Rekomendacijos Nr. 01/2020 dėl priemonių duomenų perdavimo priemonėms papildyti, siekiant užtikrinti atitiktį ES asmens duomenų apsaugos lygiui

Versija 2.0

Priimta 2021 m. birželio 18 d.

Ankstesnės versijos

Versija 2.0	2021 m. birželio 18 d.	Rekomendacijų priėmimas po viešų konsultacijų
Versija 1.0	2020 m. lapkričio 10 d.	Rekomendacijų priėmimas viešoms konsultacijoms

Santrauka

ES bendrasis duomenų apsaugos reglamentas (BDAR) buvo priimtas siekiant dviejų tikslų: palengvinti laisvą asmens duomenų judėjimą Europos Sąjungoje, kartu išsaugant pagrindines asmenų teises ir laisves, ypač jų teisę į asmens duomenų apsaugą.

Neseniai priimtame sprendime C-311/18 (*Schrems II*) Europos Sąjungos Teisingumo Teismas (ESTT) primena, kad asmens duomenų apsauga Europos ekonominėje erdvėje (EEE) turi būti užtikrinta visur, kad ir kur duomenys būtų perduodami. Asmens duomenų perdavimas trečiosioms valstybėms negali būti priemonė pakenkti EEE teikiamai apsaugai ar ją sumažinti. Šiuo atžvilgiu Teismas taip pat paaiškina, kad apsaugos lygis trečiosiose valstybėse neturi būti identiškas EEE garantuojamam apsaugos lygiui, bet turi būti iš esmės lygiavertis. Teismas taip pat patvirtina standartinių sutarčių sąlygų, kaip perdavimo priemonės, galinčios padėti užtikrinti iš esmės lygiavertį į trečiąsias valstybes perduodamų duomenų apsaugos lygį, tinkamumą.

BDAR 46 straipsnyje nurodytos standartinės sutarčių sąlygos ir kitos duomenų perdavimo priemonės neveikia vakuume. Teismas nurodo, kad duomenų valdytojai arba duomenų tvarkytojai, atliekantys duomenų eksportuotojų funkciją, kiekvienu konkrečiu atveju ir prireikus bendradarbiaudami su duomenų importuotoju trečiojoje valstybėje privalo patikrinti, ar trečiosios valstybės teisė ar praktika mažina BDAR 46 straipsnyje nurodytoms perdavimo priemonėms skirtų tinkamų apsaugos priemonių veiksmingumą. Tais atvejais Teismas vis tiek palieka duomenų eksportuotojams galimybę įgyvendinti papildomas priemones, kurios užpildo šias apsaugos spragas ir padidina apsaugos lygį iki reikalaujamo ES teisės aktais. Teismas nepatikslina, kokios priemonės tai galėtų būti. Tačiau Teismas pabrėžia, kad duomenų eksportuotojai turi jas nurodyti kiekvienu konkrečiu atveju. Tai atitinka BDAR 5 straipsnio 2 dalyje nustatytą atskaitomybės principą, pagal kurį duomenų valdytojai turi būti atsakingi už BDAR principų dėl asmens duomenų tvarkymo laikymąsi ir gebėti įrodyti, kad jų laikomasi.

Siekdama padėti duomenų eksportuotojams (nesvarbu, ar jie duomenų valdytojai, ar duomenų tvarkytojai, privatūs subjektai ar viešosios įstaigos, tvarkančios asmens duomenis BDAR taikymo srityje) atlikti sudėtingą užduotį – įvertinti trečiąsias valstybes ir prireikus nustatyti tinkamas papildomas priemones, Europos duomenų apsaugos valdyba (EDAV) priėmė šias rekomendacijas. Šiose rekomendacijose duomenų eksportuotojams nurodomi veiksmai, kurių reikia imtis, galimi informacijos šaltiniai ir papildomi taikytinų priemonių pavyzdžiai.

Pirmuoju etapu EDAV pataria jums, duomenų eksportuotojams, **žinoti apie savo perdavimus**. Stebėti visus asmens duomenų perdavimus trečiosioms valstybėms gali būti sudėtinga. Vis dėlto žinoti, kur keliauja asmens duomenys, yra būtina, siekiant užtikrinti, kad jiems būtų užtikrintas iš esmės lygiavertis apsaugos lygis, kad ir kur jie būtų tvarkomi. Taip pat turite patikrinti, ar jūsų perduodami duomenys yra adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie yra tvarkomi.

Antruoju etapu reikia **įvertinti jūsų naudojamą perdavimo priemonę** pagal BDAR V skyriuje pateiktą sąrašą. Jeigu Europos Komisija vienu iš savo sprendimų dėl tinkamumo pagal BDAR 45 straipsnį arba pagal ankstesnę Direktyvą 95/46, jau paskelbė, kad valstybė, regionas ar sektorius, į kuriuos perduodate duomenis, yra tinkami, tol, kol sprendimas tebegalioja, jums nereikės imtis jokių kitų veiksmų, išskyrus stebėti, ar sprendimas dėl tinkamumo tebegalioja. Jei nepriimtas sprendimas dėl tinkamumo, reikia taikyti vieną iš BDAR 46 straipsnyje išvardytų perdavimo priemonių. Tik kai kuriais atvejais galite remtis viena iš BDAR 49 straipsnio nukrypti leidžiančių nuostatų, jei atitinkate sąlygas. Nukrypti leidžiančios nuostatos praktiškai negali tapti „taisykle“, bet turi būti taikomos tik konkrečiais atvejais.

Trečiuoju etapu reikia **įvertinti**, ar trečiosios valstybės galiojančioje teisėje ir (arba) esamoje praktikoje yra kokių nors elementų, kurie galėtų sumažinti jūsų naudojamų perdavimo priemonių apsaugos priemonių veiksmingumą vykdant konkretų perdavimą. Jūsų vertinimas visų pirma turėtų būti sutelktas į su jūsų vykdomu perdavimu susijusius trečiosios valstybės teisės aktus ir į jūsų naudojamą BDAR 46 straipsnyje nurodytą perdavimo priemonę. Išnagrinėję trečiosios valstybės valdžios institucijų

praktiką taip pat galėsite patikrinti, ar perdavimo priemonėje numatytomis apsaugos priemonėmis galima praktiškai užtikrinti veiksmingą perduodamų asmens duomenų apsaugą. Šios praktikos nagrinėjimas bus ypač svarbus vertinant, ar:

(i.) trečiosios valstybės teisės aktai, oficialiai atitinkantys ES standartus, akivaizdžiai nėra taikomi ir (arba) jų nesilaikoma praktiškai;

(ii.) esama praktikos, nesuderinamos su perdavimo priemonės įsipareigojimais, kai trečiojoje valstybėje nėra atitinkamų teisės aktų;

(iii.) jūsų perduoti duomenys ir (arba) duomenų importuotojas patenka arba gali patekti į probleminių teisės aktų taikymo sritį (t. y. pažeidžia perdavimo priemonės sutartinę garantiją dėl iš esmės lygiaverčio apsaugos lygio ir neatitinka ES pagrindinių teisių, būtinumo ir proporcingumo standartų).

Pirmaisiais dviem atvejais, jei pageidaujate, turėsite sustabdyti duomenų perdavimą arba įgyvendinti atitinkamas papildomas priemones.

Trečiuoju atveju, atsižvelgdami į neaiškumus, susijusius su galimu probleminių teisės aktų taikymu jūsų duomenų perdavimui, galite nuspręsti: sustabdyti perdavimą, įgyvendinti papildomas priemones, kad būtų galima jį tęsti, arba galite nuspręsti toliau perduoti duomenis neįgyvendindami papildomų priemonių, jei manote, kad neturite pagrindo manyti, jog atitinkami ir probleminiai teisės aktai bus aiškinami ir (arba) taikomi praktikoje taip, kad jie būtų taikomi jūsų perduotiems duomenims ir duomenų importuotojui, ir jei galite tai įrodyti ir patvirtinti dokumentais.

Norėdami įvertinti elementus, į kuriuos reikia atsižvelgti vertinant trečiosios valstybės teisę, susijusią su valdžios institucijų prieiga prie duomenų stebėjimo tikslais, vadovaukitės EDAV rekomendacijomis dėl Europos pagrindinių garantijų.

Šį vertinimą turėtumėte atlikti kruopščiai ir išsamiai jį dokumentuoti. Jūsų kompetentingos priežiūros ir (arba) teisminės institucijos gali to paprašyti ir reikalauti, kad jūs būtumėte atskaitingi už visus tuo pagrindu priimtus sprendimus.

Ketvirtuoju etapu reikia **nustatyti ir priimti papildomas priemones**, būtinas siekiant užtikrinti, kad perduodamų duomenų apsaugos lygis atitiktų ES esminio lygiavertiškumo standartą. Šis etapas būtinas tik tuo atveju, jei jūsų vertinimas rodo, kad trečiosios valstybės teisės aktai ir (arba) praktika mažina BDAR 46 straipsnyje nurodytos perdavimo priemonės, kurią jūs taikote ar ketinate taikyti perduodami duomenis, veiksmingumą. Rekomendacijose (2 priede) taip pat pateikiamas nebaigtinis papildomų priemonių pavyzdžių ir kai kurių sąlygų, kad jos būtų veiksmingos, sąrašas. Kaip ir 46 straipsnyje nurodytų perdavimo priemonių apsaugos priemonių atveju, kai kurios papildomos priemonės gali būti veiksmingos kai kuriose valstybėse, bet nebūtinai kitose. Esate atsakingi už jų veiksmingumo vertinimą perduodant duomenis, atsižvelgiant į trečiosios valstybės teisę bei praktiką ir jūsų taikomą perdavimo priemonę, nes esate atsakingi už visus tuo pagrindu priimtus sprendimus. Dėl to jums taip pat gali prireikti derinti keletą papildomų priemonių. Galbūt galiausia konstatuosite, kad jokia papildoma priemonė negali užtikrinti iš esmės lygiaverčio apsaugos lygio konkrečiai jūsų vykdomam duomenų perdavimui. Tais atvejais, kai jokia papildoma priemonė nėra tinkama, turite vengti duomenų perdavimo, jį sustabdyti arba nutraukti, kad nebūtų pakenkta asmens duomenų apsaugos lygiui. Taip pat turėtumėte kruopščiai atlikti papildomų priemonių vertinimą ir jį dokumentuoti.

Penktuoju etapu reikia **imtis visų formalių procedūrinių veiksmų**, kurių gali prireikti jums priimant papildomą priemonę, atsižvelgiant į jūsų taikomą BDAR 46 straipsnyje nurodytą perdavimo priemonę. Tam tikros formalios procedūros nurodytos šiose rekomendacijose. Dėl kai kurių iš jų jums gali prireikti pasikonsultuoti su savo kompetentingomis priežiūros institucijomis.

Šeštajame, t. y. paskutiniame, etape turėsite atitinkamais laiko tarpais iš naujo įvertinti asmens duomenų, kuriuos perduodate į trečiąsias valstybes, apsaugos lygį ir stebėti, ar yra ir ar bus kokių nors pokyčių, kurie gali turėti jam įtakos. Pagal atskaitomybės principą būtina nuolat atidžiai stebėti asmens duomenų apsaugos lygį.

Priežiūros institucijos toliau vykdys savo įgaliojimus stebėti, kaip taikomas BDAR, ir užtikrinti jo vykdymą. Priežiūros institucijos deramai atsižvelgs į veiksmus, kurių duomenų eksportuotojai imasi, kad užtikrintų, jog jų perduodamiems duomenims būtų suteikta iš esmės lygiaverčio lygio apsauga. Kaip primena Teismas, priežiūros institucijos sustabdo arba uždraudžia duomenų perdavimą tais atvejais, kai po tyrimo ar skundo nustato, kad neįmanoma užtikrinti iš esmės lygiaverčio apsaugos lygio.

Priežiūros institucijos ir toliau rengs rekomendacijas duomenų eksportuotojams ir koordinuos savo veiksmus Europos duomenų apsaugos valdyboje, kad užtikrintų nuoseklų ES duomenų apsaugos teisės aktų taikymą.

TURINYS

Europos duomenų apsaugos valdyba,

atsižvelgdama į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – BDAR) 70 straipsnio 1 dalies e punktą,

atsižvelgdama į Europos ekonominės erdvės (EEE) susitarimą, ypač į jo XI priedą ir 37 protokolą su pakeitimais, padarytais 2018 m. liepos 6 d. EEE jungtinio komiteto sprendimu Nr. 154/2018[1],

atsižvelgdama į Darbo tvarkos taisyklių 12 ir 22 straipsnius,

kadangi:

(1) Europos Sąjungos Teisingumo Teismas (toliau – ESTT) 2020 m. liepos 16 d. sprendime *Data Protection Commissioner / Facebook Ireland Limited ir Maximillian Schrems*, C-311/18, daro išvadą, kad BDAR 46 straipsnio 1 dalis ir 2 dalies c punktas turi būti aiškinami taip, kad šiose nuostatose reikalaujamomis tinkamomis apsaugos priemonėmis, įgyvendinamomis teisėmis ir veiksmingomis duomenų subjektų teisių gynimo priemonėmis turi būti užtikrinama, kad asmenų, kurių asmens duomenys perduodami į trečiąją valstybę remiantis standartinėmis duomenų apsaugos sąlygomis, teisių apsaugos lygis būtų iš esmės lygiavertis tam, kuris garantuojamas Europos Sąjungoje šiuo reglamentu, siejamu su Europos Sąjungos pagrindinių teisių chartija[2].

(2) Kaip pabrėžė Teismas, fizinių asmenų apsaugos lygis, iš esmės lygiavertis tam, kuris užtikrinamas Europos Sąjungoje pagal BDAR, siejant su Chartija, turi būti užtikrintas, kad ir kokia būtų V skyriaus nuostata, kuria remiantis asmens duomenys perduodami į trečiąją valstybę. V skyriaus nuostatomis siekiama užtikrinti to aukšto lygio apsaugos tęstinumą, kai asmens duomenys perduodami į trečiąją valstybę[3].

(3) BDAR 108 konstatuojamojoje dalyje ir 46 straipsnio 1 dalyje nustatyta, kad tuo atveju, jei sprendimas dėl tinkamumo nepriimtas, duomenų valdytojas arba duomenų tvarkytojas turėtų duomenų subjektams numatyti tinkamas apsaugos priemones nepakankamai duomenų apsaugai trečiojoje valstybėje kompensuoti. Duomenų valdytojas arba tvarkytojas gali užtikrinti tinkamas apsaugos priemones, nereikalaudamas jokio specialaus priežiūros institucijos leidimo, naudodamasis viena iš BDAR 46 straipsnio 2 dalyje išvardytų perdavimo priemonių, pavyzdžiui, standartinėmis duomenų apsaugos sąlygomis.

(4) Teismas paaiškina, kad Komisijos priimtomis standartinėmis duomenų apsaugos sąlygomis siekiama tik suteikti sutartines garantijas, vienodai taikomas visose trečiosiose valstybėse Sąjungoje įsisteigusiems duomenų valdytojams ir tvarkytojams. Dėl savo sutartinio pobūdžio standartinės

[1] Šioje nuomonėje daromos nuorodos į valstybes nares turėtų būti suprantamos kaip nuorodos į EEE valstybes nares.
[2] 2020 m. liepos 16 d. ESTT sprendimo *Data Protection Commissioner / Facebook Ireland Ltd ir Maximillian Schrems* (toliau – sprendimas byloje C-311/18 (*Schrems II*)) antra išvada.
[3] Sprendimo *Schrems II* byloje C-311/18 92 ir 93 punktai.

duomenų apsaugos sąlygos negali būti privalomos trečiųjų valstybių valdžios institucijoms, nes jos nėra sutarties šalys. Todėl duomenų eksportuotojams gali prireikti papildyti tose standartinėse duomenų apsaugos sąlygose numatytas garantijas papildomomis priemonėmis, kad būtų užtikrintas pagal ES teisę konkrečioje trečiojoje valstybėje reikalaujamas apsaugos lygis. Teismas remiasi BDAR 109 konstatuojamąja dalimi, kurioje minima ši galimybė ir duomenų valdytojai bei duomenų tvarkytojai skatinami ja naudotis[4].

(5) Teismas nurodė, jog duomenų valdytojas arba duomenų tvarkytojas, visų pirma kiekvienu atveju ir prireikus bendradarbiaudamas su duomenų gavėju, turi patikrinti, ar pagal paskirties trečiosios valstybės teisę užtikrinama tinkama, atsižvelgiant į ES teisę, asmens duomenų, perduodamų remiantis standartinėmis duomenų apsaugos sąlygomis, apsauga ir prireikus suteikiama papildomų garantijų, be tų, kurios numatytos šiose sąlygose[5].

(6) Jeigu duomenų valdytojas arba tvarkytojas, įsteigti Europos Sąjungoje, negali imtis papildomų priemonių, kad užtikrintų apsaugos lygį, iš esmės lygiavertį tam, kuris garantuojamas pagal ES teisę, duomenų valdytojas arba tvarkytojas arba, jei jie to padaryti negali – subsidiariai kompetentinga priežiūros institucija privalo sustabdyti arba nutraukti asmens duomenų perdavimą į atitinkamą trečiąja valstybę[6].

(7) Nei BDAR, nei Teisingumo Teismas neapibrėžia ir nepatikslina „papildomų apsaugos priemonių“ ir „papildomų priemonių“, skirtų papildyti BDAR 46 straipsnio 2 dalyje išvardytų perdavimo priemonių apsaugos priemones, kurias duomenų valdytojai ir tvarkytojai gali patvirtinti, kad konkrečioje trečiojoje valstybėje būtų užtikrintas pagal ES teisę reikalaujamas apsaugos lygis.

(8) EDAV nusprendė savo iniciatyva išnagrinėti šį klausimą ir pateikti duomenis eksportuojantiems duomenų valdytojams ir tvarkytojams rekomendacijas dėl galimų papildomų priemonių nustatymo ir patvirtinimo procedūrų. Šiomis rekomendacijomis siekiama duomenų eksportuotojams pateikti metodiką, pagal kurią jie galėtų nustatyti ar reikia taikyti papildomas priemones perduodant duomenis ir, jei taip, kokias. Pagrindinė duomenų eksportuotojų pareiga – užtikrinti, kad trečiojoje valstybėje perduodamiems duomenims būtų užtikrintas apsaugos lygis, iš esmės lygiavertis tam, kuris garantuojamas EEE. Šiomis rekomendacijomis EDAV siekia paskatinti nuosekliai taikyti BDAR ir Teismo sprendimą pagal EDAV suteiktus įgaliojimus[7],

PRIĖMĖ ŠIĄ REKOMENDACIJĄ:

[4] Sprendimo byloje C-311/18 (*Schrems II*) 132 ir 133 punktai.
[5] Sprendimo byloje C-311/18 (*Schrems II*) 134 punktas.
[6] Sprendimo byloje C-311/18 (*Schrems II*) 135 punktas.
[7] BDAR 70 straipsnio 1 dalies e punktas.

1 ATSKAITOMYBĖ PERDUODANT DUOMENIS

1. ES pirminėje teisėje teisė į duomenų apsaugą laikoma pagrindine teise[8]. Todėl teisei į duomenų apsaugą suteikiama aukšto lygio apsauga, o apribojimai galimi tik tuo atveju, jei jie numatyti įstatymo, nekeičia teisės esmės, yra proporcingi, būtini ir tikrai atitinka Sąjungos pripažintus bendrus interesus arba reikalingi kitų teisėms ir laisvėms apsaugoti[9]. Teisė į asmens duomenų apsaugą nėra absoliuti; ji turi būti vertinama atsižvelgiant į jos visuomeninę paskirtį ir derėti su kitomis pagrindinėmis teisėmis, remiantis proporcingumo principu[10].

2. Kai duomenys perduodami EEE nepriklausančioms trečiosioms valstybėms, jiems turi būti užtikrintas apsaugos lygis, iš esmės lygiavertis tam, kuris garantuojamas ES, siekiant užtikrinti, kad nebūtų pakenkta BDAR garantuojamam apsaugos lygiui tiek perdavimo metu, tiek po jo.

3. Teisė į duomenų apsaugą yra aktyvaus pobūdžio. Ji įpareigoja duomenų eksportuotojus ir duomenų importuotojus (nesvarbu, ar jie yra duomenų valdytojai ar tvarkytojai) neapsiriboti šios teisės pripažinimu ar pasyviu paisymu[11]. Duomenų valdytojai ir duomenų tvarkytojai turi stengtis aktyviai ir nuolat užtikrinti teisę į duomenų apsaugą, įgyvendindami teisines, technines ir organizacines priemones, kuriomis užtikrinamas apsaugos veiksmingumas. Duomenų valdytojai ir tvarkytojai taip pat turi sugebėti parodyti šias pastangas duomenų subjektams ir duomenų apsaugos priežiūros institucijoms. Tai vadinamasis atskaitomybės principas[12].

4. Atskaitomybės principas, kuris yra būtinas siekiant užtikrinti veiksmingą BDAR suteikto apsaugos lygio taikymą, taip pat taikomas duomenų perdavimui į trečiąsias valstybes[13], nes tai yra duomenų tvarkymo forma[14]. Kaip pabrėžė Teismas, apsaugos lygis, iš esmės lygiavertis tam, kuris užtikrinamas Europos Sąjungoje pagal BDAR, siejant su Chartija, turi būti užtikrintas, kad ir kokia būtų to skyrius nuostata, kuria remiantis asmens duomenys perduodami į trečiąją valstybę[15].

