir skirti pinigines nuobaudas. Pažeidus 41712 straipsnį gali būti priimamos nutartys nutraukti veiksmus ir skiriamos piniginės nuobaudos iki 37 377 JAV dolerių už kiekvieną 41712 straipsnio pažeidimą.

Departamentas neturi įgaliojimų nurodyti atlyginti žalą arba priimti sprendimą dėl piniginių kompensacijų atskiriems skundą pateikusiems asmenims. Tačiau Departamentas turi įgaliojimus patvirtinti OACP atliktais tyrimais grindžiamus susitarimus, kurie yra tiesiogiai naudingi vartotojams (pvz., dėl grynųjų pinigų ar kuponų) ir kuriais būtų padengiamos piniginės baudos, kurias antraip reikėtų mokėti JAV vyriausybei. Tokios praktikos laikytasi anksčiau ir jos taip pat gali būti laikomasi taikant ES ir JAV DPS principus, jei tai dera atitinkamomis aplinkybėmis. Jeigu oro vežėjas pakartotinai pažeidžia 41712 straipsnį, gali kilti klausimų dėl oro vežėjo pajėgumo laikytis reikalavimų, o tokiu atveju išimtinėse situacijose gali būti pripažįstama, kad oro vežėjas nėra tinkamas vykdyti veiklą, taigi jis gali prarasti leidimą vykdyti ekonominę veiklą.

Iki šiol Transporto departamentas yra gavęs gana nedaug skundų, kuriuose bilietų pardavėjai arba vežėjai kaltinami privatumo pažeidimais. Pateikti skundai nagrinėjami laikantis pirmiau nurodytų principų.

C. Transporto departamento užtikrinama ES vartotojų teisinė apsauga

Pagal 41712 straipsnį nesąžiningos ar apgaulingos veiklos draudimas oro transporto arba oro transporto paslaugų pardavimo srityse taikomas JAV ir užsienio oro vežėjams ir bilietų pardavėjams. Transporto departamentas dažnai imasi veiksmų JAV ir užsienio oro vežėjų atžvilgiu dėl veiklos, kuri daro poveikį ir užsienio, ir JAV vartotojams, remdamasis tuo, kad ta oro vežėjų veikla buvo vykdoma teikiant vežimo į Jungtines Amerikos Valstijas ir iš jų paslaugas. Transporto departamentas naudoja ir toliau naudos visas prieinamas teisių gynimo priemones, kad apsaugotų ir užsienio, ir JAV vartotojus nuo reguliuojamų įmonių nesąžiningos ar apgaulingos veiklos oro transporto srityje.

([1]) https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.
([2]) Anksčiau vadinta Aviacijos vykdymo užtikrinimo ir procedūrų tarnyba.
([3]) http://www.transportation.gov/airconsumer/privacy-complaints.

Transporto departamentas taip pat užtikrina, kad būtų vykdomi ir kiti su oro vežėjais susiję tiksliniai teisės aktai, kuriais užtikrinama ne vien JAV vartotojų apsauga, pvz., Vaikų privatumo internete apsaugos aktas (COPPA). COPPA, be kita ko, reikalaujama, kad vaikams skirtų interneto svetainių ir internetinių paslaugų arba visai visuomenei skirtų interneto svetainių, kuriose sąmoningai renkama asmeninė informacija iš jaunesnių 13 metų vaikų, valdytojai pateiktų įspėjimą tėvams ir gautų patikrinamą tėvų sutikimą. Reikalaujama, kad JAV veikiančios interneto svetainės ir paslaugos, kurioms taikomas COPPA ir kuriose renkama asmeninė informacija iš užsienio vaikų, atitiktų COPPA. Užsienyje veikiančios interneto svetainės ir internetinės paslaugos taip pat turi atitikti COPPA, jeigu yra skirtos Jungtinių Amerikos Valstijų vaikams arba jose sąmoningai renkama asmeninė informacija iš Jungtinių Amerikos Valstijų vaikų. Jungtinėse Amerikos Valstijose veiklą vykdantiems JAV arba užsienio oro vežėjams pažeidus COPPA, Transporto departamentas turėtų jurisdikciją imtis vykdymo užtikrinimo veiksmų.

II. **ES ir JAV DPS principų laikymosi užtikrinimas**

Jeigu oro vežėjas arba bilietų pardavėjas nusprendžia dalyvauti ES ir JAV DPS, o Departamentas gauna skundą, kad toks oro vežėjas arba bilietų pardavėjas, kaip įtariama, pažeidė ES ir JAV DPS principus, Departamentas imsis toliau nurodytų veiksmų siekdamas griežtai užtikrinti, kad ES ir JAV DPS principų būtų laikomasi.

A. Įtariamų pažeidimų nagrinėjimas pirmumo tvarka

Departamento OACP išnagrinės kiekvieną skundą dėl įtariamų ES ir JAV DPS principų

pažeidimų, įskaitant iš ES duomenų apsaugos institucijų (DAI) gautus skundus, ir, jeigu esama pažeidimo įrodymų, imsis vykdymo užtikrinimo veiksmų. Be to, OACP bendradarbiaus su FPK ir Prekybos departamentu ir pirmumo tvarka nagrinės įtarimus, kad reguliuojami subjektai nesilaiko pagal ES ir JAV DPS prisiimtų įsipareigojimų dėl privatumo.

Sužinojusi apie įtarimą, kad buvo pažeisti ES ir JAV DPS principai, OACP atlikdama tyrimą gali imtis įvairių veiksmų. Pavyzdžiui, ji gali peržiūrėti bilietų pardavėjo arba oro vežėjo privatumo politiką, iš bilietų pardavėjo, oro vežėjo arba trečiųjų šalių gauti papildomos informacijos, imtis paskesnių veiksmų su klausimą perdavusiu subjektu ir įvertinti, ar yra pažeidimų modelis arba poveikį patyrė daug vartotojų. Be to, ji nustatytų, ar nagrinėjamas klausimas patenka į Prekybos departamento ar FPK kompetencijos sritį, įvertintų, ar būtų naudinga šviesti vartotojus ir įmones, ir, prireikus, pradėtų vykdymo užtikrinimo procesą.

Sužinojęs apie galimą ES ir JAV DPS principų pažeidimą, kurį padarė bilietų pardavėjai, Departamentas šiuo klausimu savo veiksmus koordinuos su FPK. Taip pat informuosime FPK ir Prekybos departamentą apie kiekvieno veiksmo, kuriuo siekiama užtikrinti, kad būtų laikomasi ES ir JAV DPS principų, rezultatus.

B. Neteisingų ar melagingų teiginių apie dalyvavimą sistemoje šalinimas

Departamentas tebėra įsipareigojęs tirti ES ir JAV DPS principų pažeidimus, be kita ko, neteisingus ar melagingus teiginius apie dalyvavimą ES ir JAV DPS. Pirmumo tvarka nagrinėsime Prekybos departamento perduotus klausimus dėl organizacijų, kurios, kaip nustatė Departamentas, nepagrįstai save laiko ES ir JAV DPS dalyvėmis arba be leidimo naudoja ES ir JAV DPS sertifikavimo ženklą.

Be to, pažymime, kad jeigu organizacijos privatumo politikoje įsipareigojama laikytis ES ir JAV DPS principų, organizacijai neatlikus arba neišlaikius savarankiško sertifikavimo Prekybos departamente, vien to veikiausiai nepakaks, kad Transporto departamentas nesiimtų veiksmų užtikrinti, kad organizacija vykdytų tuos įsipareigojimus.

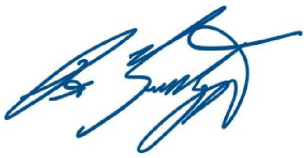
C. Su ES ir JAV DPS pažeidimais susijusių vykdomųjų nutarčių stebėsena ir skelbimas

Departamento OACP taip pat yra įsipareigojusi toliau stebėti vykdomąsias nutartis, kai to reikia siekiant užtikrinti, kad būtų laikomasi ES ir JAV DPS principų. Konkrečiau, jeigu tarnyba priima nutartį, kurioje oro vežėjui arba bilietų pardavėjui liepiama nutraukti ES ir JAV DPS ir 41712 straipsnio pažeidimus ir ateityje jų nebedaryti, ji stebės, kaip subjektas laikosi nutartyje išdėstytos nuostatos dėl veiksmų nutraukimo. Be to, tarnyba užtikrins, kad su ES ir JAV DPS principais susijusiose bylose priimtos nutartys būtų skelbiamos jos interneto svetainėje.

Spręsdami ES ir JAV DPS klausimus, toliau stengsimės dirbti su savo federaliniais partneriais ir ES suinteresuotaisiais subjektais.

Tikiuosi, kad ši informacija bus naudinga. Jeigu turite klausimų ar norite gauti daugiau informacijos, prašom susisiekti su manimi.

Pagarbiai



Pete BUTTIGIEG

VI PRIEDAS

JAV Teisingumo departamentas

Baudžiamosios teisės skyrius

Generalinio prokuroro padėjėjo tarnyba Vašingtonas, DC 20530

2023 m. birželio 23 d.

Anai Gallego Torres
Teisingumo ir vartotojų reikalų generalinei direktorei
Europos Komisija
Rue Montoyer / Montoyerstraat 59
1049 Briuselis
Belgija

Gerb. generaline direktore A. Gallego Torres,

Šiame 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]). Visi šiame rašte aprašyti teisiniai procesai yra nediskriminuojamojo pobūdžio, nes yra taikomi siekiant gauti informacijos iš Jungtinėse Amerikos Valstijose veikiančių korporacijų, įskaitant bendroves, kurios atlieka savarankišką sertifikavimą pagal ES ir JAV duomenų privatumo sistemą, nepaisant duomenų subjekto pilietybės ar gyvenamosios vietos. 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 priesaika arba patvirtinimu, ypač orderiai, kuriuose aprašoma apieškoma vieta ir asmenys arba areštuotini daiktai, negali būti išduodami“. (JAV Konstitucijos IV pataisa). IV. Kaip nurodė Jungtinių Amerikos Valstijų Aukščiausiasis Teismas Sprendime Berger / Niujorko valstija, „[p]agrindinis šio pakeitimo tikslas, kaip pripažįstama daugybėje šio Teismo sprendimų, yra apsaugoti asmenų privatumą ir užtikrinti jų saugumą nuo savavališko vyriausybės pareigūnų kišimosi“. (388 U.S. 41, 53 (1967), cituojamas Sprendimas *Camara / San Fransisko savivaldybės 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. Sprendimą *Katz / Jungtinės Amerikos Valstijos*, 389 U.S. 347, 357 (1967)). Orderių išdavimo standartai, pvz., tikėtinos priežasties ir konkretumo reikalavimai, taikomi fizinės kratos ir arešto

([1]) Šioje apžvalgoje neaprašomos su nacionaliniu saugumu susijusios tyrimo priemonės, kurias teisėsaugos institucijos naudoja vykdydamos terorizmo ir kitus nacionalinio saugumo tyrimus, įskaitant nacionalinio saugumo raštus (NSR) dėl tam tikrų įrašų informacijos kredito ataskaitose, finansinių įrašų ir elektroninių abonentų ir sandorių įrašų pagal 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 ir JAV kodekso 50 antraštinės dalies 3162 straipsnį, ir dėl elektroninio stebėjimo, kratos orderių, verslo įrašų ir kitos informacijos rinkimo pagal Užsienio žvalgybos informacijos sekimo aktą, JAV kodekso 50 antraštinės dalies 1801 ir paskesnius straipsnius.

([2]) Šiame rašte aptariamos federalinės teisėsaugos ir reguliavimo institucijos. Valstijų teisės pažeidimus tiria valstijų teisėsaugos institucijos, o bylos dėl pažeidimų nagrinėjamos valstijų teismuose. Valstijų teisėsaugos institucijos pagal valstijų teisę išduoda orderius ir potvarkius iš esmės taip pat, kaip aprašyta šiame rašte, tačiau gali būti, kad valstijų teisiniame procese taikomos valstijų konstitucijose ar įstatymuose nustatytos papildomos apsaugos priemonės, kurios yra griežtesnės, nei nustatytosios JAV Konstitucijoje. Valstijų teisėje nustatytos apsaugos priemonės turi būti bent lygiavertės JAV Konstitucijoje, įskaitant Ketvirtąją pataisą, bet ja neapsiribojant, nustatytoms priemonėms.

orderiams, taip pat orderiams dėl saugomo elektroninių ryšių turinio, išduotiems pagal Saugomų ryšių duomenų aktą, kaip aptarta toliau. Kai reikalavimas išduoti orderį netaikomas, pagal Ketvirtąją pataisą vis vien tikrinamas valdžios institucijų veiklos pagrįstumas. Todėl pačia Konstitucija užtikrinama, kad JAV Vyriausybė neturėtų neribotų arba savavališkų įgaliojimų areštuoti privačią informaciją ([3]).