5. Sprendime *Schrems II* Teismas pabrėžia duomenų eksportuotojų ir duomenų importuotojų atsakomybę užtikrinti, kad dabar ir ateityje asmens duomenys būtų tvarkomi laikantis ES duomenų apsaugos teisėje nustatyto apsaugos lygio, ir sustabdyti duomenų perdavimą ir (arba) nutraukti sutartį, jei duomenų importuotojas negali arba nebegali laikytis standartinių duomenų apsaugos sąlygų, įtrauktų į atitinkamą duomenų eksportuotojo ir duomenų importuotojo sutartį[16]. Duomenis eksportuojantis duomenų valdytojas arba duomenų tvarkytojas turi užtikrinti, kad duomenų importuotojai prireikus bendradarbiautų su šias pareigas vykdančiu duomenų eksportuotoju, informuodami jį, pavyzdžiui, apie visus pokyčius, turinčius įtakos duomenų

[8] Pagrindinių teisių chartijos 8 straipsnio 1 dalis ir SESV 16 straipsnio 1 dalis, BDAR 1 konstatuojamoji dalis, 1 straipsnio 2 dalis.
[9] ES pagrindinių teisių chartijos 52 straipsnio 1 dalis.
[10] BDAR 4 konstatuojamoji dalis ir sprendimo *Google LLC, Google Inc. teisių perėmėja / Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17, 60 punktas.
[11] Žr. 2010 m. birželio 17 d. generalinės advokatės E. Sharpston išvados byloje *Volker und Markus Schecke GbR / Land Hessen*, C-92/09 ir C-93/02, 71 punktą.
[12] BDAR 5 straipsnio 2 dalis ir 28 straipsnio 3 dalies h punktas.
[13] BDAR 44 straipsnis ir 101 konstatuojamoji dalis, taip pat BDAR 47 straipsnio 2 dalies d punktas.
[14] 2015 m. spalio 6 d. ESTT sprendimo *Maximillian Schrems / Data Protection Commissioner* (toliau – sprendimas byloje C-362/14 (*Schrems I*) 45 punktas.
[15] Sprendimo *Schrems II* byloje C-311/18 92 ir 93 punktai.
[16] Sprendimo byloje C-311/18 (*Schrems II*) 134, 135, 139, 140, 141, 142 punktai.

importuotojo valstybėje gautų asmens duomenų apsaugai[17]. Vykdant šias pareigas BDAR nustatytas atskaitomybės principas pritaikomas duomenų perdavimui[18].

2 VEIKSMŲ GAIRĖS: PRAKTINIS ATSKAITOMYBĖS PRINCIPO TAIKYMAS DUOMENŲ PERDAVIMUI

6. Toliau pateikiamos gairės dėl veiksmų, kurių reikia imtis siekiant išsiaiškinti, ar jums (duomenų eksportuotojui) reikia parengti papildomas priemones, kad galėtumėte teisėtai perduoti duomenis už EEE ribų. „Jūs“ šiame dokumente reiškia duomenų valdytoją arba duomenų tvarkytoją, kuris veikia kaip duomenų eksportuotojas[19], tvarkantis asmens duomenis BDAR taikymo srityje, įskaitant tvarkymą, kurį atlieka privatūs subjektai ir viešosios įstaigos, perduodami duomenis privačioms įstaigoms[20]. Kalbant apie asmens duomenų perdavimą tarp viešųjų įstaigų, specialios rekomendacijos numatytos *Gairėse Nr. 2/2020 dėl Reglamento (ES) 2016/679 46 straipsnio 2 dalies a punkto ir 46 straipsnio 3 dalies b punkto, kai asmens duomenys perduodami tarp EEE ir ne EEE valdžios institucijų ir įstaigų*[21].

7. Turite tinkamai dokumentuoti šį vertinimą ir jūsų pasirinktas bei įgyvendinamas papildomas priemones ir, gavę prašymą, pateikti dokumentus kompetentingai priežiūros institucijai[22].

2.1 1 etapas. Žinokite apie savo perdavimus

8. Norint sužinoti, ko jums (duomenų eksportuotojui) gali prireikti, kad galėtumėte tęsti arba pradėti asmens duomenų perdavimą[23], pirmiausia reikia užtikrinti, kad būtumėte visapusiškai informuoti apie savo perdavimus (žinotumėte apie juos). Visų perdavimų registravimas ir stebėjimas gali būti sudėtingas procesas subjektams, dalyvaujantiems keliuose, įvairiuose ir reguliariuose perdavimuose trečiosioms valstybėms ir naudojantiems keletą duomenų tvarkytojų bei pagalbinių duomenų tvarkytojų. Žinoti apie savo perdavimus yra esminis pirmas žingsnis siekiant įvykdyti savo įsipareigojimus pagal atskaitomybės principą.

9. Kad būtumėte visapusiškai informuoti apie perdavimus, galite remtis duomenų tvarkymo veiklos įrašais, kuriuos jūs galite būti įpareigoti tvarkyti kaip duomenų valdytojas arba duomenų

[17] Sprendimo byloje C-311/18 (*Schrems II*) 134 punktas.
[18] BDAR 5 straipsnio 2 dalis ir 28 straipsnio 3 dalies c punktas.
[19] Todėl, pavyzdžiui, jūs nelaikomi duomenų eksportuotoju, jei esate duomenų subjektas, kuris, užpildydamas internetinį klausimyną, pateikia savo asmens duomenis trečiojoje valstybėje įsisteigusiam duomenų valdytojui.
[20] Žr. EDAV gaires Nr. 3/2018 dėl BDAR teritorinės taikymo srities (3 straipsnis) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en.
[21] EDAV gairės Nr. 2/2020 dėl Reglamento (ES) 2016/679 46 straipsnio 2 dalies a punkto ir 46 straipsnio 3 dalies b punkto, kai asmens duomenys perduodami tarp EEE ir ne EEE valdžios institucijų ir įstaigų (žr. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en).
[22] BDAR 5 straipsnio 2 dalis ir 24 straipsnio 1 dalis.
[23] Atkreipkite dėmesį, kad trečiosios valstybės subjekto nuotolinė prieiga prie EEE esančių duomenų taip pat laikoma perdavimu.

tvarkytojas pagal BDAR 30 straipsnį[24]. Jums taip pat gali būti naudingi ankstesni veiksmai, kuriais siekta įvykdyti įsipareigojimus informuoti duomenų subjektus pagal BDAR 13 straipsnio 1 dalies f punktą ir 14 straipsnio 1 dalies f punktą apie jų asmens duomenų perdavimą trečiosioms valstybėms[25].

10. Stebėdami perdavimus, nepamirškite atsižvelgti ir į tolesnį duomenų perdavimą, pavyzdžiui, ar jūsų duomenų tvarkytojai už EEE ribų perduoda jūsų jiems patikėtus asmens duomenis pagalbiniam duomenų tvarkytojui kitoje trečiojoje valstybėje arba toje pačioje trečiojoje valstybėje[26].

11. Pagal BDAR įtvirtintą „duomenų kiekio mažinimo“ principą[27], turite patikrinti, ar jūsų perduodami duomenys yra adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie yra tvarkomi.

12. Šie veiksmai turi būti atlikti prieš perduodant duomenis ir pakartoti prieš atnaujinant perdavimą po duomenų perdavimo operacijų sustabdymo: turite žinoti, kur duomenų importuotojai gali rasti arba tvarkyti jūsų eksportuotus asmens duomenis (paskirties vietų žemėlapis).

13. Atminkite, kad nuotolinė prieiga iš trečiosios valstybės (pavyzdžiui, pagalbos atvejais) ir (arba) saugojimas debesijos duomenų saugykloje už EEE ribų, kurį siūlo paslaugų teikėjas, taip pat laikomi perdavimu[28]. Konkrečiai kalbant, jei naudojatės tarptautine debesijos infrastruktūra, turite įvertinti, ar jūsų duomenys bus perduoti trečiosioms valstybėms ir kur jie bus perduoti, išskyrus atvejus, kai debesijos paslaugų teikėjas yra įsisteigęs EEE ir savo sutartyje aiškiai nurodo, kad duomenys nebus tvarkomi trečiosiose valstybėse.

2.2 2 etapas. Nustatykite naudojamas perdavimo priemones

14. Antruoju etapu privalote nustatyti, kurias iš BDAR V skyriuje išvardytų ir numatytų duomenų perdavimo priemonių naudojate.

---

[24] Žr. BDAR 30 straipsnį, visų pirma 1 dalies e punktą ir 2 dalies c punktą. Be to, jūsų tvarkymo įrašuose turėtų būti jūsų tvarkymo veiklos aprašymas (įskaitant, be kita ko, duomenų subjektų kategorijas, asmens duomenų kategorijas ir tvarkymo tikslus bei konkrečią informaciją apie duomenų perdavimą. Kai kurie duomenų valdytojai ir duomenų tvarkytojai atleidžiami nuo prievolės saugoti duomenų tvarkymo įrašus (BDAR 30 straipsnio 5 dalis). Rekomendacijos dėl šios išimties pateiktos 29 straipsnio darbo grupės pozicijos dokumente dėl nuostatų, leidžiančių nukrypti nuo įpareigojimo tvarkyti duomenų tvarkymo veiklos įrašus pagal BDAR 30 straipsnio 5 dalį (patvirtintas EDAV 2018 m. gegužės 25 d.).

[25] Pagal BDAR skaidrumo taisykles turite informuoti duomenų subjektus apie asmens duomenų perdavimą į trečiąsias valstybes (BDAR 13 straipsnio 1 dalies f punktas ir 14 straipsnio 1 dalies f punktas). Visų pirma privalote informuoti juos, ar Europos Komisija yra priėmusi sprendimą dėl tinkamumo, o perdavimo pagal BDAR 46 ar 47 straipsnius arba 49 straipsnio 1 dalies antrą pastraipą atveju privalote taikyti tinkamas arba pritaikytas apsaugos priemones ir būdus, kad gautumėte jų kopiją arba galėtumėte su jais susipažinti. Duomenų subjektui teikiama informacija turi būti teisinga ir aktuali, ypač atsižvelgiant į Teismo praktiką, susijusią su duomenų perdavimu.

[26] Kai duomenų valdytojas pagal BDAR 28 straipsnio 2 dalį yra iš anksto suteikęs savo konkretų arba bendrą rašytinį leidimą.

[27] BDAR 5 straipsnio 1 dalies c punktas.

[28] Žr. 2020 m. liepos 23 d. paskelbtus EDAV dažnai užduodamus klausimus dėl Europos Sąjungos Teisingumo Teismo sprendimo *Data Protection Commissioner Facebook Ireland Ltd ir Maximillian Schrems*, C-311/18, DUK Nr. 11: „reikėtų turėti omenyje, kad duomenų perdavimu laikomas net prieigos prie duomenų iš trečiosios valstybės suteikimas, pavyzdžiui, administraciniais tikslais“.

Sprendimai dėl tinkamumo

15. Europos Komisija, priimdama **sprendimus dėl tinkamumo**, susijusius su kai kuriomis arba visomis trečiosiomis valstybėmis, į kurias perduodate asmens duomenis, gali pripažinti, kad jais užtikrinama tinkama asmens duomenų apsauga[29].

16. Jei yra toks sprendimas dėl tinkamumo, asmens duomenys iš EEE į tą trečiąją valstybę gali būti perduodami netaikant BDAR 46 straipsnyje nurodytos perdavimo priemonės.

17. Sprendimai dėl tinkamumo gali būti taikomi visai valstybei arba tik jos daliai. Sprendimai dėl tinkamumo gali būti taikomi visiems duomenų perdavimams į valstybę arba tik tam tikrų rūšių duomenų perdavimui (pvz., viename sektoriuje)[30].

18. Europos Komisija savo interneto svetainėje skelbia savo sprendimų dėl tinkamumo sąrašą[31].

19. Jei perduodate asmens duomenis į trečiąsias valstybes, regionus ar sektorius, kuriems taikomas Komisijos sprendimas dėl tinkamumo (tiek, kiek taikytina), **jums nereikia imtis jokių tolesnių šiose rekomendacijos aprašytų veiksmų**[32]. Tačiau vis tiek turite stebėti, ar su jūsų duomenų perdavimu susiję sprendimai dėl tinkamumo nėra atšaukti ar pripažįsti negaliojančiais[33].

20. Tačiau sprendimai dėl tinkamumo neužkerta kelio duomenų subjektams pateikti skundą. Jie taip pat neužkerta kelio priežiūros institucijoms kreiptis į nacionalinį teismą, jei joms kyla abejonių dėl sprendimo galiojimo, kad nacionalinis teismas galėtų pateikti Teisingumo Teismui prašymą priimti prejudicinį sprendimą ir išnagrinėti šį galiojimo klausimą[34].

---

[29] Europos Komisija, remdamasi BDAR 45 straipsniu, turi įgaliojimus nustatyti, ar ES nepriklausančioje valstybėje užtikrinamas tinkamas duomenų apsaugos lygis. Europos Komisija taip pat turi teisę nustatyti, kad tarptautinė organizacija užtikrina tinkamą apsaugos lygį.

[30] BDAR 45 straipsnio 1 dalis.

[31] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[32] Jei jūs ir duomenų importuotojas įgyvendino priemones, kad įvykdytumėte kitas BDAR nustatytas prievoles; priešingu atveju turite tas priemones įgyvendinti.

[33] Europos Komisija turi periodiškai peržiūrėti visus sprendimus dėl tinkamumo ir stebėti, ar trečiosios valstybės, kurios naudojasi sprendimais dėl tinkamumo, ir toliau užtikrina tinkamą apsaugos lygį (žr. BDAR 45 straipsnio 3 ir 4 dalis). Be to, ESTT gali pripažinti sprendimus dėl tinkamumo negaliojančiais (žr. Teismo sprendimus bylose C-362/14 (*Schrems I*) ir C-311/18 (*Schrems II*).

[34] Sprendimo byloje C-311/18 (*Schrems II*) 118–120 punktai. Priežiūros institucijos negali nepaisyti sprendimo dėl tinkamumo ir sustabdyti ar uždrausti asmens duomenų perdavimą tokioms šalims remdamosi tik nepakankamu apsaugos lygiu. Jos gali pasinaudoti savo įgaliojimais sustabdyti arba uždrausti asmens duomenų perdavimą į tą trečiąja valstybę tik dėl kitų priežasčių (pvz., nepakankamos saugumo priemonės – pažeidžiamas BDAR 32 straipsnis; nėra teisinio pagrindo duomenų tvarkymui pagrįsti – pažeidžiamas BDAR 6 straipsnis). Priežiūros institucijos gali visiškai nepriklausomai išnagrinėti, ar tų duomenų perdavimas atitinka BDAR nustatytus reikalavimus, ir prireikus kreiptis į nacionalinius teismus, kad jie, kilus abejonių dėl Komisijos sprendimo dėl tinkamumo galiojimo, pateiktų Europos Teisingumo Teismui prašymą priimti prejudicinį sprendimą, kad būtų patikrintas jo galiojimas.

Pavyzdys.

2013 m. birželio mėn. ES pilietis M. Schrems pateikė skundą Airijos duomenų apsaugos komisijai (*Data Protection Commission*, toliau – DPC) ir paprašė šios priežiūros institucijos uždrausti arba sustabdyti jo asmens duomenų perdavimą iš „Facebook Ireland“ Jungtinėms Amerikos Valstijoms, nes manė, kad Jungtinių Amerikos Valstijų teisė ir praktika neužtikrina tinkamos jų teritorijoje laikomų asmens duomenų apsaugos nuo valdžios institucijų vykdomos stebėjimo veiklos. DPC atmetė skundą, remdamasi, be kita ko, tuo kad Sprendime 2000/520 Europos Komisija nusprendė, jog pagal „saugaus uosto“ sistemą Jungtinės Valstijos užtikrina tinkamą perduodamų asmens duomenų apsaugos lygį (toliau – sprendimas dėl „saugaus uosto“). M. Schrems apskundė DPC ir Airijos *High Court* (Aukštasis teismas) sprendimą dėl Sprendimo 2000/520 galiojimo Europos Sąjungos Teisingumo Teismui (toliau – ESTT). Vėliau ESTT nusprendė pripažinti Komisijos sprendimą 2000/520 dėl saugaus uosto privatumo principų teikiamos apsaugos pakankamumo negaliojančiu[35].

BDAR 46 straipsnyje nurodytos perdavimo priemonės

21. BDAR 46 straipsnyje išvardytos įvairios perdavimo priemonės, numatant „*tinkamas apsaugos priemones*“, kurias duomenų eksportuotojai gali naudoti asmens duomenims į trečiąsias valstybes perduoti, jei nepriimti sprendimai dėl tinkamumo. Pagrindinės BDAR 46 straipsnyje nurodytų duomenų perdavimo priemonių rūšys yra šios:

- standartinės duomenų apsaugos sutarčių sąlygos (toliau – SSS);
- įmonėms privalomos taisyklės (toliau – ĮPT);
- elgesio kodeksai;
- sertifikavimo mechanizmai;
- *ad hoc* sutarčių sąlygos.

22. Kad ir kokią duomenų perdavimo priemonę pasirinktumėte pagal BDAR 46 straipsnį, turite užtikrinti, kad, bendrai imant, perduotiems asmens duomenims būtų taikomas iš esmės lygiavertis apsaugos lygis.

23. BDAR 46 straipsnyje nurodytos perdavimo priemonės daugiausia apima tinkamas sutartinio pobūdžio apsaugos priemones, kurios gali būti taikomos perduodant duomenis į visas trečiąsias valstybes. Atsižvelgiant į padėtį trečiojoje valstybėje, į kurią perduodate duomenis, vis tiek gali reikėti papildyti šias perdavimo priemones ir jų apsaugos priemones papildomomis priemonėmis (toliau – papildomos priemonės), kad būtų užtikrintas iš esmės lygiavertis apsaugos lygis[36].

Nukrypti leidžiančios nuostatos

24. Be sprendimų dėl tinkamumo ir BDAR 46 straipsnyje nurodytų perdavimo priemonių, BDAR numatyta trečia duomenų perdavimo galimybė, taikytina tam tikrais atvejais. Esant tam tikroms sąlygoms, galbūt vis tiek galėsite perduoti asmens duomenis pagal BDAR 49 straipsnyje nurodytą nukrypti leidžiančią nuostatą.

25. BDAR 49 straipsnis yra išimtinio pobūdžio. Jame išdėstytos nukrypti leidžiančios nuostatos aiškintinos taip, kad neprieštarautų pačiam nukrypti leidžiančių nuostatų pobūdžiui, kaip taisyklės,

[35] Byla C-362/14 (*Schrems I*).
[36] Sprendimo byloje C-311/18 (*Schrems II*) 130 ir 133 punktai. Taip pat žr. šių rekomendacijų 2.3 poskirsnį.

pagal kurią asmens duomenys negali būti perduodami į trečiąją valstybę, išimtis, nebent šalyje būtų numatytas tinkamas duomenų apsaugos lygis arba nustatytos tinkamos apsaugos priemonės. Nukrypti leidžiančios nuostatos praktiškai negali tapti „taisykle“, bet turi būti taikomos tik konkrečiais atvejais. EDAV paskelbė Gaires Nr. 2/2018 dėl nukrypti leidžiančių nuostatų pagal Reglamento 2016/679 49 straipsnį. [37]

26. Prieš pasinaudodami BDAR 49 straipsnio nukrypti leidžiančia nuostata, turite patikrinti, ar jūsų vykdomas perdavimas atitinka kiekvienai iš jų nustatytas griežtas sąlygas.

***

27. Jei jūsų vykdomas perdavimas negali būti teisiškai pagrįstas nei sprendimu dėl tinkamumo, nei pagal 49 straipsnį leidžiančia nukrypti nuostata, toliau turite atlikti 3 veiksmą.

2.3 3 etapas. Įvertinkite, ar jūsų taikoma BDAR 46 straipsnyje nurodyta duomenų perdavimo priemonė yra veiksminga, atsižvelgiant į visas perdavimo aplinkybes

28. Pasirinkta BDAR 46 straipsnyje nurodyta perdavimo priemonė turi būti veiksminga užtikrinant, kad praktiškai perdavimas nepakenktų BDAR užtikrinamos apsaugos lygiui.[38]

29. Konkrečiai kalbant, perduodamų asmens duomenų apsaugos lygis trečiojoje valstybėje turi būti iš esmės lygiavertis apsaugos lygiui, kuris EEE užtikrinamas BDAR, aiškinamu atsižvelgiant į ES pagrindinių teisių chartiją[39]. Taip nėra, jei duomenų importuotojas negali vykdyti savo pareigų pagal pasirinktą BDAR 46 straipsnyje nurodytą perdavimo priemonę dėl duomenų perdavimui taikomų trečiosios valstybės teisės aktų ir praktikos, be kita ko, persiunčiant duomenis iš duomenų eksportuotojo šalies į duomenų importuotojo šalį[40].

30. Bendradarbiaudami su duomenų importuotoju, pirmiausia turite įvertinti, ar galiojančioje trečiosios valstybės teisėje ir (arba) esamoje praktikoje[41] yra kokių nors elementų, kurie galėtų sumažinti jūsų naudojamos BDAR 46 straipsnyje nurodytos perdavimo priemonės tinkamų apsaugos priemonių veiksmingumą vykdant konkretų perdavimą. Tai reiškia, kad reikia nustatyti, ar jūsų duomenų perdavimas patenka į teisės aktų ir (arba) praktikos, kurie gali pakenkti BDAR 46 straipsnyje nurodytos jūsų perdavimo priemonės veiksmingumui, taikymo sritį. Reikalaujamas vertinimas visų pirma turi būti grindžiamas viešai prieinamais teisės aktais.

31. Šiame vertinime turi būti pateikta informacija, susijusi su jūsų duomenų importuotojo trečiosios valstybės institucijų prieiga prie duomenų, pavyzdžiui:

    - elementai, rodantys, kad jūsų duomenų importuotojo trečiosios valstybės institucijos, atsižvelgdamos į teisės aktus, praktiką ir nurodytus precedentus, sieks gauti prieigą prie duomenų su duomenų importuotojo žinia ar be jos;

---

[37] Daugiau informacijos šiuo klausimu pateikta čia: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.