Baudžiamosios teisėsaugos institucijos

Federaliniai prokurorai, kurie yra Teisingumo departamento pareigūnai, ir federalinių tyrimų agentai, įskaitant Teisingumo departamento teisėsaugos institucijos Federalinio tyrimų biuro (FTB) agentus, gali baudžiamojo tyrimo tikslais Jungtinėse Amerikos Valstijose veikiančioms korporacijoms nurodyti pateikti dokumentus ir kitą įrašų informaciją taikydami kelių rūšių privalomus teisinius procesus, įskaitant didžiosios kolegijos potvarkius, administracinius potvarkius ir kratos orderius, ir gali gauti kitų ryšių duomenų remdamiesi federaliniais baudžiamaisiais įgaliojimais slapta klausytis pokalbių ir registruoti renkamus numerius.

Didžiosios žiuri arba šaukimai į teismą. Baudžiamojo teismo šaukimai naudojami siekiant padėti teisėsaugos institucijoms vykdyti tikslinius tyrimus. Didžiosios žiuri potvarkis yra oficialus didžiosios žiuri prašymas (papratai pateikiamas federalinio prokuroro prašymu) padėti didžiajai žiuri atlikti konkretaus įtariamo baudžiamosios teisės pažeidimo tyrimą. Didžioji žiuri atlieka teismo tyrimo funkciją ir yra sudaroma teisėjo arba magistrato. Potvarkyje gali būti reikalaujama, kad asmuo liudytų teismo procese arba pateiktų veiklos įrašus, elektroniškai saugomą informaciją ar kitus materialius daiktus arba leistų su jais susipažinti. Informacija turi būti susijusi su tyrimu, o potvarkis negali būti nepagrįstas: pernelyg platus, sunkiai įvykdomas ar sukeliantis per didelę naštą. Gavėjas gali pateikti prašymą ginčyti potvarkį remdamasis šiais motyvais (žr. Federalinių baudžiamojo proceso taisyklių 17 taisyklę) . Tam tikromis aplinkybėmis teismo šaukimai dėl dokumentų gali būti naudojami po to, kai didžioji kolegija byloje priėmė sprendimą.

Įgaliojimai priimti administracinius potvarkius. Įgaliojimais priimti administracinius potvarkius galima pasinaudoti baudžiamuosiuose arba civiliniuose tyrimuose. Baudžiamosios teisėsaugos srityje pagal tam tikrus federalinius įstatymus leidžiama naudoti administracinius potvarkius reikalaujant pateikti veiklos įrašus, elektroniškai saugomą informaciją ar kitus materialius daiktus arba leisti su jais susipažinti vykdant tyrimus, susijusius su sukčiavimu sveikatos priežiūros srityje, smurtu prieš vaikus, slaptos tarnybos apsauga, kontroliuojamų medžiagų bylomis ir generalinių inspektorių tyrimais, kurie turi poveikio vyriausybės agentūroms. Jeigu vyriausybė siekia užtikrinti administracinio potvarkio vykdymą teisme, administracinio potvarkio gavėjas, kaip ir didžiosios kolegijos potvarkio gavėjas, gali teigti, jog potvarkis nepagrįstas, nes yra pernelyg platus, sunkiai įvykdomas arba sukelia per didelę naštą.

Teismo nutartys dėl renkamų numerių registratorių ir gaunamų skambučių sekiklių. Pagal renkamų numerių registratorių ir gaunamų skambučių sekiklių naudojimui taikomas baudžiamąsias nuostatas teisėsaugos institucija gali gauti teismo nutartį, kad tikruoju laiku gautų su turiniu nesusijusią skambinimo, nukreipimo, adresavimo ar signalizavimo informaciją apie telefono numerį arba el. pašto adresą, patvirtinus, kad nurodyta informacija yra svarbi vykstančiam baudžiamajam tyrimui (žr. JAV kodekso 18 antraštinės dalies 3121–3127 straipsnius). Tokio prietaiso naudojimas arba įdiegimas nesilaikant teisės aktų yra federalinis nusikaltimas.

Elektroninių ryšių privatumo aktas (ECPA). Valdžios institucijų galimybė susipažinti su informacija apie abonentą, srauto duomenimis ir saugomu ryšių turiniu, kuriuos turi interneto paslaugų teikėjai, telefono bendrovės ir kiti trečiųjų šalių paslaugų teikėjai, reglamentuojama papildomomis taisyklėmis pagal ECPA II antraštinę dalį, taip pat vadinamą Saugomų ryšių duomenų aktu (SCA) (JAV kodekso 18 antraštinės dalies 2701–2712 straipsniai). SCA nustatoma įstatymais įtvirtintų teisių į privatumą sistema, kuria ribojama teisėsaugos institucijų galimybė susipažinti su duomenimis, išskyrus duomenis, kurių pagal konstitucinę teisę reikalaujama iš vartotojų ir interneto paslaugų teikėjų abonentų. SCA nustatyti vis aukštesni privatumo apsaugos lygiai, atitinkantys duomenų rinkimo intervencinį pobūdį. Norėdamos gauti abonento registracijos informaciją, interneto protokolo (IP) adresus ir susijusias laiko žymas, taip pat sąskaitų informaciją,

([3]) Pirmiau aptartus Ketvirtosios pataisos principus dėl privatumo apsaugos ir saugumo interesų JAV teismai reguliariai taiko naujų rūšių teisėsaugos tyrimo priemonėms, kurių atsiranda dėl technologijų pažangos. Pavyzdžiui, 2018 m. Aukščiausiojo Teismo sprendimu, tai, kad valdžios institucijos, vykdydamos teisėsaugos tyrimą, iš mobiliojo ryšio bendrovės gavo ilgo laikotarpio istorinę mobiliojo ryšio vietos nustatymo informaciją, yra „paieška“, kuriai taikomas Ketvirtojoje pataisoje nustatytas reikalavimas išduoti orderį (žr. Sprendimą *Carpenter / Jungtinės Amerikos Valstijos*, 138 S. Ct. 2206 (2018)).

baudžiamosios teisėsaugos institucijos privalo gauti potvarkį. Dėl didžiosios dalies kitos saugomos su turiniu nesusijusios informacijos, pvz., el. laiškų antraščių be temos eilutės, baudžiamosios teisėsaugos institucija turi teisėjui nurodyti konkrečius faktus, įrodančius, kad prašoma informacija yra svarbi ir reikšminga vykstančiam baudžiamajam tyrimui. Kad gautų saugomą elektroninių ryšių turinį, baudžiamosios teisėsaugos institucijos paprastai privalo iš teisėjo gauti orderį remdamosi tikėtina priežastimi manyti, kad atitinkamoje paskyroje yra nusikalstamos veikos įrodymų. SCA taip pat nustatyta civilinė atsakomybė ir baudžiamosios sankcijos ([4]).

Teismo orderiai dėl stebėjimo pagal Federalinį slapto pokalbių klausymosi įstatymą. Be to, teisėsaugos institucijos pagal Federalinį slapto pokalbių klausymosi įstatymą gali tikruoju laiku perimti laidinių, žodinių ar elektroninių ryšių duomenis baudžiamojo tyrimo tikslais (žr. JAV kodekso 18 antraštinės dalies 2510–2523 straipsnius). Šiais įgaliojimais galima naudotis tik remiantis teismo nutartimi, kurioje teisėjas, be kita ko, nustato, kad yra pakankamas pagrindas manyti, jog slaptas pokalbių pasiklausymas arba elektroninių ryšių perėmimas bus federalinio nusikaltimo įrodymai. Įstatyme nustatyta civilinė atsakomybė ir baudžiamosios sankcijos už slapto pokalbių klausymosi pažeidimus.

Kratos orderis pagal Federalinių baudžiamojo proceso taisyklių 41 taisyklę. Teisėsaugos institucijos fiziškai atlikti kratą patalpose Jungtinėse Amerikos Valstijose gali gavusios atitinkamą teisėjo leidimą. Teisėsaugos institucijos, nurodydamos tikėtiną priežastį, privalo teisėjui įrodyti, kad buvo padaryta arba netrukus bus padaryta nusikalstama veika ir kad orderyje nurodytoje vietoje veikiausiai bus rasta su nusikalstama veika susijusių daiktų. Šiuo įgaliojimu dažnai naudojamasi, kai policija turi atlikti fizinę kratą patalpose, nes kyla pavojus, kad įrodymai gali būti sunaikinti, jeigu korporacijai bus įteiktas potvarkis ar kitas orderis pateikti įrodymus. Asmuo, kurio paties arba kurio turto krata atliekama, gali imtis veiksmų, kad panaikintų įrodymus, gautus arba įgytus neteisėtai atlikus kratą, jeigu tie įrodymai baudžiamajame procese pateikiami prieš tą asmenį. (žr. Sprendimą *Mapp / Ohajo valstija*, 367 U.S. 643 (1961)). Kai reikalaujama, kad duomenų turėtojas atskleistų duomenis pagal orderį, reikalavimą gavusi šalis reikalavimą atskleisti duomenis gali ginčyti dėl pernelyg didelės naštos Žr. *In Re Application of United States*, 610 F.2d 1148, 1157 (3 Cir. 1979) (laikant, jog „dėl tinkamo proceso reikalaujama, kad naštos klausimas būtų išnagrinėtas prieš įpareigojant telefono bendrovę teikti“ pagalbą pagal kratos orderį) ir *In re Application of United States*, 616 F.2d 1122 (9 Cir 1980) (kai tam tikra išvada padaroma remiantis teismo priežiūros įgaliojimais).

Teisingumo departamento gairės ir politika. Be šių Konstitucija, įstatymais ir taisyklėmis pagrįstų apribojimų valdžios institucijoms susipažinti su duomenimis, generalinis prokuroras paskelbė gaires, kuriose nustatyti papildomi teisėsaugos institucijų galimybės susipažinti su duomenimis apribojimai ir kuriose taip pat nustatyta privatumo ir piliečių laisvių apsaugos priemonių. Pavyzdžiui, Generalinio prokuroro gairėse dėl FTB vidaus operacijų (2008 m. rugsėjo mėn.) (toliau – GP FTB gairės), pateikiamose adresu http://www.justice.gov/archive/opa/docs/guidelines.pdf, nustatyti tyrimo priemonių naudojimo apribojimai siekiant gauti informacijos, susijusios su federalinės nusikalstamos veikos 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 „be abejo, FTB privalo tyrimus ir kitą veiklą vykdyti teisėtai ir pagrįstai, gerbdamas laisvę ir privatumą ir vengdamas be reikalo kištis į įstatymų besilaikančių žmonių gyvenimą“ (GP FTB gairės, p. 5). FTB šias gaires įtraukė į FTB vidaus tyrimų ir operacijų vadovą (DIOG), pateikiamą adresu https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29, – išsamų vadovą, kuriame smulkiai nurodomi tyrimo priemonių naudojimo apribojimai ir pateikiama rekomendacijų, kaip užtikrinti, kad atliekant kiekvieną tyrimą būtų saugomos piliečių laisvės ir privatumas. Papildomų taisyklių ir politikos priemonių, kuriomis nustatomi federalinių prokurorų tiriamosios veiklos apribojimai, pateikiama Teisingumo vadove, kuris taip pat skelbiamas internete adresu https://www.justice.gov/jm/justicemanual.