[38] BDAR 44 straipsnis ir sprendimo byloje C-311/18 (*Schrems II*) 126, 137 ir 148 punktai.

[39] Sprendimo byloje C-311/18 (*Schrems II*) 105 punktas ir antra išvada.

[40] Žr. sprendimo byloje C-311/18 (*Schrems II*) 183 punktą kartu su 184 punktu.

[41] Žr. sprendimo byloje C-311/18 (*Schrems II*) 126 punktą, kuriame Teismas aiškiai nurodo „atitinkamoje trečiojoje šalyje galiojančią teisę ir esamą praktiką“ ir reikalauja „<...> praktiškai užtikrinti veiksmingą atitinkamoje trečiojoje šalyje perduodamų asmens duomenų apsaugą“ (pabraukta papildomai), ir 158 punktą.

- elementai, rodantys, kad jūsų duomenų importuotojo trečiosios valstybės institucijos galės gauti prieigą prie duomenų per duomenų importuotoją, telekomunikacijų paslaugų teikėjus arba ryšių kanalus, atsižvelgdamos į teisės aktus, teisinius įgaliojimus, turimus techninius, finansinius bei žmogiškuosius išteklius ir nurodytus precedentus.

Teisės aktų ir praktikos, susijusių su visomis perdavimo aplinkybėmis, nustatymas

32. Turėsite išnagrinėti kiekvieno duomenų perdavimo ypatumus ir nustatyti, ar valstybės, į kurią duomenys perduodami (arba į kurią vykdomas tolesnis perdavimas), nacionalinė teisės sistema ir (arba) praktika turi įtakos jūsų perdavimams. Taigi jūsų vertinimas apima tik teisės aktus ir praktiką, susijusius su konkrečių jūsų perduodamų duomenų apsauga, priešingai nei bendro pobūdžio plataus masto tinkamumo vertinimai, kuriuos Europos Komisija atlieka pagal BDAR 45 straipsnį.

33. Taikytinas teisinis kontekstas ir (arba) praktika priklauso nuo konkrečių jūsų perdavimo aplinkybių, visų pirma nuo:

    - duomenų perdavimo ir tvarkymo tikslų (pvz., rinkodara, žmogiškieji ištekliai, saugojimas, IT pagalba, klinikiniai tyrimai);
    - duomenų tvarkymo procese dalyvaujančių subjektų rūšies (viešieji / privatūs; duomenų valdytojas / duomenų tvarkytojas)
    - sektoriaus, kuriame perdavimas vykdomas (pvz., reklamos technologijos, telekomunikacijos, finansai ir t. t.);
    - perduodamų asmens duomenų kategorijos (pvz., su vaikais susiję asmens duomenys gali patekti į konkrečių trečiosios valstybės teisės aktų taikymo sritį)[42];
    - to, ar duomenys bus saugomi trečiojoje valstybėje, ar yra nuotolinė prieiga prie ES ir (arba) EEE saugomų duomenų;
    - perduodamų duomenų formato (t. y. ar tai paprastas tekstas, ar apsaugotas pseudonimais arba užšifruotas[43]);
    - galimybės, kad duomenys bus toliau perduodami iš trečiosios valstybės į kitą trečiąja valstybę[44].

34. Jūsų vertinime reikėtų atsižvelgti į visus duomenų perdavimo procese dalyvaujančius subjektus (pvz., duomenų valdytojus, duomenų tvarkytojus ir pagalbinius duomenų tvarkytojus, tvarkančius duomenis trečiojoje valstybėje), kurie buvo nustatyti stebint perdavimus. Kuo daugiau

[42] Asmens duomenų perdavimas yra duomenų tvarkymo operacija (BDAR 4 straipsnio 2 punktas). Jei norite perduoti neskelbtinus duomenis, kuriems taikomi BDAR 9 ir 10 straipsniai, galite juos perduoti tik tuo atveju, jei jiems taikoma viena iš BDAR 9 ir 10 straipsniuose ir ES valstybių narių teisėje nustatytų nukrypti leidžiančių nuostatų ir sąlygų. Pagal BDAR 32 straipsnį, duomenų importuotojui veikiant kaip duomenų valdytojui arba duomenų tvarkytojui, taip pat turėsite įgyvendinti tinkamas technines ir organizacines priemones, kad būtų užtikrintas saugumo lygis, atitinkantis pavojų, kurį duomenų subjektų teisėms ir laisvėms kelia galimas perduodamų duomenų saugumo pažeidimas (BDAR 4 straipsnio 12 punktas). Perduodamų duomenų kategorijos ir jų neskelbtinumas bus svarbūs vertinant riziką ir priemonių tinkamumą.

[43] Kai kurios trečiosios valstybės neleidžia importuoti užšifruotų duomenų.

[44] Kai duomenų valdytojas pagal BDAR 28 straipsnio 2 dalį yra iš anksto suteikęs savo konkretų arba bendrą rašytinį leidimą.

dalyvaujančių duomenų valdytojų, tvarkytojų ar importuotojų, tuo sudėtingesnis bus jūsų vertinimas. Atlikdami šį vertinimą taip pat turėsite atsižvelgti į bet kokį numatomą tolesnį perdavimą.

35. Bet kuriuo atveju ypatingą dėmesį turėtumėte skirti atitinkamiems įstatymams, visų pirma įstatymams, kuriais nustatomi asmens duomenų atskleidimo valdžios institucijoms reikalavimai arba kuriais tokioms valdžios institucijoms suteikiama prieiga prie asmens duomenų (pavyzdžiui, baudžiamosios teisės vykdymo, reguliavimo priežiūros ar nacionalinio saugumo tikslais). Jei šiais reikalavimais ar įgaliojimais ribojamos pagrindinės duomenų subjektų teisės, kartu gerbiant jų esmę ir demokratinėje visuomenėje taikant būtinas ir proporcingas priemones svarbiems tikslams, kurie taip pat pripažįstami Sąjungos ar ES valstybių narių teisėje, apsaugoti[45], jie gali nepažeisti įsipareigojimų pagal jūsų pasirinktą BDAR 46 straipsnyje nurodytą perdavimo priemonę.

36. Turėsite įvertinti atitinkamas bendro pobūdžio taisykles ir praktiką tiek, kiek jos daro poveikį veiksmingam BDAR 46 straipsnyje nurodytos perdavimo priemonės apsaugos priemonių taikymui.

37. Atliekant šį vertinimą svarbūs ir įvairūs tos trečiosios valstybės teisinės sistemos aspektai, pvz., BDAR 45 straipsnio 2 dalyje išvardyti elementai. Pavyzdžiui, teisinės valstybės principų įgyvendinimas trečiojoje valstybėje gali būti svarbus elementas vertinant esamų mechanizmų, kuriais asmenys gali pasinaudoti gindami savo teises (teismo keliu) nuo neteisėtos vyriausybės prieigos prie asmens duomenų, veiksmingumą. Išsamus duomenų apsaugos įstatymas arba nepriklausoma duomenų apsaugos institucija, taip pat tarptautinių dokumentų, kuriuose numatytos duomenų apsaugos priemonės, laikymasis gali padėti užtikrinti vyriausybės taikomo suvaržymo proporcingumą.

38. Bus laikoma, kad tokiais teisės aktais ir praktika nustatytos prievolės ar įgaliojimai daro poveikį BDAR 46 straipsnyje nurodytos perdavimo priemonės įsipareigojimams arba yra su jais nesuderinami, jeigu[46]:

    - jais nepaisoma ES pagrindinių teisių chartijos pagrindinių teisių ir laisvių esmės arba
    - viršijama tai, kas būtina ir proporcinga demokratinėje visuomenėje siekiant apsaugoti vieną iš svarbių tikslų, pripažįstamų ir Sąjungos ar valstybių narių teisėje, pavyzdžiui, BDAR 23 straipsnio 1 dalyje.

39. Turėtumėte patikrinti, ar duomenų importuotojo įsipareigojimai, kuriais duomenų subjektams sudaromos sąlygos naudotis savo teisėmis, numatytomis BDAR 46 straipsnyje nurodytoje perdavimo priemonėje (pvz., prieigos prie perduotų duomenų, taisymo ir ištrynimo prašymai, taip pat (teisminės) teisių gynimo priemonės), gali būti veiksmingai taikomi praktikoje ir ar jiems neprieštarauja paskirties trečiosios valstybės įstatymai ir (arba) praktika.

---

[45] Žr. ES pagrindinių teisių chartijos 47 ir 52 straipsnius, BDAR 23 straipsnio 1 dalį ir 2020 m. lapkričio 10 d. EDAV rekomendacijas Nr. 02/2020 dėl Europos pagrindinių garantijų taikant sekimo priemones, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[46] Žr. ES pagrindinių teisių chartijos 47 ir 52 straipsnius, BDAR 23 straipsnio 1 dalį, sprendimo byloje C-311/18 (*Schrems II*) 174 ir 187 punktus ir 2020 m. lapkričio 10 d. EDAV rekomendacijas Nr. 02/2020 dėl Europos pagrindinių garantijų taikant sekimo priemones.

40. ES standartai, pvz., ES pagrindinių teisių chartijos 47 ir 52 straipsniai, turi būti naudojami kaip atskaitos taškas, ypač vertinant, ar valdžios institucijų prieiga apsiriboja tuo, kas būtina ir proporcinga demokratinėje visuomenėje, ir ar duomenų subjektams užtikrinamos veiksmingos teisių gynimo priemonės.

41. EDAV rekomendacijose dėl Europos pagrindinių garantijų (EPG)[47] pateikiami paaiškinimai dėl elementų, kuriuos reikia įvertinti siekiant nustatyti, ar teisinė sistema, reglamentuojanti trečiosios valstybės valdžios institucijų, kurios yra nacionalinės saugumo agentūros arba teisėsaugos institucijos, prieigą prie asmens duomenų, gali būti laikoma pagrįstu suvaržymu[48] ar ne. Visų pirma tai turėtų būti atidžiai įvertinta, kai teisės aktai, reglamentuojantys valdžios institucijų prieigą prie duomenų, yra dviprasmiški arba viešai neprieinami. Pirmasis Europos pagrindinių garantijų reikalavimas yra tas, kad turėtų būti nustatyta viešai prieinama ir pakankamai aiški teisinė sistema, numatanti tokią prieigą.

42. EDAV rekomendacijos dėl pagrindinių garantijų, taikomos duomenų perdavimui pagal 46 straipsnį, gali padėti duomenų eksportuotojui įvertinti, ar tokie įgaliojimai nepagrįstai pažeidžia duomenų eksportuotojo ir importuotojo pareigą užtikrinti esminį lygiavertiškumą pagal BDAR arba perdavimo priemonėje nustatytus įsipareigojimus. Iš esmės lygiavertės apsaugos trūkumas ypač akivaizdus tais atvejais, kai su jūsų perdavimu susiję trečiosios valstybės teisės aktai ir (arba) praktika neatitinka Europos pagrindinių garantijų reikalavimų. Valdyba pakartoja, kad Europos pagrindinės garantijos yra orientacinis standartas vertinant trečiųjų valstybių stebėjimo priemonių nulemtą suvaržymą tarptautinio duomenų perdavimo atvejais. Šie standartai nustatyti pagal ES teisę ir ESTT bei EŽTT praktiką, kuri yra privaloma ES valstybėms narėms.

43. Jūsų vertinimas visų pirma turi būti grindžiamas viešai skelbiamais teisės aktais. Išnagrinėję trečiosios valstybės valdžios institucijų praktiką taip pat galėsite patikrinti, ar BDAR 46 straipsnyje nurodytos perdavimo priemonės apsaugos priemonės gali būti pakankamos siekiant praktiškai užtikrinti veiksmingą perduodamų asmens duomenų apsaugą[49]. Toliau aprašytomis situacijomis jums bus ypač svarbu išnagrinėti trečiojoje valstybėje galiojančią praktiką.

43.1 **Atitinkami trečiosios valstybės teisės aktai gali oficialiai atitikti ES pagrindinių teisių ir laisvių standartus ir jų apribojimų būtinumą ir proporcingumą.** Tačiau valdžios institucijų praktika (pvz., prieiga prie privačiojo sektoriaus turimų asmens duomenų arba teisės aktų vykdymo užtikrinimas, kaip priežiūros ar teisminės institucijos) gali aiškiai rodyti, kad jos paprastai netaiko teisės aktų, kuriais iš esmės reglamentuojama jų veikla, ir jų nesilaiko. Tokiu atveju savo vertinime turite atsižvelgti į šią praktiką ir į tai, kad BDAR 46 straipsnyje nurodyta priemonė pati savaime (t. y. be papildomų priemonių) negalės veiksmingai užtikrinti iš esmės lygiaverčio lygio apsaugos. Tokiu atveju, jei norite tęsti duomenų perdavimą, turėsite įgyvendinti tinkamas papildomas priemones.

43.2 **Trečiojoje valstybėje gali trūkti atitinkamų teisės aktų (pvz., dėl prieigos prie privačiojo sektoriaus turimų asmens duomenų)**. Tokiu atveju, nesant atitinkamų teisės aktų, negalite automatiškai daryti išvados, kad jūsų BDAR 46 straipsnyje nurodyta perdavimo priemonė gali būti veiksmingai taikoma. Turėsite patikrinti, ar esama šalyje galiojančios praktikos, kuri

[47] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020.

[48] Todėl nedaro poveikio įsipareigojimams, prisiimtiems pagal BDAR 46 straipsnyje nurodytą perdavimo priemonę.

[49] Sprendimo byloje C-311/18 (*Schrems II*) 126 punktas.

nesuderinama su ES teise ir BDAR 46 straipsnyje nurodytos duomenų perdavimo priemonės įsipareigojimais, požymių. Jeigu esama nesuderinamų veiksmų, BDAR 46 straipsnyje nurodyta perdavimo priemonė pati savaime (t. y. be tinkamų papildomų priemonių) negalės veiksmingai užtikrinti iš esmės lygiaverčio lygio apsaugos. Tokiu atveju, jei norite tęsti duomenų perdavimą, turėsite įgyvendinti tinkamas papildomas priemones.

43.3 **Atlikus vertinimą gali būti nustatyta, kad atitinkami teisės aktai trečiojoje valstybėje gali būti probleminiai[50] ir kad perduoti duomenys ir (arba) duomenų importuotojas patenka arba gali patekti į šių probleminių teisės aktų taikymo sritį[51].**

Atsižvelgdami į neaiškumus, susijusius su galimu probleminių teisės aktų taikymu jūsų duomenų perdavimui, galite nuspręsti:

- sustabdyti duomenų perdavimą,
- įgyvendinti papildomas priemones[52], kad būtų išvengta rizikos, jog jūsų duomenų importuotojui ir (arba) jūsų perduotiems duomenims gali būti taikoma duomenų importuotojo trečiosios valstybės teisė ir (arba) praktika, kuri gali pakenkti perdavimo priemonės sutartinėms garantijoms dėl apsaugos lygio, kuris iš esmės yra lygiavertis EEE garantuojamam apsaugos lygiui, arba
- galite nuspręsti tęsti duomenų perdavimą neįgyvendindami papildomų priemonių, jei manote, kad neturite pagrindo manyti, jog jūsų perduotiems duomenims ir (arba) duomenų importuotojui bus taikomi atitinkami ir probleminiai teisės aktai. Atlikdami vertinimą, prireikus bendradarbiaudami su duomenų importuotoju, turėsite įrodyti ir dokumentais pagrįsti, kad teisės aktai nėra aiškinami ir (arba) taikomi praktiškai taip, kad būtų taikomi jūsų perduotiems duomenims ir duomenų importuotojui, taip pat atsižvelgiant į kitų subjektų, veikiančių tame pačiame sektoriuje ir (arba) susijusių su panašiais perduotais asmens duomenimis, patirtį ir toliau aprašytus papildomus informacijos šaltinius[53].

  Todėl turėsite įrodyti ir pagrįsti išsamia ataskaita[54] pagrįsti, kad probleminiai teisės aktai nebus praktiškai taikomi jūsų perduotiems duomenims ir (arba) duomenų importuotojui,

---

[50] „Probleminiai teisės aktai“ suprantami kaip teisės aktai, kuriais 1) asmens duomenų iš Europos Sąjungos gavėjui nustatomos pareigos ir (arba) daromas poveikis perduodamiems duomenims taip, kad gali būti pažeista sutartinė perdavimo priemonių garantija dėl iš esmės lygiaverčio apsaugos lygio ir 2) nepaisoma ES pagrindinių teisių chartijoje pripažintų pagrindinių teisių ir laisvių esmės arba viršijama tai, kas būtina ir proporcinga demokratinėje visuomenėje, siekiant apsaugoti vieną iš svarbių tikslų, pripažįstamų ir Sąjungos ar ES valstybių narių teisėje, pavyzdžiui, BDAR 23 straipsnio 1 dalyje.

[51] Gali būti neaišku, ar duomenų importuotojas ir (arba) perduodami duomenys patenka į bendrųjų terminų, dažnai vartojamų nacionalinės saugumo teisės aktuose, siekiant apriboti jų taikymo sritį, pvz., „elektroninių ryšių paslaugų teikėjas“ ir „užsienio žvalgybos informacija“, taikymo sritį.

[52] Žr. BDAR 109 konstatuojamąją dalį ir sprendimo byloje C-311/18 (*Schrems II*) 132 punktą.

[53] Žr. 45–47 punktus.

[54] Ataskaitose, kurias parengsite, turės būti pateikta išsami informacija apie teisinį teisės aktų ir praktikos vertinimą ir jų taikymą konkretiems perdavimams, vertinimo rengimo vidaus procedūrą (įskaitant informaciją apie vertinimo dalyvius, pvz., advokatų kontoras, konsultantus ar vidaus departamentus) ir patikrinimų datas. Ataskaitas turėtų patvirtinti duomenų eksportuotojo teisinis atstovas.

todėl jie netrukdys duomenų importuotojui vykdyti savo įsipareigojimų pagal BDAR 46 straipsnyje nurodytą perdavimo priemonę[55].

Galimi informacijos šaltiniai

44. Jūsų duomenų importuotojas turėtų pateikti atitinkamus šaltinius ir informaciją, susijusią su trečiąja valstybe, kurioje jis yra įsisteigęs, ir duomenų perdavimui taikytinus teisės aktus ir praktiką.

45. Jūs ir jūsų importuotojas savo vertinimą galite papildyti informacija, gauta iš šaltinių, pavyzdžiui, tų, kurie išvardyti kaip pavyzdžiai 3 priede.

46. Be perdavimui taikomos trečiosios valstybės teisinės sistemos, šaltiniai ir informacija turėtų būti svarbūs, objektyvūs, patikimi, patikrinami ir viešai arba kitaip prieinami, kad būtų galima nustatyti, ar jūsų 46 straipsnyje nurodyta perdavimo priemonė gali būti veiksmingai taikoma[56], ir turėsite įvertinti ir dokumentais pagrįsti, kad taip yra.

Svarbi: informacija turi būti susijusi su konkrečiu perdavimu ir (arba) duomenų importuotoju ir atitikti ES teisėje ir BDAR 46 straipsnyje nustatytus duomenų perdavimo priemonės reikalavimus, o ne pernelyg bendro pobūdžio ar abstrakti.

Objektyvi informacija: ar informacija pagrįsta empiriniais įrodymais, pagrįstais praeityje įgytomis žiniomis, o ne prielaidomis apie galimus įvykius ir riziką.

Patikima: duomenų eksportuotojas ir importuotojas privalo objektyviai įvertinti informacijos šaltinio ir pačios informacijos patikimumą ir atskirai tai įvertinti.

Patikrinama: informaciją ir išvadas turėtų būti galima patikrinti arba palyginti su kitų rūšių informacija ar šaltiniais, atliekant bendrą vertinimą, be kita ko, kad kompetentinga priežiūros arba teisminė institucija prireikus galėtų patikrinti šios informacijos objektyvumą ir patikimumą.

Viešai ar kitaip prieinama informacija: pageidautina, kad informacija būtų vieša arba bent jau prieinama, kad būtų lengviau patikrinti pirmiau nurodytus kriterijus ir būtų užtikrintas galimas dalijimasis ja su priežiūros institucijomis, teisminėmis institucijomis ir galiausiai duomenų subjektais.

[55] Įrodymas, kad jūsų perduotiems duomenims ir duomenų importuotojui praktiškai netaikomi probleminiai teisės aktai, taip pat atsižvelgiant į kitų subjektų, veikiančių tame pačiame sektoriuje ir (arba) susijusių su panašiais perduotais asmens duomenimis, patirtį, neatleidžia jūsų nuo pareigos numatyti būtinas papildomas priemones, siekiant apsaugoti asmens duomenis juos perduodant ir tvarkant paskirties trečiojoje valstybėje (pvz., ištisinis duomenų šifravimas – žr. 2 priede pateiktų papildomų techninių priemonių pavyzdžius), jei iš jūsų atliktos paskirties trečiosios valstybės taikytinų teisės aktų analizės matyti, kad prieiga prie duomenų taip pat gali būti suteikta šiuo perdavimo momentu, net jei duomenų importuotojas nedalyvauja. Gali būti, kad tokias priemones jau numatėte duomenų importuotojui veikiant kaip duomenų valdytojui arba duomenų tvarkytojui pagal BDAR 32 straipsnį.

[56] Žr. 3 priedą, kuriame pateikiamas nebaigtinis informacijos šaltinių, kuriais galite naudotis jūs ir importuotojas, sąrašas.