Pilietinės ir reguliavimo institucijos (viešasis interesas)

([4]) Be to, SCA 2705 straipsnio b dalyje valdžios institucijoms leidžiama gauti teismo nutartį įrodžius būtinybę užtikrinti apsaugą, kad informacija nebūtų atskleista; tokia nutartimi ryšių paslaugų teikėjui uždraudžiama savanoriškai pranešti naudotojams apie tai, kad pagal SCA pradėtas teisinis procesas. 2017 m. spalio mėn. generalinio prokuroro pavaduotojas Rodas Rosensteinas paskelbė Teisingumo departamento advokatams ir atstovams skirtą memorandumą, kuriame išdėstė gaires, kaip užtikrinti, kad prašymai išduoti tokius apsaugos orderius būtų pritaikyti prie konkrečių tyrimo faktų ir susirūpinimą keliančių klausimų, ir nustatė bendrą vienų metų terminą, kiek gali būti prašoma atidėti pranešimą. 2022 m. gegužės mėn. generalinio prokuroro pavaduotoja Lisa Monaco paskelbė papildomas gaires šia tema, kuriose, be kita ko, nustatė Teisingumo departamento vidaus reikalavimus dėl prašymų pratęsti apsaugos orderio galiojimą ilgiau nei pradiniam vienų metų laikotarpiui patvirtinimo ir nustatė reikalavimą, kad užbaigus tyrimą apsaugos orderiai būtų panaikinti.

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 sričių pareigų turinčios agentūros gali priimti korporacijoms skirtus potvarkius pateikti veiklos įrašus, elektroniškai saugomą informaciją ir kitus materialius daiktus. Tokioms agentūroms naudojantis savo įgaliojimais išduoti administracinį arba civilinį potvarkį, apribojimai taikomi ne tik pagal jų įstatus, bet ir atliekant nepriklausomą potvarkių teisminę peržiūrą prieš galimą vykdymo užtikrinimą teisme (žr. Federalinių civilinio proceso taisyklių 45 taisyklę). Agentūros gali prašyti leisti susipažinti tik su duomenimis, susijusiais su klausimais, kuriuos yra įgaliotos reguliuoti. Be to, administracinio potvarkio gavėjas gali ginčyti to potvarkio vykdymą teisme pateikdamas įrodymų, kad agentūra veikė nesilaikydama esminių pagrįstumo standartų, kaip aptarta pirmiau.

Administracinių agentūrų prašymus susipažinti su duomenimis bendrovės gali ginčyti remdamosi ir kitais teisiniais pagrindais pagal savo konkrečius sektorius ir turimų duomenų rūšis. Pavyzdžiui, finansų įstaigos administracinius potvarkius, kuriais siekiama gauti tam tikrų rūšių informacijos, gali ginčyti kaip Bankų paslapties akto ir jo įgyvendinimo reglamentų pažeidimus (JAV kodekso 31 antraštinės dalies 5318 straipsnis, Federalinių reglamentų kodekso 31 antraštinės dalies X skyrius). Kitos įmonės gali remtis Sąžiningo kredito informacijos teikimo aktu, t. y. JAV kodekso 15 antraštinės dalies 1681b straipsniu, arba įvairiais kitais atitinkamiems sektoriams skirtas teisės aktais. 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 3401–3423 straipsnius). Todėl Jungtinių Amerikos Valstijų teismai vykdo netinkamų reguliavimo prašymų atranką ir nepriklausomą federalinių agentūrų veiksmų priežiūrą.

Galiausiai visi administracinių institucijų turimi įstatymais įtvirtinti įgaliojimai fiziškai areštuoti Jungtinėse Amerikos Valstijose veikiančios bendrovės įrašus vykdant administracinę kratą turi atitikti pagal Ketvirtąją pataisą nustatytus reikalavimus (žr. Sprendimą *See* / *Siatlo miestas*, 387 U.S. 541 (1967)).

Išvada

Visa teisėsaugos ir reguliavimo veikla Jungtinėse Amerikos Valstijose turi atitikti taikomus teisės aktus, be kita ko, JAV Konstituciją, įstatymus, taisykles ir reglamentus. Tokia veikla taip pat turi atitikti taikomas politikos priemones, be kita ko, Generalinio prokuroro gaires, kuriomis reglamentuojama federalinių teisėsaugos institucijų veikla. 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.

Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

VII PRIEDAS

GENERALINIO ADVOKATO NACIONALINIO ŽVALGYBOS BIURO DIREKTORIAUS TARNYBA

VAŠINGTONAS, DC 20511

2022 m. gruodžio 9 d.

Generalinei advokatei
Leslie B. Kiernan
JAV prekybos departamentas
1401 Constitution
Ave., NW Washington, DC 20230

Gerb. L. B. Kiernan,

2022 m. spalio 7 d. Prezidentas J. Bidenas pasirašė Vykdomąjį potvarkį Nr. 14086 *dėl Jungtinių Amerikos Valstijų signalų žvalgybos veiklos apsaugos priemonių griežtinimo*, kuriuo stiprinamos JAV signalų žvalgybos veiklai taikomos griežtos privatumo ir piliečių laisvių apsaugos priemonės. Pagal šias apsaugos priemones, be kita ko: reikalaujama, kad signalų žvalgybos veikla atitiktų nurodytus teisėtus tikslus; aiškiai uždraudžiama vykdyti tokią veiklą siekiant konkrečių draudžiamų tikslų; įdiegiamos naujos procedūros, skirtos užtikrinti, kad signalų žvalgybos veikla padėtų siekti tų teisėtų tikslų ir nepadėtų siekti draudžiamų tikslų; reikalaujama, kad signalų žvalgybos veikla būtų vykdoma tik remiantis pagrįstu visų aktualių veiksnių įvertinimu nustačius, kad vykdyti veiklą būtina siekiant įgyvendinti patvirtintą žvalgybos prioritetą, ir tik tokiu mastu ir tokiu būdu, kuris yra proporcingas patvirtintam žvalgybos prioritetui, dėl kurio buvo suteiktas leidimas; nurodoma žvalgybos bendruomenės subjektams atnaujinti savo politiką ir procedūras, kad jos atitiktų Vykdomajame potvarkyje nustatytas reikalaujamas signalų žvalgybos apsaugos priemones. Svarbiausia, kad Vykdomuoju potvarkiu taip pat nustatomas nepriklausomas ir privalomas mechanizmas, pagal kurį asmenys iš „reikalavimus atitinkančių valstybių“, kaip nustatyta pagal Vykdomąjį potvarkį, gali ginti savo teises, jei mano, kad jų atžvilgiu neteisėtai vykdoma JAV signalų žvalgybos veikla, įskaitant veiklą, kuria pažeidžiamos Vykdomajame potvarkyje nustatytos apsaugos priemonės.

Prezidento J. Bideno paskelbtame Vykdomajame potvarkyje Nr. 14086, kuris vainikavo ilgiau nei metus trukusias nuodugnias Europos Komisijos (EK) ir Jungtinių Amerikos Valstijų atstovų derybas, nurodoma, kokių veiksmų Jungtinės Amerikos Valstijos imsis, kad įgyvendintų savo įsipareigojimus pagal ES ir JAV duomenų privatumo sistemą. Žinau, kad remiantis bendradarbiavimo dvasia, iš kurios ir kilo ši sistema, iš EK gavote du rinkinius klausimų apie tai, kaip žvalgybos bendruomenė įgyvendins Vykdomąjį potvarkį. Mielai atsakysiu į tuos klausimus šiame rašte.

1978 m. Užsienio žvalgybos informacijos sekimo akto 702 straipsnis (FISA 702 straipsnis)

Pirmasis klausimų rinkinys susijęs su FISA 702 straipsniu, pagal kurį leidžiama rinkti užsienio žvalgybos informaciją stebint ne JAV piliečius, kaip pagrįstai manoma, esančius ne Jungtinėse Amerikos Valstijose, naudojantis būtinąja elektroninių ryšių paslaugų teikėjų pagalba. Konkrečiai, klausimai susiję su tos nuostatos ir Vykdomojo potvarkio Nr. 14086 sąveika, taip pat su kitomis apsaugos priemonėmis, taikomomis pagal FISA 702 straipsnį vykdomai veiklai.

Pirmiausia galime patvirtinti, kad žvalgybos bendruomenė pagal FISA 702 straipsnį vykdomai veiklai taikys Vykdomajame potvarkyje Nr. 14086 nustatytas apsaugos priemones.

Be to, vyriausybei naudojantis FISA 702 straipsniu taikoma daug kitų apsaugos priemonių. Pavyzdžiui, visus pagal FISA 702 straipsnį išduodamus sertifikatus turi pasirašyti ir generalinis prokuroras, ir Nacionalinės žvalgybos direktorius (DNI), o vyriausybė visus tokius sertifikatus turi pateikti patvirtinti Užsienio žvalgybos stebėjimo teismui (FISC), kurį sudaro iki gyvos galvos dirbantys nepriklausomi teisėjai, šias pareigas einantys nepratęsiamą septynerių metų kadenciją. Sertifikatuose nurodomos rinktinos užsienio žvalgybos informacijos kategorijos, kurios turi atitikti teisės aktais nustatytą užsienio žvalgybos informacijos apibrėžtį, nustatant ne JAV piliečius, kaip pagrįstai manoma, esančius ne Jungtinėse Amerikos Valstijose, kurių informaciją norima rinkti. Sertifikatuose pateikiama informacijos apie tarptautinį terorizmą ir kitas temas, pvz., apie gaunamą informaciją apie masinio naikinimo ginklus. Kiekvienas metinis sertifikavimas turi būti pristatytas FISC patvirtinti pateikiant sertifikavimo paraiškos dokumentų rinkinį, kurį sudaro generalinio prokuroro ir DNI sertifikatai, tam tikrų žvalgybos agentūrų vadovų rašytiniai patvirtinimai, taip pat asmenų, kurių informaciją norima rinkti, nustatymo procedūros, duomenų kiekio mažinimo procedūros ir užklausų teikimo procedūros, kurių vyriausybė privalo laikytis. Pagal asmenų, kurių informaciją norima rinkti, nustatymo procedūras, be kita ko, reikalaujama, kad žvalgybos bendruomenė, atsižvelgdama į visas aplinkybes, pagrįstai įvertintų, ar taikant asmenų, kurių informaciją norima rinkti, nustatymo procedūras veikiausiai bus renkama pagal FISA 702 straipsnį išduotame sertifikate nurodyta užsienio žvalgybos informacija.

Be to, rinkdama informaciją pagal FISA 702 straipsnį, žvalgybos bendruomenė privalo: raštu paaiškinti, kokiu pagrindu remiamasi tuo metu, kai nustatomi asmenys, kurių informaciją norima rinkti, vertinant, ar tas asmuo, kaip numatoma, turi, gaus ar veikiausiai perduos pagal FISA 702 straipsnį išduodamame sertifikate nurodytos užsienio žvalgybos informacijos; patvirtinti, kad pagal FISA 702 straipsnį vykdomose procedūrose įtvirtinto asmenų, kurių informaciją norima rinkti, nustatymo standarto vis dar laikomasi; nutraukti duomenų rinkimą, jeigu to standarto nebesilaikoma (žr. JAV vyriausybės pateiktą informaciją Užsienio žvalgybos stebėjimo teismui, *2015 m. svarbių 702 straipsnio reikalavimų santrauka*, p. 2–3 (2015 m. liepos 15 d.)).

Reikalaujant, kad žvalgybos bendruomenė raštu registruotų ir reguliariai patvirtintų savo vertinimą, kad pagal FISA 702 straipsnį stebimi asmenys atitinka taikomus asmenų, kurių informaciją norima rinkti, nustatymo standartus, FISC lengviau prižiūrėti žvalgybos bendruomenės vykdomą asmenų, kurių informaciją norima rinkti, nustatymo veiklą. Kiekvieną užregistruotą asmenų, kurių informaciją norima rinkti, nustatymo vertinimą ir pagrindimą kas du mėnesius peržiūri Teisingumo departamento žvalgybos priežiūros prokurorai, kurie šią priežiūros funkciją vykdo nepriklausomai nuo užsienio žvalgybos operacijų. Šią funkciją atliekantis Teisingumo departamento skyrius pagal seniai galiojančią FISC taisyklę privalo FISC pranešti apie visus taikomų procedūrų pažeidimus. Tokie pranešimai, taip pat reguliarūs FISC ir to Teisingumo departamento skyriaus atstovų susitikimai dėl pagal FISA 702 straipsnį vykdomo asmenų, kurių informaciją norima rinkti, nustatymo priežiūros suteikia galimybę FISC užtikrinti, kad būtų laikomasi FISA 702 straipsnyje nustatytų asmenų, kurių informaciją norima rinkti, nustatymo ir kitų procedūrų, ir kitaip užtikrinti, kad vyriausybės veikla būtų teisėta. Konkrečiai, FISC tai gali padaryti įvairiais būdais, be kita ko, priimdamas privalomus taisomuosius sprendimus nutraukti vyriausybės įgaliojimus rinkti duomenis apie konkretų stebimą asmenį arba pakeisti ar atidėti duomenų rinkimą pagal FISA 702 straipsnį. FISC taip pat gali reikalauti, kad vyriausybė teiktų papildomas ataskaitas ar informacinius pranešimus apie tai, kaip laikosi asmenų, kurių informaciją norima rinkti, nustatymo ir kitų procedūrų, arba gali reikalauti pakeisti tas procedūras.