47. Taip pat galite atsižvelgti į dokumentais įformintą praktinę duomenų importuotojo patirtį, susijusią su atitinkamais ankstesniais atvejais, kai trečiosios valstybės valdžios institucijos pateikė prašymus suteikti prieigą. Naudotis duomenų importuotojo patirtimi kaip papildomu informacijos šaltiniu galėsite tik tuo atveju, jei pagal trečiosios valstybės teisinę sistemą duomenų importuotojui nedraudžiama pateikti informacijos apie valdžios institucijų prašymus atskleisti informaciją arba apie tai, kad tokių prašymų nėra (taip pat turėtumėte tokį vertinimą pagrįsti dokumentais). Tačiau turite atkreipti dėmesį į tai, kad tai, jog duomenų importuotojas anksčiau negavo prašymų, niekada negali būti laikoma lemiamu veiksniu, lemiančiu BDAR 46 straipsnyje nurodytos perdavimo priemonės, kuri leidžia perduoti duomenis netaikant papildomų priemonių, veiksmingumą. Šią informaciją kartu su kitų rūšių informacija, gauta iš kitų šaltinių, galėsite apsvarstyti bendrai vertindami trečiosios valstybės teisės aktus ir praktiką, susijusius su jūsų perdavimu. Atitinkama ir dokumentais patvirtinta duomenų importuotojo patirtis turėtų būti patvirtinta svarbia, objektyvia, patikima, patikrinama ir viešai arba kitaip prieinama informacija apie praktinį atitinkamos teisės taikymą (pvz., kitų tame pačiame sektoriuje veikiančių subjektų gautų prašymų suteikti prieigą ir (arba) susijusių su panašiais perduotais asmens duomenimis buvimu[57] ir (arba) teisės taikymu praktikoje, pavyzdžiui, teismų praktika ir nepriklausomų priežiūros įstaigų ataskaitomis) ir jai neturėtų prieštarauti.

Jūsų vertinimo rezultatai

48. Šį bendrą jūsų duomenų importuotojo trečiosios valstybės teisės ir praktikos, taikomos jūsų perdavimui, vertinimą turėtumėte atlikti kruopščiai ir išsamiai jį dokumentuoti. Jūsų kompetentingos priežiūros ir (arba) teisminės institucijos gali to paprašyti ir reikalauti, kad jūs būtumėte atskaitingi už visus tuo pagrindu priimtus sprendimus[58].

49. Jūsų vertinimas galiausiai gali atskleisti, kad jūsų taikoma BDAR 46 straipsnyje nurodyta perdavimo priemonė:

    - veiksmingai užtikrina, kad perduodamų asmens duomenų apsaugos lygis trečiojoje valstybėje būtų iš esmės lygiavertis EEE garantuojamam apsaugos lygiui. Dėl duomenų perdavimui taikomų trečiosios valstybės teisės aktų ir praktikos duomenų importuotojas gali vykdyti savo pareigas pagal pasirinktą perdavimo priemonę. Vertinimą turėtumėte pakartoti tinkamais intervalais arba paaiškėjus svarbiems pokyčiams (žr. 6 etapą), arba

    - neužtikrina iš esmės lygiaverčio apsaugos lygio veiksmingai. Duomenų importuotojas negali vykdyti savo įsipareigojimų dėl duomenų perdavimui taikomų trečiosios valstybės teisės aktų ir (arba) praktikos, taikomos perduodant duomenis nesilaikant ES pagrindinių teisių ir laisvių standartų, ir dėl jų apribojimų būtinumo ir proporcingumo, kad būtų apsaugoti teisėti viešojo intereso tikslai. ESTT pabrėžė, kad tais atvejais, kai BDAR 46 straipsnyje nurodytų perdavimo priemonių nepakanka, duomenų eksportuotojas privalo arba nustatyti veiksmingas papildomas priemones, arba neperduoti asmens duomenų[59].

[57] Kitų tiesiogiai žinomų subjektų patirtis gali būti susijusi su ankstesniais tokio paties pobūdžio perdavimais, kuriuos atlikote arba apie kuriuos pranešate atitinkamoje teismų praktikoje, NVO ataskaitose ir t. t. (žr. 3 priedą).
[58] BDAR 5 straipsnio 2 dalis.
[59] Sprendimo byloje C-311/18 (*Schrems II*) 134 ir 135 punktai.

Pavyzdys.

Bendroji informacija.
ESTT nusprendė, kad JAV užsienio žvalgybos stebėjimo įstatymo (*Foreign Intelligence Surveillance Act*, FISA) 702 straipsniu neužtikrinamos minimalios apsaugos priemonės, kylančios iš ES teisėje įtvirtinto proporcingumo principo, ir negali būti laikoma, kad minėta JAV nuostata apsiriboja tik tuo, kas tikrai būtina. Tai reiškia, kad duomenų apsaugos lygis įgyvendinant programas pagal FISA 702 straipsnį nėra iš esmės lygiavertis pagal Sąjungos teisę būtinoms apsaugos priemonėms.

Vertinimas.
Jei, įvertinę atitinkamus JAV teisės aktus, manote, kad jūsų perdavimas gali patekti į FISA 702 straipsnio taikymo sritį, tačiau nesate tikri, ar jis patenka į jo praktinę taikymo sritį, galite nuspręsti:

1. sustabdyti duomenų perdavimą,
2. priimti tinkamas papildomas priemones, kuriomis veiksmingai užtikrinamas perduodamų duomenų apsaugos lygis, iš esmės lygiavertis garantuojamam EEE, arba
3. susipažinti su kita objektyvia, patikima, svarbia, patikrinama ir, pageidautina, viešai prieinama informacija (kuri gali apimti informaciją, kurią jums pateikė jūsų duomenų importuotojas), kad būtų paaiškinta FISA 702 straipsnio praktinio taikymo jūsų konkrečiam perdavimui sritis. Ši informacija turėtų padėti atsakyti į kai kuriuos svarbius klausimus, pavyzdžiui:

- Ar iš viešai prieinamos informacijos matyti, kad yra teisinis draudimas informuoti apie konkretų prašymą leisti susipažinti su gautais duomenimis ir plataus masto apribojimai teikti bendrą informaciją apie prašymus suteikti prieigą prie gautų duomenų arba apie gautų prašymų nebuvimą?

- Ar jūsų duomenų importuotojas patvirtino, kad anksčiau gavo JAV valdžios institucijų prašymus dėl prieigos prie duomenų? O gal jūsų duomenų importuotojas patvirtino, kad anksčiau nėra gavęs JAV valdžios institucijų prašymų suteikti prieigą prie duomenų ir kad jam nedraudžiama teikti informacijos apie tokius prašymus arba jų nebuvimą?

- Ar viešai prieinama informacija, kurią gavote apie JAV teismų praktiką, ir iš priežiūros įstaigų, pilietinės visuomenės organizacijų ir akademinių institucijų gautos ataskaitos[60] atskleidžia to paties sektoriaus duomenų importuotojus, kurie anksčiau yra gavę prašymus dėl prieigos prie duomenų, susijusius su panašiais perduotais duomenimis?

Atsakymai į šiuos klausimus, kuriuos gaunate per bendrą vertinimą, leidžia daryti išvadą, kad:

- Konkrečiai jūsų duomenų perdavimui praktiškai taikomas FISA 702 straipsnis, todėl tai kenkia jūsų BDAR 46 straipsnyje nurodytos perdavimo priemonės veiksmingumui. Todėl, jei norite tęsti perdavimą, turite apsvarstyti, jei reikia, bendradarbiaudami su duomenų importuotoju, ar galite imtis papildomų priemonių, kuriomis veiksmingai užtikrinamas perduodamų duomenų apsaugos lygis, iš esmės lygiavertis EEE garantuojamam lygiui. Jei negalite rasti veiksmingų papildomų priemonių, asmens duomenų perduoti negalima.
Arba

[60] Pavyzdžiui, FISA 702 straipsnio nuostatos; Užsienio žvalgybos stebėjimo teismo (FISC) darbo tvarkos taisyklės, išslaptintos FISC nuomonės ir sprendimai, JAV teismų praktika; Privatumo ir pilietinių laisvių priežiūros valdybos (PCLOB) ataskaitos ir klausymo stenogramos; generalinio inspektoriaus tarnybos – JAV teisingumo departamento ataskaitos; NSA Piliečių laisvių ir privatumo biuro direktoriaus ataskaitos; Kongreso tyrimų tarnybos parengtos ataskaitos; Amerikos piliečių laisvių sąjungos fondo (ACLU) ataskaitos.

- FISA 702 straipsnis praktiškai netaikomas jūsų konkrečiam duomenų perdavimui, todėl nedaro poveikio jūsų BDAR 46 straipsnyje nurodytos duomenų perdavimo priemonės veiksmingumui. Tada galite tęsti duomenų perdavimą nesiimdami jokių papildomų priemonių.

2.4 4 etapas. Patvirtinkite papildomas priemones

50. Jei pagal 3 etapą atliktas jūsų vertinimas parodė, kad jūsų duomenų perdavimo pagal BDAR 46 straipsnį priemonė nėra veiksminga, prireikus bendradarbiaujant su duomenų importuotoju turėsite įvertinti, ar yra papildomų priemonių, kuriomis, kartu su perdavimo priemonių apsaugos priemonėmis, būtų galima užtikrinti, kad trečiojoje valstybėje perduodamiems duomenims būtų suteiktas apsaugos lygis, iš esmės lygiavertis apsaugos garantuojamam ES[61]. „Papildomos priemonės“ iš esmės papildo apsaugos priemones, kurios jau numatytos pagal BDAR 46 straipsnyje nurodytą perdavimo priemonę, ir bet kokius kitus BDAR nustatytus taikytinus saugumo reikalavimus (pvz., techninio saugumo priemones)[62].

51. Kiekvienu konkrečiu atveju turite nustatyti, kokios papildomos priemonės galėtų būti veiksmingos vykdant duomenų perdavimą į konkrečią trečiąja valstybę, kai naudojamasi konkrečia BDAR 46 straipsnyje nurodyta duomenų perdavimo priemone. Vertinimo nereikia kartoti kaskart, kai tam tikros rūšies duomenys perduodami tai pačiai trečiajai valstybei. Kai kuriems duomenims, kuriuos planuojama perduoti, gali prireikti papildomų priemonių, o kitiems duomenims (atsižvelgiant į oficialų ir (arba) praktinį trečiosios valstybės teisės aktų taikymą) gali prireikti kitų priemonių. Galėsite remtis savo ankstesniais vertinimais ir išvadomis per 1, 2 ir 3 etapus ir pagal jų rezultatus patikrinti, ar papildomos priemonės gali būti veiksmingos užtikrinant reikiamą apsaugos lygį.

52. Iš esmės papildomos priemonės gali būti sutartinio, techninio arba organizacinio pobūdžio. Įvairių priemonių derinimas taip, kad jos palaikytų viena kitą ir remtųsi viena kita, gal pakelti apsaugos lygį, taigi ir padėti siekti ES standartų.

53. Vien tik sutartinės ir organizacinės priemonės paprastai nepanaikina trečiosios valstybės valdžios institucijų prieigos prie asmens duomenų, remiantis probleminiais teisės aktais ir (arba) praktika[63]. Iš tiesų būna atvejų, kai tik tinkamai įgyvendintomis techninėmis priemonėmis gali būti sutrukdyta trečiųjų valstybių valdžios institucijoms gauti prieigą prie asmens duomenų, visų pirma stebėjimo tikslais, arba dėl tų priemonių prieiga gali tapti neveiksminga[64]. Tokiais atvejais sutartinės arba organizacinės priemonės gali papildyti technines priemones ir sustiprinti bendrą duomenų

[61] Sprendimo byloje C-311/18 (*Schrems II*) 96 punktas.
[62] BDAR 109 konstatuojamoji dalis ir sprendimo byloje C-311/18 (*Schrems II*) 133 punktas.
[63] „Probleminiai teisės aktai“ suprantami kaip teisės aktai, kuriais 1) asmens duomenų iš Europos Sąjungos gavėjui nustatomos pareigos ir (arba) daromas poveikis perduodamiems duomenims taip, kad gali būti pažeista sutartinė perdavimo priemonių garantija dėl iš esmės lygiaverčio apsaugos lygio ir 2) nepaisoma ES pagrindinių teisių chartijoje pripažintų pagrindinių teisių ir laisvių esmės arba viršijama tai, kas būtina ir proporcinga demokratinėje visuomenėje, siekiant apsaugoti vieną iš svarbių tikslų, pripažįstamų ir Sąjungos ar ES valstybių narių teisėje, pavyzdžiui, BDAR 23 straipsnio 1 dalyje.
[64] Jei tokia prieiga viršija tai, kas būtina ir proporcinga demokratinėje visuomenėje; žr. ES pagrindinių teisių chartijos 47 ir 52 straipsnius, BDAR 23 straipsnio 1 dalį ir 2020 m. lapkričio 10 d. EDAV rekomendacijas Nr. 02/2020 dėl Europos pagrindinių garantijų taikant sekimo priemones https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

apsaugos lygį, (pvz., įvedant patikras ir panaikinant automatizmą, kai valdžios institucijos bando susipažinti su duomenimis ES standartų neatitinkančiu būdu).

54. Galite susipažinti su toliau pateiktu (neišsamiu) veiksnių sąrašu, prireikus bendradarbiaudami su duomenų importuotoju, ir įvertinti, kurios papildomos priemonės būtų veiksmingiausios siekiant apsaugoti perduodamus duomenis nuo valdžios institucijų prašymų suteikti prieigą prie duomenų remiantis praktiškai taikomais probleminiais teisės aktais:

    - perduodamų duomenų formatas (t. y. ar tai paprastas tekstas, ar apsaugotas pseudonimais arba ar užšifruotas);
    - duomenų pobūdis (pvz., EEE užtikrinamas aukštesnis duomenų kategorijų, kurioms taikomi BDAR 9 ir 10 straipsniai, apsaugos lygis)[65];
    - duomenų tvarkymo darbo trukmė ir sudėtingumas, duomenų tvarkyme dalyvaujančių subjektų skaičius ir jų tarpusavio santykiai (pvz., ar perduodant duomenis dalyvauja keli duomenų valdytojai arba ir duomenų valdytojai, ir duomenų tvarkytojai, ar dalyvauja duomenų tvarkytojai, kurie duomenis iš jūsų perduos jūsų duomenų importuotojui (atsižvelgiant į atitinkamas nuostatas, taikomas jiems pagal paskirties trečiosios valstybės teisės aktus))[66];
    - trečiosios valstybės teisės praktinio taikymo metodas arba parametrai, nustatyti 3 etapu;
    - galimybė, kad duomenys gali būti toliau perduodami toje pačioje trečiojoje valstybėje ar net į kitas trečiąsias valstybes (pvz., duomenų importuotojo pagalbinių duomenų tvarkytojų dalyvavimas[67]).

<u>Papildomų priemonių pavyzdžiai</u>

55. Kai kurie techninių, sutartinių ir organizacinių priemonių, į kurias būtų galima atsižvelgti, pavyzdžiai, jei jie dar neįtraukti į taikytą BDAR 46 straipsnyje nurodytą perdavimo priemonę, pateikiami 2 priede aprašytuose nebaigtiniuose sąrašuose.

***

56. Jei įdiegėte veiksmingas papildomas priemones, kurios kartu su jūsų pasirinkta BDAR 46 straipsnyje nurodyta duomenų perdavimo priemone pasiekia tokį apsaugos lygį, kuris dabar iš esmės yra lygiavertis EEE garantuojamam apsaugos lygiui, galite tęsti savo perdavimus.

57. Jei negalite nustatyti arba įgyvendinti veiksmingų papildomų priemonių, kuriomis būtų užtikrinta, kad perduotiems asmens duomenims būtų taikomas iš esmės lygiavertis apsaugos lygis[68], negalite pradėti perduoti asmens duomenų į atitinkamą trečiąją valstybę pagal jūsų naudojamą BDAR 46 straipsnyje nurodytą perdavimo priemonę. Jei duomenis jau perduodate, turite sustabdyti arba

---

[65] Žr. 42 išnašą.

[66] BDAR duomenų valdytojams ir duomenų tvarkytojams nustato atskiras prievoles. Perdavimas gali būti atliekamas tarp duomenų valdytojo ir duomenų valdytojo, tarp bendradarbiaujančių duomenų valdytojų, duomenų valdytojo ir duomenų tvarkytojo ir, gavus duomenų valdytojo leidimą, tarp duomenų tvarkytojo ir duomenų valdytojo arba tarp duomenų tvarkytojo ir kito duomenų tvarkytojo.

[67] Žr. 26 išnašą.

[68] Jei tokia prieiga viršija tai, kas būtina ir proporcinga demokratinėje visuomenėje; žr. ES pagrindinių teisių chartijos 47 ir 52 straipsnius, BDAR 23 straipsnio 1 dalį ir 2020 m. lapkričio 10 d. EDAV rekomendacijas Nr. 02/2020 dėl Europos pagrindinių garantijų taikant sekimo priemones https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

nutraukti asmens duomenų perdavimą[69] . Vadovaudamasis BDAR 46 straipsnyje nurodytų perdavimo priemonių apsaugos priemonėmis, duomenų importuotojas turėtų grąžinti jums duomenis, kuriuos jau perdavėte tai trečiajai valstybei, ir jų kopijas arba juos visus sunaikinti[70].

Pavyzdys.

Trečiosios valstybės įstatymais draudžiamos jūsų nurodytos papildomas priemones (pvz., draudžiama naudoti šifravimą) arba kitaip užkertamas kelias jų taikymui. Negalite pradėti perduoti asmens duomenų į šią valstybę arba turite nutraukti vykdomus perdavimus į šią valstybę.

58. Kompetentinga priežiūros institucija gali taikyti bet kokią kitą taisomąją priemonę (pvz., baudą), jei pradedate arba tęsiate perdavimą, nepaisant to, kad negalite įrodyti iš esmės lygiaverčio apsaugos lygio trečiojoje valstybėje.

2.5 5 etapas. Procedūros etapai, jei nustatėte veiksmingas papildomas priemones

59. Procedūriniai veiksmai, kurių gali prireikti nustačius veiksmingas papildomas priemones, gali skirtis priklausomai nuo 46 straipsnyje nurodytos BDAR perdavimo priemonės, kurią naudojate arba ketinate naudoti.

2.5.1 Standartinės duomenų apsaugos sąlygos (BDAR 46 straipsnio 2 dalies c ir d punktai)

60. Jei be SSS ketinate nustatyti papildomas priemones, jums nereikia prašyti kompetentingos priežiūros institucijos leidimo pridėti tokias sąlygas ar papildomas apsaugos priemones, jei nustatytos papildomos priemonės nei tiesiogiai, nei netiesiogiai neprieštarauja SSS ir yra pakankamos norint užtikrinti, kad nebūtų pakenkta BDAR garantuojamam apsaugos lygiui[71]. Duomenų eksportuotojas ir importuotojas turi užtikrinti, kad papildomos sąlygos negalėtų būti aiškinamos siekiant apriboti SSS nustatytas teises ir pareigas arba kokiu nors kitu būdu sumažinti duomenų apsaugos lygį. Turite sugebėti įrodyti visa tai, įskaitant visų sąlygų nedviprasmiškumą, vadovaudamiesi atskaitomybės principu ir savo pareiga užtikrinti pakankamą duomenų apsaugos lygį. Kompetentingos priežiūros institucijos turi įgaliojimus prireikus peržiūrėti šias papildomas sąlygas (pvz., gavusios skundą arba atlikdamos tyrimą savo iniciatyva).

61. Jei ketinate keisti pačias standartines duomenų apsaugos sąlygas arba jei pridėtos papildomos priemonės tiesiogiai ar netiesiogiai „prieštarauja“ SSS, nebelaikoma, kad remiatės standartinėmis

[69] Sprendimo byloje C-311/18 (*Schrems II*) 135 punktas.
[70] Pavyzdžiui, žr. Sprendimo 87/2010 dėl SSS priedo 12 punktą; žr. (neprivalomą) papildomą nutraukimo sąlygą Sprendimo 2004/915/EB dėl SSS B priede.
[71] BDAR 109 konstatuojamojoje dalyje nurodyta: „galimybė duomenų valdytojui arba duomenų tvarkytojui remtis Komisijos ar priežiūros institucijos priimtomis standartinėmis duomenų apsaugos sąlygomis neturėtų užkirsti kelio duomenų valdytojams arba duomenų tvarkytojams standartines duomenų apsaugos sąlygas įtraukti į platesnes sutartis, tokias kaip duomenų tvarkytojo sutartis su kitais duomenų tvarkytojais, ar jas papildyti kitomis sąlygomis ar papildomomis apsaugos sąlygomis, jei jos tiesiogiai ar netiesiogiai neprieštarauja Komisijos ar priežiūros institucijos priimtoms standartinėms sutarčių sąlygoms ar nedaro poveikio duomenų subjektų pagrindinėms teisėms ir laisvėms”. Panašios nuostatos pateikiamos SSS rinkiniuose, kuriuos Europos Komisija priėmė pagal Direktyvą 95/45/EB.

sutarčių sąlygomis[72], ir turite kreiptis į kompetentingą priežiūros instituciją dėl leidimo pagal BDAR 46 straipsnio 3 dalies a punktą.

2.5.2 ĮPT (BDAR 46 straipsnio 2 dalies b punktas)

62. Sprendime *Schrems II* pateikti argumentai taip pat taikomi kitoms perdavimo priemonėms pagal BDAR 46 straipsnio 2 dalį, nes visos šios priemonės iš esmės yra sutartinio pobūdžio, todėl jose numatytos garantijos ir šalių prisiimti įsipareigojimai negali būti privalomi trečiųjų valstybių valdžios institucijoms[73].

63. Sprendimas *Schrems II* yra svarbus asmens duomenų perdavimui pagal ĮPT, nes trečiųjų valstybių įstatymai gali turėti įtakos tokiomis priemonėmis užtikrinamai apsaugai.

64. Visi įsipareigojimai, kuriuos reikia įtraukti, bus nurodyti atnaujintose WP256/257 nuorodose[74], į kurias visos grupės, kurios remiasi įmonėms privalomomis taisyklėmis kaip perkėlimo priemonėmis, turės suderinti savo esamas ir būsimas įmonėms privalomas taisykles.

65. Teisingumo Teismas pažymėjo, kad įvertinti, ar atitinkamoje trečiojoje valstybėje yra užtikrinamas pagal ES teisę reikalaujamas apsaugos lygis, turi duomenų eksportuotojas ir duomenų importuotojas, jeigu jie nori nustatyti, ar SSS arba ĮPT užtikrinamas garantijas galima įgyvendinti praktiškai. Jeigu ne, turėtumėte įvertinti, ar galite numatyti papildomas priemones, kad užtikrintumėte iš esmės lygiavertį apsaugos lygį, kaip tas, kuris užtikrinamas EEE, ir ar trečiosios valstybės teisės aktai nedarys poveikio šioms papildomoms priemonėms taip, kad jos taptų neveiksmingos.

2.5.3 *Ad hoc* sutarčių sąlygos (BDAR 46 straipsnio 3 dalies a punktas)

66. Sprendime *Schrems II* pateikti argumentai taip pat taikomi kitoms perdavimo priemonėms pagal BDAR 46 straipsnio 2 dalį, nes visos šios priemonės iš esmės yra sutartinio pobūdžio, todėl jose numatytos garantijos ir šalių prisiimti įsipareigojimai negali būti privalomi trečiųjų valstybių valdžios institucijoms[75]. Todėl sprendimas *Schrems II* yra svarbus asmens duomenų perdavimui pagal ad hoc sutarčių sąlygas, nes trečiųjų valstybių įstatymai gali turėti įtakos tokiomis priemonėmis užtikrinamai apsaugai.

---

[72] Pagal analogiją žr. EDAV nuomonę 17/2020 dėl Slovėnijos priežiūros institucijos pateikto standartinių sutarčių sąlygų projekto (BDAR 28 straipsnio 8 dalis) dėl jau priimtų SSS 28 straipsnio, kurioje yra panaši nuostata („Be to, Valdyba primena, kad galimybė taikyti priežiūros institucijos priimtas standartines sutarčių sąlygas netrukdo šalims įtraukti kitų sąlygų ar papildomų apsaugos priemonių, jei jos nei tiesiogiai, nei netiesiogiai neprieštarauja priimtoms standartinėms sutarčių sąlygoms ir nepažeidžia duomenų subjektų pagrindinių teisių ar laisvių. Be to, pakeitus standartines duomenų apsaugos nuostatas nebebus laikoma, kad šalys yra įgyvendinusios patvirtintas standartines sutarčių sąlygas“), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_en.pdf.

[73] ESTT sprendimo byloje C-311/18 (*Schrems II*) 132 punktas.

[74] 29 straipsnio darbo grupės darbinis dokumentas, kuriuo nustatoma įmonei privalomose taisyklėse turinčių būti elementų ir principų lentelė, paskutinį kartą peržiūrėtas ir patvirtintas 2018 m. vasario 6 d., WP256, 1-oji peržiūrėta redakcija; 29 straipsnio darbo grupės darbinis dokumentas, kuriuo nustatoma įmonėms privalomose taisyklėse turinčių būti elementų ir principų lentelė, paskutinį kartą peržiūrėtas ir patvirtintas 2018 m. vasario 6 d. dokumentu WP257, 1-oji peržiūrėta redakcija.

[75] ESTT sprendimo byloje C-311/18 (*Schrems II*) 132 punktas.

2.6 6 etapas. Reikiamais intervalais įvertinti iš naujo

67. Privalote nuolat ir, jei reikia, bendradarbiaudami su duomenų importuotojais, stebėti pokyčius trečiojoje valstybėje, į kurią perdavėte asmens duomenis, galinčius turėti įtakos jūsų pradiniam apsaugos lygio vertinimui ir sprendimams, kuriuos atitinkamai priėmėte dėl savo duomenų perdavimo. Atskaitomybė yra nuolatinis įsipareigojimas (BDAR 5 straipsnio 2 dalis).

68. Turėtumėte įdiegti pakankamai patikimus mechanizmus, kad užtikrintumėte greitą perdavimo sustabdymą arba nutraukimą, jei:

    - duomenų importuotojas pažeidė įsipareigojimus, prisiimtus pagal BDAR 46 straipsnyje nurodytą perdavimo priemonę, arba negali jų vykdyti, arba
    - toje trečiojoje valstybėje papildomos priemonės nebeveiksmingos.

3 IŠVADA

69. BDAR nustatytos asmens duomenų tvarkymo EEE taisyklės ir taip sudaromos sąlygos laisvam asmens duomenų judėjimui EEE. BDAR V skyriuje reglamentuojamas asmens duomenų perdavimas į trečiąsias valstybes ir nustatomas griežtas reikalavimas: perdavimas negali pakenkti BDAR garantuojamam fizinių asmenų apsaugos lygiui (BDAR 44 straipsnis). ESTT sprendime C-311/18 (*Schrems II*) pabrėžiama, kad reikia užtikrinti BDAR suteikiamos asmens duomenų, perduodamų į trečiąją valstybę, apsaugos lygio tęstinumą[76].

70. Norėdami užtikrinti iš esmės lygiavertį duomenų apsaugos lygį savo duomenims, pirmiausia turite išsamiai žinoti apie savo persiuntimus. Taip pat turite patikrinti, ar jūsų perduodami duomenys yra adekvatūs, tinkami ir tik tokie, kokių reikia siekiant tikslų, dėl kurių jie yra tvarkomi.

71. Taip pat turite nurodyti perdavimo priemonę, kurią taikote vykdydami perdavimą. Jei perdavimo priemonė nėra sprendimas dėl tinkamumo, kiekvienu konkrečiu atveju turite patikrinti, ar paskirties trečiosios valstybės įstatymai arba praktika nepažeidžia BDAR 46 straipsnyje nustatytų apsaugos priemonių, kai vykdomi jūsų perdavimai. Kai vien taikant BDAR 46 straipsnyje nurodytą perdavimo priemonę nepavyksta pasiekti iš esmės lygiaverčio asmens duomenų apsaugos lygio, spraga gali būti užpildyta papildomomis priemonėmis.

72. Jei negalite nustatyti arba įgyvendinti veiksmingų papildomų priemonių, užtikrinančių, kad perduotiems asmens duomenims būtų taikomas iš esmės lygiavertis apsaugos lygis, turite nepradėti asmens duomenų perdavimo į atitinkamą trečiąją valstybę pagal jūsų pasirinktą perdavimo priemonę. Jei duomenis jau perduodate, turite nedelsdami sustabdyti arba nutraukti asmens duomenų perdavimą.

73. Kompetentinga priežiūros institucija turi įgaliojimus sustabdyti arba nutraukti asmens duomenų perdavimą į trečiąją valstybę, jei neužtikrinama duomenų apsauga pagal ES teisę, visų pirma BDAR 45 ir 46 straipsnius ir Pagrindinių teisių chartiją.

Europos duomenų apsaugos valdybos vardu
Pirmininkė
(Andrea Jelinek)

---

[76] Sprendimo byloje C-311/18 (*Schrems II*) 93 punktas.

1 PRIEDAS. APIBRĖŽTYS

- Trečioji valstybė – valstybė, kuri nėra EEE valstybė narė.
- EEE – Europos ekonominė erdvė, apimanti Europos Sąjungos valstybes nares ir Islandiją, Norvegiją bei Lichtenšteiną. Lichtenšteinui BDAR taikomas pagal EEE susitarimą, konkrečiai pagal jo XI priedą ir 37 protokolą.
- BDAR – 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).
- Chartija – Europos Sąjungos pagrindinių teisių chartija, OL C 326, 2012 10 26, p. 391–407.
- ESTT arba Teismas – Europos Sąjungos Teisingumo Teismas. Tai Europos Sąjungos teisminė institucija, kuri, bendradarbiaudama su valstybių narių teismais, užtikrina vienodą ES teisės taikymą ir aiškinimą.
- Duomenų eksportuotojas – duomenų valdytojas arba duomenų tvarkytojas EEE, kuris asmens duomenis perduoda duomenų valdytojui arba duomenų tvarkytojui trečiojoje valstybėje.
- Duomenų importuotojas – duomenų valdytojas arba duomenų tvarkytojas trečiojoje valstybėje, kuris gauna iš EEE perduotus asmens duomenis arba prieigą prie jų.
- BDAR 46 straipsnyje nurodyta perdavimo priemonė – tai atitinkamos apsaugos priemonės pagal BDAR 46 straipsnį, kurias duomenų eksportuotojai taiko perduodami asmens duomenis trečiajai valstybei, jei nėra priimtas sprendimas dėl tinkamumo pagal BDAR 45 straipsnio 3 dalį. BDAR 46 straipsnio 2 ir 3 dalyse pateikiamas BDAR 46 straipsnyje nurodytų perdavimo priemonių, kuriomis gali naudotis duomenų valdytojai ir duomenų tvarkytojai, sąrašas.
- SSS – standartinės duomenų apsaugos sąlygos (arba „standartinės sutarčių sąlygos“), kurias Europos Komisija patvirtino asmens duomenų perdavimui tarp EEE duomenų valdytojų arba tvarkytojų ir už EEE ribų esančių duomenų valdytojų arba tvarkytojų. Europos Komisijos patvirtintos standartinės sutarčių sąlygos yra perdavimo priemonė pagal BDAR, kaip nurodyta BDAR 46 straipsnio 2 dalies c punkte ir 5 dalyje .

2 PRIEDAS. PAPILDOMŲ PRIEMONIŲ PAVYZDŽIAI

74. Toliau išvardyti papildomų priemonių pavyzdžiai, į kuriuos galite atsižvelgti pasiekę 4 etapą „Patvirtinkite papildomas priemones“. Šis sąrašas nėra išsamus. Galite ieškoti kitų papildomų priemonių. Dėl būsimų technologinių, teisinių ar organizacinių pokyčių gali atsirasti naujų papildomų priemonių, kurias turėsite apsvarstyti. Vienos ar keleto iš šių priemonių pasirinkimas nereiškia, kad bus tikrai ir sistemingai užtikrinta jūsų vykdomo perdavimo atitiktis esminio lygiavertiškumo standartui pagal ES teisę. Turėtumėte pasirinkti tas papildomas priemones, kurios gali veiksmingai garantuoti tokį apsaugos lygį jūsų vykdomiems perdavimams.

75. Bet kokia papildoma priemonė gali būti laikoma veiksminga ESTT sprendimo *Schrems II* prasme tik tuo atveju, jei ir tiek, kiek ja savaime arba kartu su kitomis priemonėmis pašalinami konkretūs trūkumai, kuriuos nustatėte vertindami teisinę padėtį trečiojoje valstybėje, kiek tai susiję su jūsų perdavimui taikomais teisės aktais ir praktika. Jei galiausiai negalite užtikrinti iš esmės lygiaverčio apsaugos lygio, negalite perduoti asmens duomenų.

76. Iš jūsų, kaip duomenų valdytojo arba tvarkytojo, jau gali būti reikalaujama įgyvendinti kai kurias šiame priede aprašytas priemones, kad būtų laikomasi BDAR. Tai reiškia, kad gali reikėti nustatyti panašias priemones EEE tvarkomiems asmens duomenims, perduodamiems duomenų importuotojui, kuriam taikomas sprendimas dėl tinkamumo, arba kitoms trečiosioms valstybėms[77].

2.1 Techninės priemonės

77. Šiame skirsnyje neišsamiai aprašomos pavyzdinės techninės priemonės, kurios galėtų papildyti BDAR 46 straipsnyje nurodytų perdavimo priemonių apsaugos priemones, kad būtų užtikrintas ES teisėje reikalaujamas apsaugos lygis perduodant asmens duomenis trečiai valstybei. Šios priemonės bus ypač reikalingos tais atvejais, kai tos valstybės teisės aktais duomenų importuotojui nustatomi įpareigojimai, kurie prieštarauja BDAR 46 straipsnyje nurodytų perdavimo priemonių apsaugos priemonėms ir visų pirma gali pažeisti sutartinę garantiją dėl iš esmės lygiaverčio lygio apsaugos nuo tos trečiosios valstybės valdžios institucijų prieigos prie tų duomenų[78].

78. Siekiant didesnio aiškumo, šiame skirsnyje pirmiausia aprašomi keli scenarijų, pagal kuriuos kai kurios techninės priemonės galėtų būti veiksmingos siekiant užtikrinti iš esmės lygiavertį apsaugos lygį, pavyzdžiai. Toliau šiame skirsnyje aprašyti tam tikri scenarijai, kai nenustatytos jokios techninės priemonės šiam apsaugos lygiui užtikrinti.

[77] BDAR 5 straipsnio 2 dalis ir 32 straipsnis.
[78] Sprendimo byloje C-311/18 (*Schrems II*) 135 punktas.

Scenarijų, susijusių su atvejais, kai nustatomos *veiksmingos* priemonės, pavyzdžiai

79. Toliau išvardytomis priemonėmis siekiama užtikrinti, kad trečiųjų valstybių valdžios institucijų prieiga prie perduotų duomenų nesumažintų BDAR 46 straipsnyje nustatytų perdavimo priemonių tinkamų apsaugos priemonių veiksmingumo. Šios priemonės būtų būtinos siekiant užtikrinti iš esmės lygiavertį apsaugos lygį garantuojamam EEE net tais atvejais, kai valdžios institucijų prieiga atitinka duomenų importuotojo valstybės įstatymų reikalavimus, jei praktiškai tokia prieiga viršija tai, kas būtina ir proporcinga demokratinėje visuomenėje[79]. Šiomis priemonėmis siekiama užkirsti kelią galimai neteisėtai prieigai, neleidžiant valdžios institucijoms nustatyti duomenų subjektų tapatybės, gauti apie juos informacijos, išskirti juos kitame kontekste arba susieti perduotus duomenis su kitais duomenų rinkiniais, kuriuose, be kitų duomenų, gali būti duomenų subjektų kitomis aplinkybėmis naudojamų prietaisų, taikomųjų programų, įrankių ir protokolų suteiktų internetinių identifikatorių.

80. Trečiųjų valstybių valdžios institucijos gali bandyti gauti prieigą prie perduodamų duomenų šiais būdais:

    a) persiuntimo metu gauti prieigą prie ryšio linijų, naudojamų duomenims gaunančiajai šaliai perduoti. Tokia prieiga gali būti pasyvi – tokiu atveju paprasčiausiai padaroma komunikacijos turinio kopija, galbūt po atrankos proceso. Tačiau prieiga taip pat gali būti aktyvi – tokiu atveju valdžios institucijos įsitraukia į komunikacijos procesą, ne tik susipažindamos su turiniu, bet ir manipuliuodamos jo dalimis ar neleisdamos jų gauti.

    b) kai duomenys saugomi pas numatytą gavėją – patekti į duomenų tvarkymo įrenginius arba pareikalauti, kad duomenų gavėjas nustatytų dominančių duomenų buvimo vietą, juos gautų ir perduotų valdžios institucijoms.

81. Šiame skirsnyje nagrinėjami scenarijai, kai taikomos abiem atvejais veiksmingos priemonės. Tam tikromis konkretaus perdavimo aplinkybėmis gali būti taikomos skirtingos papildomos priemonės, kurių gali pakakti, jei gaunančiosios valstybės teisėje numatyta tik vienos rūšies prieiga. Todėl būtina, kad duomenų eksportuotojas, padedamas duomenų importuotojo, atidžiai išanalizuotų pastarajam nustatytus įpareigojimus.

Pavyzdžiui, JAV duomenų importuotojai, kuriems taikomas USC 50 antraštinės dalies 1881a skyrius (FISA 702 straipsnis) yra tiesiogiai įpareigoti suteikti prieigą prie jų turimų, saugomų ar kontroliuojamų importuotų asmens duomenų arba juos perduoti. Tai gali būti taikoma bet kokiems šifravimo raktams, kurie būtini, kad duomenys būtų suprantami.

82. Scenarijuose aprašomos konkrečios aplinkybės ir priemonės, kurių imtasi kaip pavyzdžio. Bet kokie scenarijų pakeitimai gali lemti skirtingas išvadas. Scenarijai susiję su situacijomis, kai daroma išvada, kad visų pirma reikia papildomų priemonių, t. y. kai atitinkamam duomenų perdavimui praktiškai taikomi probleminiai trečiosios valstybės teisės aktai.

[79] Žr. ES pagrindinių teisių chartijos 47 ir 52 straipsnius, BDAR 23 straipsnio 1 dalį ir 2020 m. lapkričio 10 d. EDAV rekomendacijas Nr. 02/2020 dėl Europos pagrindinių garantijų taikant sekimo priemones.

83. Duomenų valdytojams gali prireikti taikyti kai kurias arba visas čia aprašytas priemones, neatsižvelgiant į duomenų importuotojui taikomuose įstatymuose nustatytą apsaugos lygį, nes konkrečiomis perdavimo aplinkybėmis jie turi laikytis BDAR 25 ir 32 straipsnių. Kitaip tariant, gali būti reikalaujama, kad duomenų eksportuotojai įgyvendintų šiame dokumente aprašytas priemones, net jei jų duomenų importuotojams taikomas sprendimas dėl tinkamumo, o iš duomenų valdytojų ir tvarkytojų gali būti reikalaujama jas įgyvendinti, kai duomenys tvarkomi EEE.

Naudojimo atvejis Nr. 1. Duomenų saugojimas atsarginei kopijai ir kitiems tikslams, kuriems nereikia prieigos prie nešifruotų duomenų

84. Duomenų eksportuotojas naudojasi prieglobos paslaugų teikėjo paslaugomis trečiojoje valstybėje asmens duomenims saugoti, pvz., kad turėtų atsarginę kopiją.

Jeigu:

1. prieš perdavimą asmens duomenys tvarkomi naudojant sudėtingą šifravimą ir patikrinama duomenų importuotojo tapatybė;
2. šifravimo algoritmas ir jo parametrai (pvz., rakto ilgis, veikimo režimas, jei taikoma) atitinka naujausius technikos laimėjimus ir gali būti laikomi patikimais, palyginti su duomenis gaunančios valstybės valdžios institucijų atliekama kriptoanalize, atsižvelgiant į jų turimus išteklius ir techninius pajėgumus (pvz., skaičiavimo galią grubios jėgos atakoms vykdyti)[80];
3. nustatant šifravimo sudėtingumą ir rakto ilgį, atsižvelgiama į konkretų laikotarpį, per kurį turi būti išsaugotas šifruotų asmens duomenų konfidencialumas[81];
4. šifravimo algoritmas yra teisingai įgyvendinamas tinkamai prižiūrimos programinės įrangos, kuri neturi žinomų trūkumų ir kurios atitiktis pasirinkto algoritmo specifikacijoms buvo patvirtinta, pavyzdžiui, sertifikavimo būdu;
5. raktai patikimai tvarkomi (generuojami, administruojami, saugomi, prireikus susiejami su numatomo gavėjo tapatybe, ir atšaukiami)[82];

---

[80] Vertindami šifravimo algoritmų sudėtingumą, jų atitiktį pažangiausioms technologijoms ir jų patikimumą atsižvelgiant į kriptoanalizę laikui bėgant, duomenų eksportuotojai gali remtis ES ir jos valstybių narių oficialių kibernetinio saugumo institucijų paskelbtomis techninėmis gairėmis. Žr., pvz., ENISA ataskaitą „Kokie naujausi technikos laimėjimai pasiekti IT saugumo srityje? “, 2019 m. https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security; Vokietijos Federalinio informacijos saugumo biuro gaires, pateiktas TR-02102 serijos techninėse gairėse ir „Algoritmų, rakto dydžio ir protokolų ataskaitą (2018 m.)“, H2020-ICT-2014 – projektas 645421, D5.4, ECRYPT-CSA, 2018 m. vasario mėn https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

[81] Kriptografinių algoritmų apsauginis pajėgumas ilgainiui mažėja dėl to, kad atrandama naujų kriptoanalizės metodų, atsiranda naujų kompiuterijos paradigmų, pvz., kvantinės kompiuterijos, ir apskritai padidėja turima skaičiavimo galia, nebent įrodoma, kad taikomi algoritmai yra teoriškai saugūs informacijos atžvilgiu. Tai visų pirma pasakytina apie viešojo rakto algoritmus, kurie tuo metu, kai rašomi, yra naudojami bendrai. Todėl duomenų eksportuotojas turi atsižvelgti į tai, kad valdžios institucijos gali įsipareigoti susipažinti su užšifruotais duomenimis 80 punkte aprašytomis aplinkybėmis ir juos saugoti tol, kol jų ištekliai bus pakankami iššifruoti. Papildoma priemonė gali būti laikoma veiksminga tik tuo atveju, jei toks iššifravimas ir tolesnis duomenų tvarkymas tuo metu nebebūtų duomenų subjektų teisių pažeidimas, pvz., dėl to, kad duomenys nebegali būti naudojami siekiant tiesiogiai ar netiesiogiai nustatyti duomenų subjektų tapatybę.

[82] NIST specialusis leidinys Nr. 800-57, Rekomendacija dėl rakto valdymo https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

6. raktus saugo tik duomenų eksportuotojas arba duomenų eksportuotojo įgaliotas subjektas EEE arba jurisdikcija, kurioje užtikrinamas apsaugos lygis, iš esmės lygiavertis garantuojamam EEE,

EDAV daro išvadą, kad atliktas šifravimas yra veiksminga papildoma priemonė.

Naudojimo atvejis Nr. 2. Pseudoniminių duomenų perdavimas

85. Duomenų eksportuotojas pirmiausia duomenims suteikia pseudonimus, o tada perduoda juos į trečiąją valstybę analizei, pvz., mokslinių tyrimų tikslais.