Masinis signalų žvalgybos duomenų rinkimas

Antrasis klausimų rinkinys susijęs su masiniu signalų žvalgybos duomenų rinkimu, kuris Vykdomajame potvarkyje Nr. 14086 apibrėžiamas kaip „leidžiamas didelio kiekio signalų žvalgybos duomenų, kurie dėl techninių ar operatyvinių priežasčių gaunami nenaudojant atskyrimo priemonių (pvz., netaikant konkrečių identifikatorių ar atrankos sąlygų), rinkimas“.

Dėl šių klausimų pirmiausia pažymime, kad nei FISA, nei nacionalinio saugumo raštais masiškai rinkti duomenų neleidžiama. Dėl FISA:

— FISA I ir III antraštinėse dalyse, kuriose atitinkamai leidžiamas elektroninis stebėjimas ir fizinės kratos, reikalaujama teismo nutarties (su nedidelėmis išimtimis, pvz., nepaprastosiomis aplinkybėmis) ir visada reikalaujama, kad būtų tikėtina priežastis manyti, kad stebimas subjektas yra užsienio valstybė arba užsienio valstybės agentas (žr. JAV kodekso 50 antraštinės dalies 1805 ir 1824 straipsnius);

— 2015 m. JAV laisvės aktu iš dalies pakeista FISA IV antraštinė dalis, pagal kurią naudoti renkamų numerių registratorius ir gaunamų skambučių sekiklius leidžiama remiantis teismo nutartimi (išskyrus nepaprastąsias aplinkybes), nustačius reikalavimą, kad vyriausybė teikdama prašymus remtųsi „konkrečia atrankos sąlyga“ (žr. JAV kodekso 50 antraštinės dalies 1842 straipsnio c dalies 3 punktą);

— pagal FISA V antraštinę dalį, pagal kurią Federaliniam tyrimų biurui (FTB) leidžiama gauti tam tikrų rūšių veiklos įrašus, reikalaujama, kad teismo nutartis būtų priimta remiantis prašymu, kuriame nurodyta, kad „yra konkrečių ir aiškių faktų, dėl kurių yra priežasčių manyti, kad asmuo, su kuriuo susiję įrašai, yra užsienio subjektas arba užsienio valstybės agentas“ (žr. JAV kodekso 50 antraštinės dalies 1862 straipsnio b dalies 2 punkto B papunktį ([1]));

— galiausiai pagal FISA 702 straipsnį leidžiama „siekiant gauti užsienio žvalgybos informacijos stebėti asmenis, kurie, kaip pagrįstai manoma, yra ne Jungtinėse Amerikos Valstijose“ (žr. JAV kodekso 50 antraštinės dalies 188la straipsnio a dalį). Taigi, kaip pažymėjo Privatumo ir piliečių laisvių priežiūros valdyba, vyriausybės vykdomas duomenų rinkimas pagal FISA 702 skirsnį „taikomas tik pavieniams asmenims ir siekiant gauti su tais asmenimis susijusių ryšių duomenų, iš kurių vyriausybė turi priežasčių tikėtis gauti tam tikrų rūšių užsienio žvalgybos informacijos“, todėl „pagal programą ryšių duomenys masiškai nerenkami“ (Privatumo ir piliečių laisvių priežiūros valdyba, *Pagal Užsienio žvalgybos informacijos sekimo akto 702 straipsnį vykdomos stebėjimo programos ataskaita*, p. 103 (2014 m. liepos 2 d.)) ([2]).

Dėl nacionalinio saugumo raštų 2015 m. JAV laisvės aktu nustatytas reikalavimas naudojant tokius raštus remtis „konkrečia atrankos sąlyga“ (žr. JAV kodekso 12 antraštinės dalies 3414 straipsnio a dalies 2 punktą, JAV kodekso 15 antraštinės dalies 1681u straipsnį, JAV kodekso 15 antraštinės dalies 1681v straipsnio a dalį, JAV kodekso 18 antraštinės dalies 2709 straipsnio b dalį).

Be to, Vykdomajame potvarkyje Nr. 14086 nustatyta, kad „[p]irmumas teikiamas tiksliniam duomenų rinkimui“, o kai žvalgybos bendruomenė vykdo masinį duomenų rinkimą, „masinis signalų žvalgybos duomenų rinkimas leidžiamas tik nustačius, <...> kad informacijos, būtinos siekiant įgyvendinti patvirtintą žvalgybos prioritetą, pagrįstai negalima gauti tikslinio rinkimo būdu“ (žr. Vykdomojo potvarkio Nr. 14086 2 straipsnio c dalies ii punkto A papunktį).

Be to, žvalgybos bendruomenei nustačius, kad masinis duomenų rinkimas atitinka šiuos standartus, Vykdomuoju potvarkiu Nr. 14086 nustatoma papildomų apsaugos priemonių. Konkrečiai, Vykdomajame potvarkyje reikalaujama, kad masiškai rinkdama duomenis žvalgybos bendruomenė „taikytų pagrįstus metodus ir technines priemones, kad duomenų būtų renkama ne daugiau, nei būtina patvirtintam žvalgybos prioritetui įgyvendinti, taip pat būtų renkama kuo mažiau nesusijusios informacijos“ (žr. ten pat). Potvarkyje taip pat nurodyta, kad „signalų žvalgybos veikla“, kuri apima užklausas dėl masiškai renkamų signalų žvalgybos duomenų, „vykdoma tik remiantis pagrįstu visų aktualių veiksnių įvertinimu nustačius, kad vykdyti veiklą būtina siekiant įgyvendinti patvirtintą žvalgybos prioritetą“ (žr. ten pat, 2 straipsnio a dalies ii punkto A papunktį). Potvarkyje šis principas taip pat įgyvendinamas nurodant, kad žvalgybos bendruomenė gali teikti užklausas tik dėl nesumažinto kiekio signalų žvalgybos duomenų, masiškai gautų siekiant šešių leidžiamų tikslų, ir kad tokios užklausos turi būti vykdomos laikantis politikos ir procedūrų, kuriomis „tinkamai atsižvelgiama į [užklausų] poveikį visų asmenų privatumui ir piliečių laisvėms, neatsižvelgiant į jų pilietybę ar gyvenamąją vietą“ (žr. ten pat, 2 straipsnio c dalies iii punkto D papunktį). Galiausiai įsake numatytos surinktų duomenų tvarkymo, saugumo užtikrinimo ir galimybės susipažinti su duomenimis kontrolės priemonės (žr. ten pat, 2 straipsnio c dalies iii punkto A papunktį ir 2 straipsnio c dalies iii punkto B papunktį).