Jeigu:

1. duomenų eksportuotojas tvarkomus asmens duomenis perduoda taip, kad jų nebebūtų galima priskirti konkrečiam duomenų subjektui arba panaudoti duomenų subjektui išskirti didesnėje grupėje nenaudojant papildomos informacijos[83];
2. tą papildomą informaciją turi tik duomenų eksportuotojas ir ji atskirai laikoma valstybėje narėje arba trečiojoje valstybėje, duomenų eksportuotojo įgaliotas subjektas EEE arba jurisdikcija, užtikrinanti apsaugos lygį, iš esmės lygiavertį garantuojamam EEE;
3. atitinkamomis techninėmis ir organizacinėmis apsaugos priemonėmis užkertamas kelias atskleisti tą papildomą informaciją ar neleistinai ja naudotis, užtikrinama, kad algoritmą ar saugyklą, leidžiančią iš naujo nustatyti tapatybę panaudojant papildomą informaciją, ir toliau kontroliuotų tik duomenų eksportuotojas;
4. duomenų valdytojas, atlikęs išsamią atitinkamų duomenų analizę, atsižvelgdamas į bet kokią informaciją, kurią gali turėti ir naudoti duomenis gaunančios valstybės valdžios institucijos, nustatė, kad pseudoniminiai asmens duomenys negali būti priskirti fiziniam asmeniui, kurio tapatybė nustatyta arba gali būti nustatyta, net jei juose ir minėtoje informacijoje yra tarpusavio nuorodų,

EDAV daro išvadą, kad pseudonimų suteikimas yra veiksminga papildoma priemonė.

86. Pažymėtina, kad daugeliu atvejų dėl fizinio asmens fizinei, fiziologinei, genetinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingų veiksnių, jo fizinės buvimo vietos ar naudojimosi internetine paslauga tam tikru metu[84] gali būti įmanoma nustatyti to asmens tapatybę, net jei nenurodytas jo vardas, pavardė, adresas ar kiti įprasti identifikatoriai.

87. Tai ypač aktualu tais atvejais, kai duomenys yra susiję su naudojimusi informacinėmis paslaugomis (prieigos laikas, pasiekiamų funkcijų seka, naudojamo prietaiso charakteristikos ir pan.). Šių

[83] Pagal BDAR 4 straipsnio 5 dalį: „pseudonimų suteikimas – asmens duomenų tvarkymas taip, kad asmens duomenys nebegalėtų būti priskirti konkrečiam duomenų subjektui nesinaudojant papildoma informacija, jeigu tokia papildoma informacija yra saugoma atskirai ir jos atžvilgiu taikomos techninės bei organizacinės priemonės siekiant užtikrinti asmens duomenų nepriskyrimą fiziniam asmeniui, kurio tapatybė yra nustatyta arba kurio tapatybę galima nustatyti“. Papildomi duomenys gali būti lentelės, kuriose pateikiami pseudonimai su juos pakeičiančiais identifikavimo požymiais, kriptografiniai raktai ar kiti parametrai požymių keitimui arba kiti duomenys, kuriais remiantis pseudoniminius duomenis galima priskirti fiziniams asmenims, kurių tapatybė yra nustatyta arba kurių tapatybę galima nustatyti.

[84] BDAR 4 straipsnio 1 dalis: „asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius“.

paslaugų teikėjai, kaip ir asmens duomenų importuotojas, gali būti įpareigoti suteikti prieigą toms pačioms jų jurisdikcijoje esančioms valdžios institucijoms, kurios tada tikriausia turės duomenų apie jas dominančio (-ų) asmens (-ų) naudojimąsi tomis informacinėmis paslaugomis.

88. Be to, atsižvelgiant į tai, kad kai kuriomis informacinėmis paslaugomis naudojamasi viešai arba kad jomis gali pasinaudoti daug išteklių turinčios šalys, duomenų valdytojai turi būti ypač atsargūs, nes jų jurisdikcijoje esančios valdžios institucijos tikriausiai turi duomenų apie jas dominančio asmens naudojimąsi informacinėmis paslaugomis.

89. Jeigu pseudonimų suteikimo metu asmens duomenyse esantys požymiai pakeičiami naudojant kriptografinį algoritmą, taikomos 80 ir 81 išnašose pateiktos gairės. Nuo šiol rekomenduojama atsisakyti išimtinio kriptografijos naudojimo ir taikyti transformacijas, pagrįstas lentelės paieškos mechanizmais.

Naudojimo atvejis Nr. 3. Duomenų šifravimas, siekiant apsaugoti juos nuo duomenų importuotojo trečiosios valstybės valdžios institucijų prieigos, kai jie siunčiami tarp duomenų eksportuotojo ir importuotojo

90. Duomenų eksportuotojas nori perduoti duomenis į paskirties vietą, kurioje pagal įstatymus ir (arba) praktiką valdžios institucijos gali gauti prieigą prie duomenų siunčiant iš duomenų eksportuotojo šalies į paskirties šalį.

Jeigu:

1. duomenų eksportuotojas perduoda asmens duomenis duomenų importuotojui jurisdikcijoje, kurioje pagal įstatymus ir (arba) praktiką valdžios institucijos gali gauti prieigą prie duomenų, kai jie internetu perduodami į šią trečiąją valstybę be esminių Europos garantijų, susijusių su šia prieiga, naudojamas srauto šifravimas, užtikrinant, kad naudojami šifravimo protokolai atspindėtų naujausius technikos laimėjimus ir veiksmingai apsaugotų nuo aktyvių ir pasyvių atakų naudojant trečiosios valstybės valdžios institucijoms prieinamus išteklius;
2. komunikacijoje dalyvaujančios šalys susitaria dėl patikimos viešojo rakto sertifikavimo institucijos arba infrastruktūros;
3. taikomos specialios apsaugos ir pažangiausios priemonės, skirtos apsisaugoti nuo aktyvių ir pasyvių išpuolių prieš siunčiančiąsias ir priimančiąsias sistemas, užtikrinančias srauto šifravimą, įskaitant programinės įrangos pažeidžiamumo ir galimus bandymus patekti slaptai;
4. jei srauto šifravimas pats savaime neužtikrina tinkamo saugumo dėl infrastruktūros ar naudojamos programinės įrangos pažeidžiamumo, taikomas ir ištisinis asmens duomenų šifravimas taikomųjų programų lygmenyje naudojant pažangiausius šifravimo metodus;
5. šifravimo algoritmas ir jo parametrai (pvz., rakto ilgis, veikimo režimas, jei taikoma) atitinka naujausius technikos laimėjimus ir gali būti laikomi patikimais, palyginti su valstybės, kai į ją siunčiami duomenys, valdžios institucijų atliekama kriptoanalize, atsižvelgiant į jų turimus išteklius ir techninius pajėgumus (pvz., skaičiavimo galią grubios jėgos atakoms vykdyti) (žr. 80 išnašą)[85];
6. nustatant šifravimo sudėtingumą, atsižvelgiama į konkretų laikotarpį, per kurį turi būti išsaugotas šifruotų asmens duomenų konfidencialumas;

[85] Žr. 80 išnašą dėl kai kurių nuorodų į ES ir jos valstybių narių oficialių kibernetinio saugumo institucijų paskelbtas technines gaires.

7. šifravimo algoritmas yra teisingai įgyvendinamas tinkamai prižiūrimos programinės įrangos, kuri neturi žinomų trūkumų ir kurios atitiktis pasirinkto algoritmo specifikacijoms buvo patvirtinta, pavyzdžiui, sertifikavimo būdu;
8. raktus patikimai valdo (generuoja, administruoja, saugo, prireikus susieja su numatomo gavėjo tapatybe ir panaikina) duomenų eksportuotojas arba subjektas, kuriuo duomenų eksportuotojas pasitiki, jurisdikcijoje, kurioje užtikrintas iš esmės lygiavertis apsaugos lygis,

EDAV daro išvadą, kad srauto šifravimas, prireikus kartu su ištisiniu turinio šifravimu, yra veiksminga papildoma priemonė.

Naudojimo atvejis Nr. 4. Apsaugotas gavėjas

91. Duomenų eksportuotojas perduoda asmens duomenis duomenų importuotojui trečiojoje valstybėje, kuris yra specialiai apsaugotas tos valstybės teisės aktais, pvz., siekiant kartu teikti medicininį gydymą pacientui arba teisines paslaugas klientui.

Jeigu:

1. pagal trečiosios valstybės įstatymus duomenų importuotojui taikoma išimtis ir nesuteikiama galimai neteisėta prieiga prie duomenų, kuriuos tas gavėjas turi konkrečiu tikslu, pvz., dėl duomenų importuotoją saistančios profesinės paslapties;
2. išimtis taikoma visai duomenų importuotojo turimai informacijai, kuri gali būti naudojama siekiant apeiti konfidencialios informacijos (šifravimo raktų, slaptažodžių, kitų identifikavimo priemonių ir t. t.) apsaugą;
3. duomenų importuotojas nesinaudoja duomenų tvarkytojo paslaugomis taip, kad valdžios institucijos galėtų gauti prieigą prie duomenų tvarkytojo turimų duomenų, taip pat duomenų importuotojas neperduoda duomenų kitam subjektui, kuris nėra apsaugotas, remdamasis BDAR 46 straipsnyje nurodytomis perdavimo priemonėmis;
4. prieš perdavimą duomenys užšifruojami pažangiausiu metodu, užtikrinančiu, kad iššifravimas nebus įmanomas be iššifravimo rakto (ištisinis šifravimas) per visą duomenų apsaugos laikotarpį;
5. iššifravimo raktą saugo tik apsaugotas duomenų importuotojas ir galbūt pats duomenų eksportuotojas arba kitas duomenų eksportuotojo įgaliotas subjektas, įsikūręs EEE arba jurisdikcijoje, kurioje užtikrinamas apsaugos lygis, iš esmės lygiavertis garantuojamam EEE, ir raktas yra tinkamai apsaugotas nuo neteisėto naudojimo ar atskleidimo pažangiausiomis techninėmis ir organizacinėmis priemonėmis;
6. duomenų eksportuotojas tinkamai nustatė, kad šifravimo raktas, kurį jis ketina naudoti, atitinka gavėjo turimą iššifravimo raktą,

EDAV daro išvadą, kad atliekamas srauto šifravimas yra veiksminga papildoma priemonė.

Naudojimo atvejis Nr. 5. Duomenų tvarkymas juos padalijus arba daugiašalis tvarkymas

92. Duomenų eksportuotojas pageidauja, kad asmens duomenis kartu tvarkytų du ar daugiau nepriklausomų duomenų tvarkytojų, esančių skirtingose jurisdikcijose, neatskleidžiant jiems duomenų turinio. Prieš perduodant duomenis, jie suskaidomi taip, kad nė vienos dalies, kurią gauna vienas duomenų tvarkytojas, nepakaktų visiems asmens duomenims arba jų daliai atkurti. Duomenų eksportuotojas iš kiekvieno duomenų tvarkytojo atskirai gauna duomenų tvarkymo

rezultatą ir sujungia gautus duomenis, kad gautų galutinį rezultatą – asmens arba suvestinius duomenis.

Jeigu:

1. duomenų eksportuotojas tvarko asmens duomenis taip, kad jie padalijami į dvi ar daugiau dalių, kurių kiekvienos nebegalima suprasti arba priskirti konkrečiam duomenų subjektui nenaudojant papildomos informacijos;
2. kiekviena dalis perduodama atskiram duomenų tvarkytojui, esančiam kitoje jurisdikcijoje;
3. duomenų tvarkytojai gali tvarkyti duomenis kartu, pvz., saugaus daugiašalio skaičiavimo būdu, kad nė vienam iš jų nebūtų atskleista jokia informacija, kurios jie iki skaičiavimo neturėjo;
4. bendram skaičiavimui naudojamas algoritmas yra apsaugotas nuo aktyvių atakų;
5. duomenų valdytojas, atlikęs išsamią atitinkamų duomenų analizę, atsižvelgdamas į bet kokią informaciją, kurią gali turėti ir naudoti duomenis gaunančios valstybės valdžios institucijos, nustatė, kad jos perduodami asmens duomenų vienetai, kuriuos jis perduoda duomenų tvarkytojams, negali būti priskirti fiziniam asmeniui, kurio tapatybė nustatyta arba gali būti nustatyta, net jei minėtoje informacijoje ir duomenyse yra tarpusavio nuorodų;
6. nėra įrodymų, kad valdžios institucijos, esančios atitinkamose jurisdikcijose, kuriose įsikūręs kiekvienas iš duomenų tvarkytojų, bendradarbiautų taip, kad tai suteiktų joms prieigą prie tvarkytojų turimų asmens duomenų bei galimybę aiškiai atkurti bei panaudoti asmens duomenų turinį tokiomis aplinkybėmis, kai tokiu panaudojimu būtų pažeista duomenų subjektų pagrindinių teisių ir laisvių esmė. Be to, nei vienos valstybės valdžios institucijoms neturėtų būti suteikta teisė susipažinti su visų susijusių jurisdikcijų duomenų tvarkytojų turimais asmens duomenimis,

EDAV daro išvadą, kad atliekamas padalytų duomenų tvarkymas yra veiksminga papildoma priemonė.

Scenarijų, susijusių su atvejais, kai *veiksmingos* priemonės nenustatomos, pavyzdžiai

93. Toliau aprašytos priemonės pagal tam tikrus scenarijus nebūtų veiksmingos užtikrinant iš esmės lygiavertę trečiajai valstybei perduodamų duomenų apsaugą. Todėl jos nebūtų laikomos tinkamomis papildomomis priemonėmis.

Naudojimo atvejis Nr. 6. Perdavimas debesijos paslaugų teikėjams ar kitiems duomenų tvarkytojams, kuriems reikalinga prieiga prie nešifruotų duomenų

94. Duomenų eksportuotojas perduoda asmens duomenis elektroniniu būdu arba sudarydamas galimybę jais naudotis debesijos paslaugų teikėjui ar kitam duomenų tvarkytojui, kad asmens duomenys būtų tvarkomi pagal jo nurodymus trečiojoje valstybėje (pvz., techninės paramos teikimo arba bet kokios rūšies nuotolinių kompiuterinių išteklių tvarkymo tikslais), ir šie duomenys nėra (arba negali būti) pseudoniminiai, kaip aprašyta 2 naudojimo atveju, arba užšifruoti, kaip aprašyta 1 naudojimo atveju, nes tvarkant duomenis reikia aiškiai susipažinti su duomenimis.

Jeigu:

1. duomenų valdytojas perduoda asmens duomenis debesijos paslaugų teikėjui arba kitam duomenų tvarkytojui;
2. debesijos paslaugų teikėjui arba kitam duomenų tvarkytojui reikia prieigos prie nešifruotų duomenų, kad galėtų vykdyti paskirtą užduotį;
3. duomenis gaunančios valstybės valdžios institucijoms suteikti įgaliojimai susipažinti su atitinkamais perduotais duomenimis viršija tai, kas būtina ir proporcinga demokratinėje visuomenėje, kurioje nagrinėjamiems perdavimams praktiškai taikomi probleminiai trečiosios valstybės teisės aktai (žr. 3 etapą)[86],

atsižvelgdama į naujausius techninius laimėjimus, EDAV nemato veiksmingų techninių priemonių, kurios galėtų užtikrinti, kad ta prieiga nepažeistų duomenų subjekto pagrindinių teisių. EDAV neatmeta galimybės, kad dėl tolesnės technologijų plėtros gali atsirasti priemonių, kuriomis būtų galima pasiekti numatytų verslo tikslų be būtinybės turėti prieigą prie nešifruotų duomenų.

95. Nurodytais atvejais, kai duomenų tvarkytojui teikiant paslaugą yra techniškai būtini nešifruoti asmens duomenys, srauto šifravimas ir nenaudojamų duomenų šifravimas, net kartu paėmus, nėra papildoma priemonė, užtikrinanti iš esmės lygiavertį apsaugos lygį, jei duomenų importuotojas turi šifravimo raktus.

Naudojimo atvejis Nr. 7. Asmens duomenų perdavimas verslo tikslais, be kita ko, naudojantis nuotoline prieiga

96. Duomenų eksportuotojas perduoda asmens duomenis subjektams trečiojoje valstybėje, kad jie būtų naudojami dalijimosi verslo tikslais (elektroniniu būdu arba duomenų importuotojui suteikiant galimybę su jais susipažinti nuotoliniu būdu), ir šiems duomenims nėra arba negali būti suteikti pseudonimai, kaip aprašyta 2 naudojimo atveju, arba jie negali būti šifruojami, kaip aprašyta 1 naudojimo atveju, nes tvarkant duomenis reikia aiškiai susipažinti su duomenimis. Tipinę struktūrą gali sudaryti duomenų valdytojas arba duomenų tvarkytojas, įsisteigęs valstybės narės teritorijoje, perduodantis asmens duomenis duomenų valdytojui arba duomenų tvarkytojui trečiojoje valstybėje, priklausančiam tai pačiai įmonių grupei arba bendrą ekonominę veiklą vykdančių įmonių grupei. Pavyzdžiui, duomenų importuotojas gautus duomenis gali naudoti teikdamas personalo paslaugas duomenų eksportuotojui, ir šiam tikslui jam reikia žmogiškųjų išteklių duomenų, arba naudoti juos bendraudamas telefonu ar elektroniniu paštu su Europos Sąjungoje gyvenančiais duomenų eksportuotojo klientais.

Jeigu:

1. duomenų eksportuotojas perduoda asmens duomenis duomenų importuotojui trečiojoje valstybėje, sudarydamas sąlygas su jais susipažinti informacinėje sistemoje taip, kad duomenų importuotojas galėtų tiesiogiai susipažinti su savo pasirinktais duomenimis, arba tiesiogiai, individualiai ar dideliais kiekiais juos perduoda naudodamasi ryšių paslauga;
2. duomenų importuotojas[87] tvarko duomenis aiškiai trečiojoje šalyje (taip pat ir savo tikslais, kai duomenų importuotojas yra duomenų valdytojas);

[86] Žr. ES pagrindinių teisių chartijos 47 ir 52 straipsnius, BDAR 23 straipsnio 1 dalį ir 2020 m. lapkričio 10 d. EDAV rekomendacijas Nr. 02/2020 dėl Europos pagrindinių garantijų taikant sekimo priemones.

[87] Nesvarbu, ar tai yra duomenų valdytojas ar duomenų tvarkytojas trečiojoje valstybėje, gaunantis asmens duomenis, perduodamus iš EEE, arba gaunantis prieigą prie jų.

3. duomenis gaunančios valstybės valdžios institucijoms suteikti įgaliojimai susipažinti su perduotais duomenimis viršija tai, kas būtina ir proporcinga demokratinėje visuomenėje, kurioje nagrinėjamiems perdavimams praktiškai taikomi probleminiai trečiosios valstybės teisės aktai (žr. 3 etapą),

EDAV nemato veiksmingų techninių priemonių, kurios galėtų užtikrinti, kad ta prieiga nepažeistų duomenų subjekto pagrindinių teisių.

97. Nurodytais atvejais, kai duomenų tvarkytojui teikiant paslaugą yra techniškai būtini nešifruoti asmens duomenys, srauto šifravimas ir nenaudojamų duomenų šifravimas, net kartu paėmus, nėra papildoma priemonė, užtikrinanti iš esmės lygiavertį apsaugos lygį, jei duomenų importuotojas turi šifravimo raktus.

2.2. Papildomos sutartinės priemonės

98. Šias priemones paprastai sudaro vienašaliai, dvišaliai ar daugiašaliai[88] sutartiniai įsipareigojimai[89]. Jei naudojama pagal 46 straipsnį sukurta BDAR perdavimo priemonė, į ją daugeliu atvejų jau bus įtraukti keli (daugiausia sutartiniai) duomenų eksportuotojo ir duomenų importuotojo įsipareigojimai, kuriais siekiama užtikrinti asmens duomenų apsaugą[90].

99. Kai kuriais atvejais šios priemonės gali papildyti ir sustiprinti apsaugos priemones, numatytas duomenų perdavimo priemonėje ir atitinkamuose trečiosios valstybės teisės aktuose, kai, atsižvelgiant į perdavimo aplinkybes, jos neatitinka visų sąlygų, reikalingų norinti užtikrinti apsaugos lygį, iš esmės lygiavertį EEE garantuojamam lygiui. Atsižvelgiant į sutartinių priemonių, kuriomis paprastai negalima įpareigoti atitinkamos trečiosios valstybės valdžios institucijų, kai jos nėra sutarties šalys[91], pobūdį, šios priemonės dažnai turėtų būti derinamos su kitomis techninėmis ir organizacinėmis priemonėmis, kad būtų užtikrintas reikiamas duomenų apsaugos lygis. Vienos ar keleto iš šių priemonių pasirinkimas nereiškia, kad bus tikrai ir sistemingai užtikrinta jūsų vykdomo perdavimo atitiktis esminio lygiavertiškumo standartui pagal ES teisę.

100. Priklausomai nuo to, kokios sutartinės priemonės jau įtrauktos į BDAR 46 straipsnio perdavimo priemonę, kuria remiamasi, taip pat gali būti naudingos papildomos sutartinės priemonės, kad EEE įsikūrę duomenų eksportuotojai galėtų sužinoti apie naujus pokyčius, turinčius įtakos trečiosioms valstybėms perduodamų duomenų apsaugai.

---

[88] Pavyzdžiui, pagal ĮPT, kuriomis bet kuriuo atveju turėtų būti reglamentuojamos kai kurios iš toliau išvardytų priemonių.

[89] Jie bus privataus pobūdžio ir nebus laikomi tarptautiniais susitarimais pagal viešąją tarptautinę teisę. Todėl, kaip Teisingumo Teismas pabrėžė savo sprendimo byloje C-311/18 (*Schrems II*) 125 punkte, jais paprastai neįpareigojamos trečiosios valstybės valdžios institucijos, nes jos nėra trečiųjų valstybių privačių subjektų sutarčių šalys.

[90] Žr. sprendimo C-311/18 (*Schrems II*) 137 punktą, kuriame Teisingumo Teismas atitinkamai pripažino, kad SSS yra „veiksmingi mechanizmai, leidžiantys praktiškai užtikrinti, kad būtų laikomasi Sąjungos teisėje reikalaujamo apsaugos lygio ir kad asmens duomenų perdavimas, grindžiamas tokiomis sąlygomis, būtų sustabdytas arba uždraustas pažeidus šias sąlygas arba nesant galimybės jų laikytis“, taip pat žr. 148 punktą.

[91] Sprendimo byloje C-311/18 (*Schrems II*) 125 punktas.

101. Kaip minėta, sutartinėmis priemonėmis negalima panaikinti EDAV nustatyto Europos pagrindinių garantijų standarto neatitinkančios trečiosios valstybės teisės aktų galiojimo tais atvejais, kai teisės aktais duomenų importuotojai įpareigojami vykdyti iš valdžios institucijų gautus nurodymus atskleisti duomenis[92].

102. Toliau išvardyti keli galimų sutartinių priemonių pavyzdžiai, suklasifikuoti pagal jų pobūdį:

Sutartinės prievolės naudoti specialias technines priemones nustatymas

103. Atsižvelgiant į konkrečias perdavimo aplinkybes (įskaitant praktinį trečiosios valstybės teisės aktų taikymą), sutartyje gali tekti numatyti, kad norint įvykdyti perdavimą reikia įgyvendinti specialias technines priemones (žr. pirmiau pasiūlytas technines priemones).

104. Veiksmingumo sąlygos

- Ši sąlyga galėtų būti veiksminga tais atvejais, kai duomenų eksportuotojas nustato techninių priemonių poreikį. Tuomet ji turėtų būti pateikta teisine forma, siekiant užtikrinti, kad duomenų importuotojas taip pat įsipareigotų prireikus imtis reikiamų techninių priemonių.

Įsipareigojimai dėl skaidrumo

105. Duomenų eksportuotojas galėtų prie sutarties pridėti priedus su informacija, kurią dėdamas visas pastangas pateiktų importuotojas prieš sudarydamas sutartį, dėl valdžios institucijų prieigos prie duomenų paskirties valstybėje, įskaitant žvalgybos srityje, jei teisės aktai atitinka EDAV nustatytas Europos pagrindines garantijas. Tai galėtų padėti duomenų eksportuotojui įvykdyti savo įsipareigojimą dokumentuoti savo atliktą apsaugos lygio trečiojoje valstybėje vertinimą. Tai taip pat gali išryškinti duomenų importuotojo pareigą padėti eksportuotojui atlikti vertinimą ir prisiimti atsakomybę teikiant jam objektyvią, patikimą, svarbią, patikrinamą ir viešai ar kitaip prieinamą informaciją.

106. Pavyzdžiui, iš duomenų importuotojo gali būti reikalaujama:

> (1) išvardyti paskirties valstybėje duomenų importuotojui arba jo duomenų tvarkytojams (pagalbiniams duomenų tvarkytojams) taikomus įstatymus ir kitus teisės aktus, kurie leistų valdžios institucijoms susipažinti su perduodamais asmens duomenimis, visų pirma žvalgybos, teisėsaugos ir perduodamų duomenų administracinės bei reguliavimo priežiūros srityse;
>
> (2) jei nėra įstatymų, reglamentuojančių valdžios institucijų prieigą prie duomenų – teikti informaciją ir statistinius duomenis, pagrįstus duomenų importuotojo patirtimi arba informacija iš įvairių šaltinių (pvz., partnerių, atvirųjų šaltinių, nacionalinių teismų praktikos ir priežiūros įstaigų sprendimų) dėl valdžios institucijų prieigos prie asmens duomenų tais atvejais, kai vykdomas atitinkamo pobūdžio duomenų perdavimas (t. y. konkrečioje reguliavimo srityje; susijęs su tokio pobūdžio subjektais kaip duomenų importuotojas;...)
>
> (3) nurodyti priemonės, kurių imtasi siekiant užkirsti kelią prieigai prie perduodamų duomenų (jei tokių yra);

[92] ESTT sprendimo byloje C-311/18 (*Schrems II*) 132 punktas.

(4) pateikti pakankamai išsamią informaciją apie visus valdžios institucijų prašymus susipažinti su asmens duomenimis, kuriuos duomenų importuotojas gavo per nustatytą laikotarpį[93], visų pirma 1 punkte nurodytose srityse, įskaitant informaciją apie gautus prašymus, prašomus duomenis, prašančiąją įstaigą ir atskleidimo teisinį pagrindą bei apie tai, kokiu mastu duomenų importuotojas atskleidė prašymą pateikti duomenis[94];

nurodyti, ar duomenų importuotojui teisiškai draudžiama pateikti 1-5 punktuose nurodytą informaciją ir kokiu mastu.

107. Šią informaciją būtų galima pateikti naudojant struktūruotus klausimynus, kuriuos duomenų importuotojas užpildytų, pasirašytų, taip pat jis turėtų sutartinę prievolę per nustatytą laikotarpį pranešti apie bet kokį galimą šios informacijos pasikeitimą, kaip daroma pagal dabartinę išsamaus patikrinimo tvarką.

108. Veiksmingumo sąlygos

- Duomenų importuotojas turi sugebėti pateikti duomenų eksportuotojui šių rūšių informaciją, kiek ji jam žinoma ir dėdamas visas pastangas jai gauti.
- Šis duomenų importuotojui nustatytas įpareigojimas yra priemonė užtikrinti, kad duomenų eksportuotojas būtų informuotas ir žinotų apie riziką, susijusią su duomenų perdavimu į trečiąja valstybę. Tokiu būdu duomenų eksportuotojas galės atsisakyti sudaryti sutartį arba, jei informacija pasikeistų ją sudarius, įvykdyti savo įsipareigojimą sustabdyti siuntimą ir (arba) nutraukti sutartį, jei trečiosios valstybės teisė, naudojamos BDAR 46 straipsnyje numatytos perdavimo priemonės apsaugos priemonės ir bet kokios jo priimtos papildomos apsaugos priemonės nebegali užtikrinti apsaugos lygio, iš esmės lygiaverčio EEE apsaugos lygiui. Tačiau šis įpareigojimas nesuteikia teisės duomenų importuotojui atskleisti asmens duomenų ir neleidžia tikėtis, kad nebebus prašymų dėl prieigos.

***

109. Duomenų eksportuotojas taip pat galėtų pridėti sąlygas, pagal kurias duomenų importuotojas patvirtina, kad: 1) jis sąmoningai nesukūrė slapto patekimo galimybių ar panašių programų, kurios galėtų būti panaudotos prieigai prie sistemos ir (arba) asmens duomenų; 2) jis sąmoningai nesukūrė ir nepakeitė savo verslo procesų taip, kad palengvintų prieigą prie asmens duomenų ar sistemų; 3) kad nacionalinėje teisėje ar vyriausybės politikoje nereikalaujama, kad duomenų importuotojas sukurtų ar palaikytų slapto patekimo galimybes arba palengvintų prieigą prie asmens duomenų ar sistemų arba kad duomenų importuotojas turėtų ar perduotų šifravimo raktą[95].

110. Veiksmingumo sąlygos

- Dėl galiojančių teisės aktų ar vyriausybės politikos, neleidžiančios duomenų importuotojams atskleisti šios informacijos, ši sąlyga gali tapti neveiksminga. Todėl duomenų importuotojas

[93] Laikotarpio trukmė turėtų priklausyti nuo grėsmės duomenų subjektų, kurių duomenys perduodami, teisėms ir laisvėms, pvz., paskutiniai metai iki duomenų eksporto priemonės taikymo duomenų eksportuotojui pabaigos.
[94] Šios pareigos laikymasis savaime nereiškia tinkamo apsaugos lygio. Kita vertus, bet kokio netinkamo faktinio atskleidimo atveju būtina įgyvendinti papildomas priemones.
[95] Ši sąlyga yra svarbi siekiant užtikrinti tinkamą perduodamų asmens duomenų apsaugos lygį ir paprastai turėtų būti privaloma.

negalės sudaryti sutarties arba turės pranešti duomenų eksportuotojui, kad nebegali toliau laikytis sutartinių įsipareigojimų.

- Sutartyje turi būti numatytos nuobaudos ir (arba) duomenų eksportuotojo galimybė nutraukti sutartį per trumpą laiką tais atvejais, jei duomenų importuotojas neatskleidžia, kad egzistuoja slapto patekimo arba panašios programos arba yra manipuliuojama verslo procesais, arba yra nustatytas reikalavimas juos įgyvendinti, arba sužinojęs apie jų egzistavimą nedelsdamas neinformuoja duomenų eksportuotojo.
- Tais atvejais, kai duomenų importuotojas atskleidė asmens duomenis, perduotus pažeidžiant pagal pasirinktą duomenų perdavimo priemonę prisiimtus įsipareigojimus, į sutartį taip pat gali būti įtraukta duomenų importuotojo kompensacija duomenų subjektui už bet kokią patirtą turtinę ir neturtinę žalą.

***

111. Duomenų eksportuotojas galėtų sustiprinti savo įgaliojimus atlikti duomenų importuotojo duomenų tvarkymo įrangos auditą[96] arba patikrinimus vietoje ir (arba) nuotoliniu būdu, kad įvertintų, ar duomenys buvo atskleisti valdžios institucijoms ir kokiomis sąlygomis (ar prieiga neviršija to, kas būtina ir proporcinga demokratinėje visuomenėje), pavyzdžiui, numatydamas skubų įspėjimą ir mechanizmus, užtikrinančius greitą kontrolės įstaigų įsikišimą, ir sustiprindamas duomenų eksportuotojo savarankiškumą atrenkant kontrolės įstaigas.

112. Veiksmingumo sąlygos

- Kad auditas būtų visiškai veiksmingas, jis turėtų teisiškai ir techniškai apimti bet kokį duomenų importuotojo duomenų tvarkytojų ar pagalbinių duomenų tvarkytojų atliekamą trečiojoje valstybėje perduotų asmens duomenų tvarkymą.
- Prieigos žurnalai ir kiti panašūs atsekimo duomenys turėtų būti apsaugoti nuo klastojimo (pvz., jie turėtų būti nepakeičiami naudojant pažangiausius šifravimo metodus, kaip antai maišas, ir sistemingai periodiškai perduodami duomenų eksportuotojui), kad auditoriai galėtų rasti atskleidimo įrodymų. Prieigos žurnaluose ir kituose panašiuose atsekimo duomenyse taip pat turėtų būti atskirta prieiga dėl įprastų verslo operacijų ir prieiga pagal nurodymus ar prašymus suteikti prieigą.

***

113. Jei iš pradžių buvo įvertinti duomenų importuotojo trečiosios valstybės įstatymai bei praktika ir padaryta išvada, kad jie duomenų eksportuotojo perduodamiems duomenims užtikrina apsaugos lygį, iš esmės lygiavertį garantuojamam ES, duomenų eksportuotojas vis tiek galėtų sugriežtinti duomenų importuotojo pareigą, pasikeitus situacijai, skubiai informuoti duomenų eksportuotoją,

[96] Žr., pavyzdžiui, Sprendimo 2010/87/ES dėl duomenų valdytojų ir duomenų tvarkytojų sutarčių standartinių sąlygų 5 sąlygos f punktą, pagal kurį auditas taip pat galėtų būti atliekamas pagal elgesio kodeksą arba sertifikavimo būdu.

kad jis negali laikytis sutartinių įsipareigojimų, taigi ir užtikrinti reikalaujamo „iš esmės lygiaverčio duomenų apsaugos lygio“[97].

114. Šį įsipareigojimų nevykdymą gali lemti trečiosios valstybės teisės aktų ar praktikos pakeitimai[98]. Sąlygose galėtų būti nustatyti konkretūs ir griežti laiko apribojimai bei tvarka, kaip greitai sustabdyti duomenų perdavimą ir (arba) nutraukti sutartį ir kaip duomenų importuotojas turi grąžinti arba ištrinti gautus duomenis. Stebėdamas gautus prašymus, jų apimtį ir jiems atmesti skirtų priemonių veiksmingumą, duomenų eksportuotojas turėtų gauti pakankamai informacijos, kad galėtų įvykdyti savo pareigą sustabdyti arba nutraukti perdavimą ir (arba) nutraukti sutartį.

115. Veiksmingumo sąlygos

- Pranešimas turi būti pateiktas prieš suteikiant prieigą prie duomenų. Priešingu atveju, duomenų eksportuotojui gavus pranešimą, asmens teisės jau gali būti pažeistos, jei prašymas grindžiamas tos trečiosios valstybės įstatymais, kurie viršija tai, kas leidžiama pagal ES teisės aktuose užtikrinamą duomenų apsaugos lygį. Pranešimas vis tiek gali padėti užkirsti kelią būsimiems pažeidimams ir leisti duomenų eksportuotojui įvykdyti savo pareigą sustabdyti asmens duomenų perdavimą trečiajai valstybei ir (arba) nutraukti sutartį.
- Duomenų importuotojas privalo stebėti visus teisinius ar politinius pokyčius, dėl kurių jis gali nesugebėti laikytis savo įsipareigojimų, ir nedelsdamas informuoti duomenų eksportuotoją apie visus tokius pakeitimus ir pokyčius, jei įmanoma, prieš juos įgyvendinant, kad duomenų eksportuotojas galėtų susigrąžinti duomenis iš duomenų importuotojo.
- Sąlygose turėtų būti numatytas greitas mechanizmas, pagal kurį duomenų eksportuotojas leistų duomenų importuotojui nedelsiant apsaugoti arba grąžinti duomenis duomenų eksportuotojui arba, jei tai neįmanoma, ištrinti arba saugiai užšifruoti duomenis nelaukiant duomenų eksportuotojo nurodymų, jei laikomasi konkrečios ribos[99] , dėl kurios turi susitarti duomenų eksportuotojas ir duomenų importuotojas. Duomenų importuotojas turėtų įgyvendinti šį mechanizmą nuo duomenų perdavimo pradžios ir reguliariai jį tikrinti, kad būtų užtikrinta galimybė jį taikyti nedelsiant.
- Kitos sąlygos galėtų padėti duomenų eksportuotojui stebėti, kaip duomenų importuotojas laikosi šių įsipareigojimų, atliekant auditą, patikrinimus ir taikant kitas tikrinimo priemones, ir užtikrinti jų įgyvendinimą nuobaudomis duomenų importuotojui ir (arba) įgyvendinant duomenų eksportuotojo teisę sustabdyti perdavimą ir (arba) nedelsiant nutraukti sutartį.

***

[97] Sprendimo 2010/87/ES dėl SSS 5 sąlygos a punktas ir d punkto i papunktis.

[98] Žr. sprendimo byloje C-311/18 (*Schrems II*) 139 punktą, kuriame Teismas nurodė, jog „nors pagal tos pačios 5 sąlygos d punkto i papunktį perduodamų asmens duomenų gavėjui leidžiama nepranešti Sąjungoje įsteigtam duomenų valdytojui apie bet kokį teisiškai įpareigojantį teisėsaugos institucijų prašymą atskleisti asmens duomenis, jei pagal teisės aktus jam tai draudžiama, pavyzdžiui, nustatytas draudimas pagal baudžiamąją teisę, kuriuo siekiama užtikrinti teisėsaugos institucijų vykdomo tyrimo konfidencialumą, jis vis tiek pagal SAS sprendimo priedo 5 sąlygos a punktą privalo informuoti duomenų valdytoją, kad negali laikytis standartinių duomenų apsaugos sąlygų”.

[99] Šia riba turėtų būti užtikrinta, kad duomenų subjektams ir toliau būtų taikomas apsaugos lygis, lygiavertis EEE garantuojamam apsaugos lygiui.

116. Jei tai leidžiama pagal trečiosios valstybės nacionalinę teisę, sutartimi galėtų būti sugriežtinti duomenų importuotojo skaidrumo įsipareigojimai, numatant galimybę panaudoti „Warrant Canary“ (slapto perspėjimo) metodą, pagal kurį duomenų importuotojas įsipareigoja reguliariai (pvz., ne rečiau kaip kas 24 valandas) skelbti užšifruotai pasirašytą pranešimą, informuojantį duomenų eksportuotoją, kad nuo tam tikros datos ir laiko jis negavo nurodymo atskleisti asmens duomenis ar pan. Jei šis pranešimas neatnaujinamas, duomenų eksportuotojas žinos, kad duomenų importuotojas galėjo gauti tokį nurodymą.

117. Veiksmingumo sąlygos

- Trečiosios valstybės teisės aktuose duomenų importuotojui turi būti leidžiama pateikti duomenų eksportuotojui pasyvų pranešimą.
- Duomenų eksportuotojas privalo automatiškai stebėti „Warrant Canary“ tipo pranešimus.
- Duomenų importuotojas turi užtikrinti, kad jo privatus raktas, naudojamas pasirašant „Warrant Canary“ tipo pranešimą, būtų laikomas saugiai ir kad pagal trečiosios valstybės teisės aktus jis negalėtų būti verčiamas teikti netikrus „Warrant Canary“ tipo pranešimus. Šiuo tikslu galėtų būti naudinga nustatyti reikalavimą, kad „Warrant Canary“ tipo pranešimą pasirašytų keli skirtingi asmenys arba kad jį pateiktų asmuo, nepatenkantis į trečiosios valstybės jurisdikciją.

Įpareigojimai imtis konkrečių veiksmų

118. Duomenų importuotojas galėtų įsipareigoti pagal paskirties valstybės teisę įvertinti bet kokio nurodymo atskleisti duomenis teisėtumą, visų pirma, ar jis atitinka prašančiajai valdžios institucijai suteiktus įgaliojimus, ir užginčyti nurodymą, jei, atidžiai įvertinęs, jis padaro išvadą, kad pagal paskirties valstybės teisę yra pagrindo tai daryti. Užginčydamas nurodymą, duomenų importuotojas turėtų kreiptis dėl laikinųjų apsaugos priemonių, kad nurodymo galiojimas būtų sustabdytas, kol teismas priims sprendimą iš esmės. Duomenų importuotojas būtų įpareigotas neatskleisti prašomų asmens duomenų tol, kol to nebus reikalaujama pagal taikomas procedūrines taisykles. Duomenų importuotojas taip pat įsipareigotų, pagrįstai įvertinęs nurodymą, atsakyti į jį pateikiant mažiausią galimą informacijos kiekį.

119. Veiksmingumo sąlygos

- Trečiosios valstybės teisės sistemoje turi būti numatyti veiksmingi teisiniai būdai užginčyti nurodymus atskleisti duomenis.
- Ši sąlyga visada suteikia labai ribotą papildomą apsaugą, nes nurodymas atskleisti duomenis gali būti teisėtas pagal trečiosios valstybės teisinę sistemą, tačiau ši teisinė sistema gali neatitikti ES standartų. Ši sutartinė priemonė visada bus skirta kitoms papildomoms priemonėms papildyti.
- Nurodymų užginčijimas turi turėti stabdomąjį poveikį pagal trečiosios valstybės įstatymus. Priešingu atveju valdžios institucijos vis tiek turėtų prieigą prie asmens duomenų, o bet kokie tolesni veiksmai asmens naudai turėtų ribotą poveikį – leistų jam reikalauti atlyginti žalą dėl neigiamų pasekmių, atsirandančių dėl duomenų atskleidimo.
- Duomenų importuotojas turi sugebėti dokumentais pagrįsti ir įrodyti duomenų eksportuotojui veiksmus, kurių ėmėsi dėdamas visas pastangas, kad įvykdytų šį įsipareigojimą.

***

120. Tokiu pačiu atveju, kaip aprašyta pirmiau, duomenų importuotojas galėtų įsipareigoti informuoti prašančiąją valdžios instituciją apie nurodymo nesuderinamumą su BDAR 46 straipsnyje nurodytos perdavimo priemonės apsaugos priemonėmis[100] ir dėl to kylantį duomenų importuotojo įsipareigojimų konfliktą. Duomenų importuotojas tuo pat metu ir kuo greičiau informuotų duomenų eksportuotoją ir (arba) kompetentingą priežiūros instituciją EEE, jei tai įmanoma pagal trečiosios valstybės teisinę sistemą.

121. Veiksmingumo sąlygos

- Tokia informacija apie ES teisės suteiktą apsaugą ir pareigų konfliktą turėtų turėti tam tikrų teisinių pasekmių trečiosios valstybės teisės sistemoje, kaip antai teismo ar administracinė nurodymo ar prašymo suteikti prieigą peržiūra, reikalavimas pateikti teismo orderį ir (arba) laikinas nurodymo sustabdymas siekiant sustiprinti duomenų apsaugą.
- Valstybės teisinė sistema neturi trukdyti duomenų importuotojui pranešti duomenų eksportuotojui arba bent kompetentingai EEE priežiūros institucijai apie gautą nurodymą ar prašymą suteikti prieigą.
- Duomenų importuotojas turi sugebėti dokumentais pagrįsti ir įrodyti duomenų eksportuotojui veiksmus, kurių ėmėsi dėdamas visas pastangas, kad įvykdytų šį įsipareigojimą.

Galimybės duomenų subjektams įgyvendinti savo teises sudarymas

122. Sutartyje galėtų būti numatyta, kad su asmens duomenimis, perduotais paprastu tekstu vykdant įprastinę verslo veiklą (įskaitant pagalbos atvejus), galima susipažinti tik gavus aiškų arba numanomą duomenų eksportuotojo ir (arba) duomenų subjekto sutikimą dėl konkrečios prieigos prie duomenų.