* * * * *

Tikimės, kad šie paaiškinimai bus naudingi. Jeigu turite papildomų klausimų, kaip JAV žvalgybos bendruomenė ketina įgyvendinti Vykdomąjį potvarkį Nr. 14086, nedvejodami kreipkitės į mus.

([1]) 2001–2020 m. pagal FISA V antraštinę dalį FTB buvo leidžiama prašyti FISC leidimo gauti „materialius daiktus“, kurie yra susiję su tam tikrais patvirtintais tyrimais (žr. JAV patriotų aktą, Oficialusis leidinys Nr. 107–56, 115 Stat. 272, 215 straipsnis (2001)). Šioje formuluotėje, kuri nebegalioja, taigi nebėra teisės aktas, buvo numatytas įgaliojimas, pagal kurį vyriausybė vienu metu masiškai rinko telefonijos metaduomenis. Tačiau dar iki tol, kol ta nuostata nustojo galioti, JAV laisvės aktu ji buvo iš dalies pakeista nustatant reikalavimą, kad vyriausybė teikdama FISC prašymą remtųsi „konkrečia atrankos sąlyga“ (žr. JAV laisvės aktą, Oficialusis leidinys Nr. 114–23129 Stat. 268, I 03 straipsnis (2015)).

([2]) Pagal 703 ir 704 straipsnius, pagal kuriuos žvalgybos bendruomenei leidžiama stebėti užsienyje esančius JAV piliečius, reikalaujama teismo nutarties (išskyrus nepaprastąsias aplinkybes) ir visada reikalaujama, kad būtų tikėtina priežastis manyti, kad stebimas subjektas yra užsienio valstybė, užsienio valstybės agentas arba užsienio valstybės pareigūnas ar darbuotojas (žr. JAV kodekso 50 antraštinės dalies 1881b ir1881c straipsnius).

Sincerely,

Christopher C. FONZONE
Generalinis advokatas

VIII PRIEDAS

Santrumpų sąrašas

Šiame sprendime vartojamos šios santrumpos:

AAA	Amerikos arbitražo asociacija
GP reglamentas	Generalinio prokuroro reglamentas dėl Duomenų apsaugos apeliacinio teismo
AGG-DOM	Generalinio prokuroro gairės dėl vidaus FTB operacijų
APA	Administracinių procedūrų aktas
CŽA	Centrinė žvalgybos agentūra
CNSS	Nacionalinio saugumo sistemų komitetas
Teisingumo Teismas	Europos Sąjungos Teisingumo Teismas
Sprendimas	Komisijos įgyvendinimo sprendimas, priimtas pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679, dėl tinkamo asmens duomenų apsaugos lygio pagal ES ir JAV duomenų privatumo sistemą
VSD	Vidaus saugumo departamentas
DNI	Nacionalinės žvalgybos direktorius
PD	JAV Prekybos departamentas
DOJ	JAV Teisingumo departamentas
DoT	JAV Transporto departamentas
DAI	Duomenų apsaugos institucija
DPS sąrašas	Duomenų privatumo sistemos sąrašas
DPRC	Duomenų apsaugos apeliacinis teismas
ECOA	Vienodų galimybių gauti kreditą aktas
ECPA	Elektroninių ryšių privatumo aktas
EEE	Europos ekonominė erdvė
VP 12333	Vykdomasis potvarkis Nr. 12333 „Jungtinių Amerikos Valstijų žvalgybos veikla“
VP 14086, VP	Vykdomasis potvarkis Nr. 14086 „Jungtinių Amerikos Valstijų signalų žvalgybos veiklos apsaugos priemonių griežtinimas“
ES ir JAV DPS arba DPS	ES ir JAV duomenų privatumo sistema
ES ir JAV DPS kolegija	ES ir JAV duomenų privatumo sistemos kolegija
FTB	Federalinis tyrimų biuras
FCRA	Sąžiningo kredito informacijos teikimo aktas
FISA	Užsienio žvalgybos stebėjimo aktas
FISC	Užsienio žvalgybos stebėjimo teismas
FISCR	Apeliacinis užsienio žvalgybos stebėjimo teismas
FOIA	Informacijos laisvės aktas
FRA	Federalinių registrų aktas

FPK	JAV federalinė prekybos komisija
HIPAA	Sveikatos draudimo perkeliamumo ir atskaitomybės aktas
ICDR	Tarptautinis ginčų sprendimo centras
IOB	Žvalgybos priežiūros valdyba
NIST	Nacionalinis standartų ir technologijų institutas
NSA	Nacionalinio saugumo agentūra
NSR	Nacionalinio saugumo raštas (-ai)
ODNI	Nacionalinės žvalgybos direktoriaus biuras
ODNI CLPO, CLPO	Nacionalinės žvalgybos direktoriaus biuro piliečių laisvių apsaugos pareigūnas
OMB	Valdymo ir biudžeto tarnyba
OPCL	Teisingumo departamento Privatumo ir piliečių laisvių tarnyba
PCLOB	Privatumo ir piliečių laisvių priežiūros valdyba
PIAB	Prezidento žvalgybos patariamoji taryba
PPD 28	Prezidento politikos direktyva Nr. 28
Reglamentas (ES) 2016/679	2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB
SAOP	Vyresnysis agentūros privatumo apsaugos pareigūnas
Principai	ES ir JAV duomenų privatumo sistemos principai
JAV	Jungtinės Amerikos Valstijos
Sąjunga	Europos Sąjunga