123. Veiksmingumo sąlygos

- Ši sąlyga galėtų būti veiksminga tais atvejais, kai duomenų importuotojai gauna valdžios institucijų prašymus bendradarbiauti savanoriškai, o ne, pvz., kai valdžios institucijos turi prieigą prie duomenų be duomenų importuotojo žinios arba prieš jo valią.
- Kai kuriais atvejais duomenų subjektas gali neturėti galimybės prieštarauti prieigai arba duoti sutikimą, atitinkantį visas ES teisėje nustatytas sąlygas (suteikiamas laisva valia, konkretus, informacija pagrįstas ir vienareikšmis) (pvz., darbuotojų atveju)[101].
- Nacionalinės teisės aktai ar politika, įpareigojantys duomenų importuotoją neatskleisti nurodymo suteikti prieigą, gali padaryti šią sąlygą neveiksmingą, nebent ji gali būti paremta techniniais metodais, reikalaujančiais duomenų eksportuotojo ar duomenų subjekto įsikišimo, kad būtų prieinami paprastame tekste esantys duomenys. Tokios techninės priemonės prieigai

[100] Pavyzdžiui, SSS numatyta, kad duomenys buvo ir bus tvarkomi, įskaitant jų perdavimą, laikantis „*taikytinos duomenų apsaugos teisės*“. Taikytina duomenų apsaugos teisė apibrėžiama kaip „*teisės aktai, ginantys pagrindines asmenų teises ir laisves (ypač jų teisę į privatų gyvenimą) tvarkant asmens duomenis, kurių turi laikytis duomenų valdytojas toje valstybėje narėje, kurioje įsikūręs duomenų eksportuotojas*“. ESTT patvirtina, kad BDAR nuostatos, aiškinamos atsižvelgiant į ES pagrindinių teisių chartiją, yra minėtos teisės dalis, žr. ESTT sprendimo byloje C-311/18 (*Schrems II*) 138 punktą.

[101] BDAR 4 straipsnio 11 dalis.

apriboti gali būti numatytos visų pirma tuo atveju, jei prieiga suteikiama tik konkrečiais pagalbos ar paslaugų teikimo atvejais, tačiau patys duomenys saugomi EEE.

***

124. Sutartimi duomenų importuotojas ir (arba) duomenų eksportuotojas galėtų būti įpareigoti nedelsiant pranešti duomenų subjektui apie iš trečiosios valstybės valdžios institucijų gautą prašymą ar nurodymą arba apie duomenų importuotojo nesugebėjimą vykdyti savo sutartinių įsipareigojimų, kad duomenų subjektas galėtų ieškoti informacijos ir veiksmingai ginti savo teises (pvz., pateikti reikalavimą savo kompetentingai priežiūros institucijai ir (arba) teisminei institucijai ir įrodyti savo teisę kreiptis į trečiosios valstybės teismus), įskaitant kompensaciją iš duomenų importuotojo už bet kokią turtinę ir neturtinę žalą, patirtą dėl jo asmens duomenų, perduotų pagal pasirinktą duomenų perdavimo priemonę, atskleidimo pažeidžiant joje numatytus įsipareigojimus.

125. Veiksmingumo sąlygos

- Šis pranešimas galėtų įspėti duomenų subjektą apie galimą trečiųjų valstybių valdžios institucijų prieigą prie jo duomenų. Tokiu būdų duomenų subjektas galėtų gauti papildomos informacijos iš duomenų eksportuotojų ir pateikti reikalavimą savo kompetentingai priežiūros institucijai. Šia sąlyga taip pat būtų galima išspręsti ir kompensuoti kai kuriuos sunkumus, su kuriais asmuo gali susidurti įrodydamas savo teisę kreiptis į trečiųjų valstybių teismus (*locus standi*), kad užginčytų valdžios institucijų prieigą prie jo duomenų.
- Nacionalinės teisės aktai ir politika gali užkirsti kelią tokiam duomenų subjekto informavimui. Nepaisant to, duomenų eksportuotojas ir duomenų importuotojas galėtų įsipareigoti informuoti duomenų subjektą, kai tik bus panaikinti duomenų atskleidimo apribojimai, ir dėti visas pastangas, kad būtų panaikintas draudimas atskleisti duomenis. Duomenų eksportuotojas arba kompetentinga priežiūros institucija galėtų pranešti duomenų subjektui bent apie jo asmens duomenų perdavimo sustabdymą arba nutraukimą dėl to, kad duomenų importuotojas, gavęs prašymą dėl prieigos prie duomenų, negalėjo įvykdyti savo sutartinių įsipareigojimų.

***

126. Sutartimi duomenų eksportuotojas ir duomenų importuotojas galėtų būti įpareigoti padėti duomenų subjektui naudotis savo teisėmis trečiosios valstybės jurisdikcijoje taikant ad hoc teisių gynimo mechanizmus ir teikiant teisines konsultacijas.

127. Veiksmingumo sąlygos

- Kai kuriais nacionalinės teisės aktais duomenų importuotojui gali būti neleidžiama teikti tokios rūšies pagalbos tiesiogiai duomenų subjektams, nors pagal juos duomenų importuotojui gali būti leidžiama gauti šią pagalbą duomenų subjektams.
- Nacionalinės teisės aktuose ir politikoje gali būti nustatytos sąlygos, galinčios sumažinti numatytų *ad hoc* teisių gynimo mechanizmų veiksmingumą.
- Teisinės konsultacijos galėtų būti naudingos duomenų subjektui, ypač atsižvelgiant į tai, kaip sudėtinga ir brangu gali būti duomenų subjektui suprasti trečiosios valstybės teisinę sistemą ir imtis teisinių veiksmų iš užsienio, galbūt užsienio kalba. Tačiau ši sąlyga visada suteiks ribotą papildomą apsaugą, nes pagalbos ir teisinių konsultacijų teikimas duomenų subjektams pats

savaime negali ištaisyti padėties, kai trečiosios valstybės teisės sistema neužtikrina apsaugos lygio, iš esmės lygiaverčio EEE garantuojamam lygiui. Ši sutartinė priemonė visada bus skirta kitoms papildomoms priemonėms papildyti.

- Ši papildoma priemonė būtų veiksminga tik tuo atveju, jei trečiosios valstybės teisėje būtų numatyta teisių gynimo jos nacionaliniuose teismuose galimybė arba egzistuotų *ad hoc* teisių gynimo mechanizmas, be kita ko, dėl priežiūros priemonių.

2.3. Organizacinės priemonės

128. Papildomos organizacinės priemonės gali būti vidaus politika, organizaciniai metodai ir standartai kuriuos duomenų valdytojai ir duomenų tvarkytojai galėtų taikyti sau ir duomenų importuotojams trečiosiose valstybėse. Jos gali padėti užtikrinti asmens duomenų apsaugos nuoseklumą per visą tvarkymo ciklą. Organizacinės priemonės taip pat gali pagerinti duomenų eksportuotojų informuotumą apie riziką ir bandymus gauti prieigą prie duomenų trečiosiose valstybėse bei jų gebėjimą į juos reaguoti. Vienos ar keleto iš šių priemonių pasirinkimas nereiškia, kad bus tikrai ir sistemingai užtikrinta jūsų vykdomo perdavimo atitiktis esminio lygiavertiškumo standartui pagal ES teisę. Atsižvelgiant į konkrečias perdavimo aplinkybes ir atliktą trečiosios valstybės teisės aktų vertinimą, reikia imtis organizacinių priemonių, papildančių sutartines ir (arba) techninės priemones, kad būtų užtikrintas asmens duomenų apsaugos lygis, iš esmės lygiavertis EEE garantuojamam lygiui.

129. Tinkamiausios priemonės kiekvienu konkrečiu atveju turi būti vertinamos atsižvelgiant į tai, kad duomenų valdytojai ir duomenų tvarkytojai turi laikytis atskaitomybės principo. Toliau EDAV pateikia keletą organizacinių priemonių, kurias duomenų eksportuotojai gali įgyvendinti, pavyzdžių, tačiau šis sąrašas nėra išsamus, gali būti tinkamos ir kitos priemonės:

Perdavimų valdymo vidaus politika, ypač įmonių grupių atveju

130. Priimti tinkamą vidaus politiką, aiškiai paskirstant atsakomybę už duomenų perdavimą, ataskaitų teikimo kanalus ir standartines veiklos procedūras tais atvejais, kai valdžios institucijos pateikia oficialius arba neoficialius prašymus susipažinti su duomenimis. Ypač tais atvejais, kai duomenys perduodami tarp įmonių grupių, ši politika gali apimti, be kita ko, specialios grupės, kurią sudarytų IT, duomenų apsaugos ir privatumą reglamentuojančių teisės aktų ekspertai, suformavimą prašymams, susijusiems su iš EEE perduotais asmens duomenimis, nagrinėti; pranešimą vyresniesiems teisės reikalų ir įmonės vadovams bei duomenų eksportuotojui gavus tokius prašymus; procedūrinius veiksmus, siekiant užginčyti neproporcingus ar neteisėtus prašymus, ir skaidrios informacijos teikimą duomenų subjektams.

131. Parengti specialias personalo, atsakingo už valdžios institucijų prašymų susipažinti su asmens duomenimis tvarkymą, mokymo procedūras, kurios turėtų būti periodiškai atnaujinamos, kad atspindėtų naujus teisės aktų ir teismų praktikos pokyčius trečiojoje valstybėje ir EEE. Į mokymo procedūras turėtų būti įtraukti ES teisės aktų reikalavimai dėl valdžios institucijų galimybės susipažinti su asmens duomenimis, visų pirma remiantis Pagrindinių teisių chartijos 52 straipsnio 1 dalimi. Personalo informuotumas turėtų būti didinamas visų pirma vertinant praktinius valdžios institucijų prašymų susipažinti su duomenimis pavyzdžius ir tokiems praktiniams pavyzdžiams taikant Pagrindinių teisių chartijos 52 straipsnio 1 dalimi pagrįstą standartą. Tokiuose mokymuose turėtų būti atsižvelgiama į konkrečią duomenų importuotojo padėtį, pvz., trečiosios valstybės teisės aktus ir reglamentus, taikomus duomenų importuotojui, ir, jei įmanoma, jie turėtų būti rengiami bendradarbiaujant su duomenų eksportuotoju.

132. Veiksmingumo sąlygos

- Tokia politika gali būti numatyta tik tais atvejais, kai trečiosios valstybės valdžios institucijų prašymas suderinamas su ES teise[102]. Jei prašymas nesuderinamas, šios politikos nepakaktų lygiaverčiam asmens duomenų apsaugos lygiui užtikrinti ir, kaip minėta pirmiau, duomenų perdavimas turi būti sustabdytas arba reikia imtis atitinkamų papildomų priemonių, kad būtų užkirstas kelias prieigai.

Skaidrumo ir atskaitomybės priemonės

133. Dokumentuoti ir registruoti iš valdžios institucijų gautus prašymus leisti susipažinti su dokumentais ir pateiktus atsakymus, taip pat nurodyti teisinį pagrindą ir susijusius subjektus (pvz., ar pranešta duomenų eksportuotojui ir koks jo atsakymas, grupės, atsakingos už tokių prašymų nagrinėjimą, vertinimas ir t. t.). Šie įrašai turėtų būti prieinami duomenų eksportuotojui, kuris, savo ruožtu, turėtų juos pateikti atitinkamiems duomenų subjektams.

134. Veiksmingumo sąlygos

- Trečiosios valstybės nacionalinės teisės aktais gali būti uždrausta atskleisti prašymus ar jų esminę informaciją, todėl ši praktika gali tapti neveiksminga. Duomenų importuotojas turėtų informuoti duomenų eksportuotoją, jei negali pateikti tokių dokumentų ir įrašų, taip suteikdamas duomenų eksportuotojui galimybę sustabdyti perdavimą, jei dėl tokio negalėjimo nebūtų užtikrintas tinkamas apsaugos lygis.

***

135. Reguliariai skelbti skaidrumo ataskaitas arba santraukas dėl vyriausybės prašymų leisti susipažinti su duomenimis ir jai pateikto atsakymo, jei tai leistina pagal valstybės įstatymus.

136. Veiksmingumo sąlygos

- Pateikta informacija turėtų būti aktuali, aiški ir kuo išsamesnė. Trečiosios valstybės nacionalinės teisės aktais gali būti uždrausta atskleisti išsamią informaciją. Tokiais atvejais duomenų importuotojas turėtų dėti visas pastangas, kad paskelbtų statistinę informaciją ar panašaus tipo suvestinę informaciją.

Organizavimo metodai ir duomenų kiekio mažinimo priemonės

137. Duomenų perdavimo kontekste naudingos priemonės gali būti jau galiojantys organizaciniai reikalavimai pagal atskaitomybės principą, pavyzdžiui, patvirtinta griežta ir detali prieigos prie duomenų ir konfidencialumo politika bei geriausia praktika, griežtai remiantis būtinumo žinoti principu, kurios būtų stebimos reguliariai atliekant auditą ir įgyvendinamos pasitelkiant drausmines priemones. Šiuo atžvilgiu turi būti įvertinta duomenų kiekio mažinimo galimybė, siekiant apsaugoti asmens duomenis nuo neteisėtos prieigos. Pavyzdžiui, kai kuriais atvejais tam tikrų duomenų perduoti nebūtina (pvz., nuotolinės prieigos prie EEE duomenų atveju, kaip antai

[102] Žr. sprendimo byloje C-362/14 (*Schrems I*) 94 punktą ir sprendimo byloje C-311/18 (*Schrems II*) 168, 174, 175, 176 punktus.

pagalbos atvejais, kai vietoj visiškos prieigos suteikiama ribota prieiga arba kai teikiant paslaugą reikia perduoti tik ribotą duomenų rinkinį, o ne visą duomenų bazę).

138. Veiksmingumo sąlygos

- Turėtų būti numatyti reguliarus auditas ir griežtos drausminės priemonės, siekiant stebėti ir užtikrinti atitiktį duomenų kiekio mažinimo priemonėms, taip pat ir duomenų perdavimo kontekste.
- Prieš perdavimą duomenų eksportuotojas įvertina turimus asmens duomenis, kad nustatytų tuos duomenų rinkinius, kurių nebūtina perduoti ir todėl jie nebus pateikti duomenų importuotojui.
- Kartu su duomenų kiekio mažinimo priemonėmis turėtų būti taikomos techninės priemonės, siekiant užkirsti kelią neteisėtai prieigai prie duomenų. Pavyzdžiui, saugių daugiašalių skaičiavimo mechanizmų įdiegimas ir šifruotų duomenų rinkinių platinimas tarp įvairių patikimų subjektų gali užtikrinti pagal pritaikytosios apsaugos principą, kad dėl vienašalės prieigos nebūtų atskleisti identifikuojami duomenys.

***

139. Plėtoti gerąją patirtį siekiant tinkamai ir laiku įtraukti duomenų apsaugos pareigūną, jei toks yra, ir suteikti jam prieigą prie informacijos, taip pat prie teisinių ir vidaus audito paslaugų su tarptautiniu asmens duomenų perdavimu susijusiais klausimais.

140. Veiksmingumo sąlygos

- Duomenų apsaugos pareigūnui, jei toks yra, ir teisės ir vidaus audito grupei visa svarbi informacija pateikiama prieš perdavimą ir su jais konsultuojamasi dėl perdavimo būtinumo ir papildomų apsaugos priemonių, jei tokių yra.
- Atitinkama informacija turėtų apimti, pavyzdžiui, konkrečių asmens duomenų perdavimo būtinumo vertinimą, taikytinų trečiosios valstybės teisės aktų apžvalgą ir apsaugos priemones, kurias duomenų importuotojas įsipareigojo įgyvendinti.

Standartų ir geriausios praktikos patvirtinimas

141. Patvirtinti griežtą duomenų saugumo ir duomenų privatumo politiką, pagrįstą ES sertifikavimu ar elgesio kodeksais arba tarptautiniais standartais (pvz., ISO normomis) ir geriausia praktika (pvz., ENISA), deramai atsižvelgiant į naujausius technikos laimėjimus, taip pat į tvarkomų duomenų kategorijų riziką.

Kita

142. Priimti ir reguliariai peržiūrėti vidaus politiką, siekiant įvertinti įgyvendintų papildomų priemonių tinkamumą ir prireikus nustatyti bei įgyvendinti papildomus arba alternatyvius sprendimus, kad būtų išlaikytas apsaugos lygis, iš esmės lygiavertis EEE garantuojamam perduodamų asmens duomenų apsaugos lygiui.

***

143. Duomenų importuotojo įsipareigojimas toliau neperduoti asmens duomenų toje pačioje ar kitose trečiosiose valstybėse arba sustabdyti vykdomą perdavimą, kai trečiojoje valstybėje negalima užtikrinti asmens duomenų apsaugos lygio, iš esmės lygiaverčio EEE užtikrinamam lygiui[103].

[103] Sprendimo byloje C-311/18 (*Schrems II*) 135 ir 137 punktai.

3 PRIEDAS. GALIMI INFORMACIJOS ŠALTINIAI TREČIAJAI VALSTYBEI ĮVERTINTI

144. Jūsų duomenų importuotojas turi turėti galimybę pateikti jums atitinkamus šaltinius ir informaciją, susijusią su trečiąja valstybe, kurioje jis yra įsisteigęs, įskaitant duomenų importuotojui ir perduodamiems duomenims taikytinus teisės aktus ir praktiką. Jūs ir duomenų importuotojas galite remtis keliais informacijos šaltiniais, pavyzdžiui, šiame neišsamiame sąraše išvardytais ir pirmumo tvarka pateiktais šaltiniai:

- Europos Sąjungos Teisingumo Teismo (ESTT) ir Europos Žmogaus Teisių Teismo (EŽTT) praktika[104], nurodyta rekomendacijose dėl Europos pagrindinių garantijų[105];
- sprendimai dėl tinkamumo paskirties valstybėje, jei perdavimas grindžiamas kitu teisiniu pagrindu[106];
- tarpvyriausybinių organizacijų, pvz., Europos Tarybos[107], kitų regioninių institucijų ir JT organų bei agentūrų[108] (pvz., JT Žmogaus teisių tarybos[109], Žmogaus teisių komiteto[110]) rezoliucijos ir ataskaitos;
- kompetentingų reguliavimo tinklų, pavyzdžiui, Visuotinės privatumo asamblėjos (GPA), ataskaitos ir analizė[111];
- nacionalinė teismų praktika arba nepriklausomų teisminių ar administracinių institucijų, kompetentingų duomenų privatumo ir trečiųjų valstybių duomenų apsaugos klausimais, priimti sprendimai;
- nepriklausomų priežiūros ar parlamentinių įstaigų ataskaitos;
- ataskaitos, pagrįstos praktine patirtimi, susijusia su ankstesniais atvejais, kai valdžios institucijos pateikė prašymus atskleisti informaciją arba tokių prašymų nėra, iš subjektų, veikiančių tame pačiame sektoriuje kaip duomenų importuotojas;
- kitų subjektų, tvarkančių duomenis toje pačioje srityje kaip duomenų importuotojas, „Warrant canaries“;

---

[104] Žr. informacijos suvestinę dėl EŽTT praktikos masinio stebėjimo klausimais, https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[105] 2020 m. lapkričio 10 d. EDAV rekomendacijos Nr. 02/2020 dėl Europos pagrindinių garantijų taikant stebėjimo priemones, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en

[106] Sprendimo byloje C-311/18 (*Schrems II*) 141 punktas; žr. sprendimus dėl tinkamumo, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[107] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[108] Žr., pavyzdžiui, Amerikos šalių žmogaus teisių komisijos (IACHR) valstybių ataskaitas, https://www.oas.org/en/iachr/reports/country.asp.

[109] Žr. https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx

[110] Žr. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5

[111] Žr., pavyzdžiui, https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

- prekybos rūmų, verslo, profesinių ir prekybos asociacijų, duomenų eksportuotojo arba kitų trečiųjų valstybių, eksportuojančių į trečiąją valstybę, į kurią vykdomas perdavimas, vyriausybinių diplomatinių, prekybos ir investicijų agentūrų parengtos arba užsakytos ataskaitos;
- akademinių institucijų ir pilietinės visuomenės organizacijų (pvz., NVO) ataskaitos;
- privačių verslo informacijos teikėjų ataskaitos apie finansinę, reguliavimo ir įmonių reputacijos riziką;
- paties duomenų importuotojo „Warrant canaries“[112];
- skaidrumo ataskaitos, su sąlyga, kad jose aiškiai nurodyta, jog nebuvo gauta jokių prašymų leisti susipažinti su dokumentais. Skaidrumo ataskaitos, kuriose nieko nepasakyta šiuo klausimu, nebūtų laikomos pakankamais įrodymais, nes šiose ataskaitose daugiausia dėmesio skiriama iš teisėsaugos institucijų gautiems prieigos prašymams ir pateikiami duomenys tik apie šį aspektą, tačiau nekalbama apie gautus prašymus suteikti prieigą nacionalinio saugumo tikslais. Tai nereiškia, kad nebuvo gauta prašymų suteikti prieigą, o tai reiškia, kad šia informacija negalima dalytis[113];
- duomenų importuotojo vidaus pareiškimai arba įrašai, kuriuose aiškiai nurodyta, kad pakankamai ilgą laiką negauta jokių prašymų leisti susipažinti su dokumentais, pirmenybę teikiant pareiškimams ir įrašams, už kuriuos atsako duomenų importuotojas, ir (arba) pateiktiems vidaus pareigybes užimančių asmenų, turinčių tam tikrą autonomiją, pavyzdžiui, vidaus auditorių, duomenų apsaugos pareigūnų ir t. t.[114]

[112] Žr. sąlygas, kuriomis atsižvelgiama į dokumentais įformintą praktinę duomenų importuotojo patirtį, susijusią su atitinkamais ankstesniais atvejais, kai iš trečiosios valstybės valdžios institucijų buvo gauti prašymai suteikti prieigą, 47 punkte.
[113] *Ten pat.*
[114] *Ten pat.*