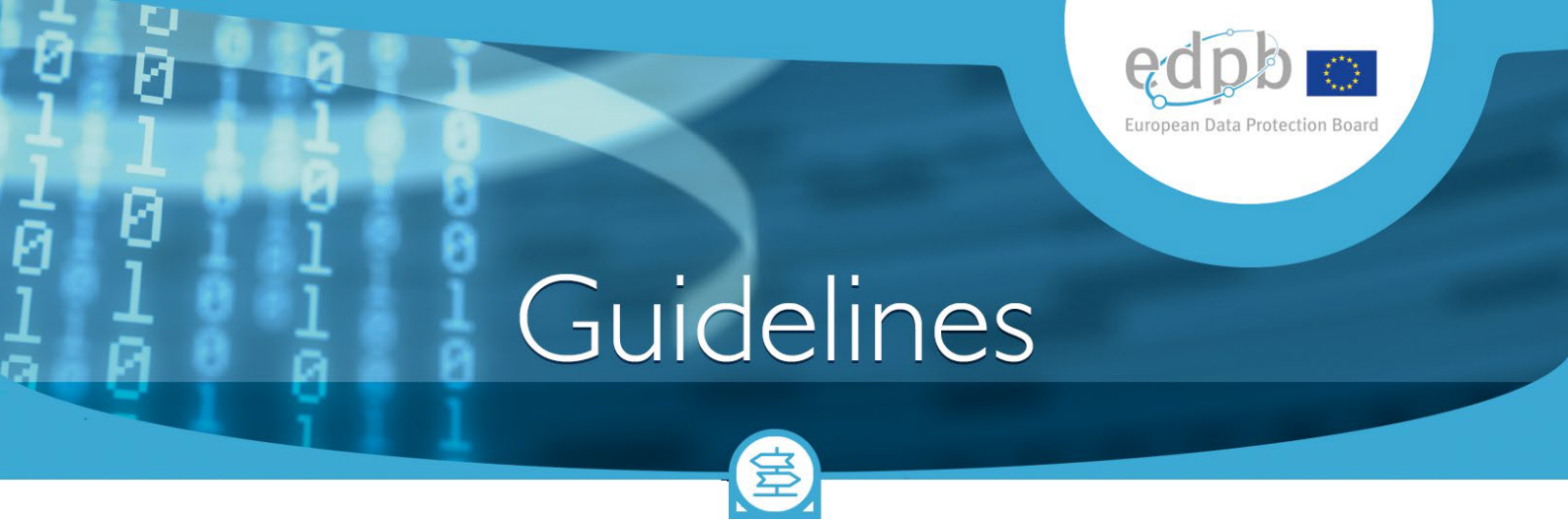


Gairės Nr. 07/2022 dėl sertifikavimo kaip duomenų perdavimo priemonės

2.0 versija

Priimta 2023 m. vasario 14 d.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

INFORMACIJA APIE VERSIJAS

1.0 versija	2022 m. birželio 14 d.	Gairių, dėl kurių rengiamasi skelbti viešas konsultacijas, priėmimas
2.0 versija	2023 m. vasario 14 d.	Gairių priėmimas po viešų konsultacijų

SANTRAUKA

BDAR 46 straipsnyje reikalaujama, kad duomenų eksportuotojai nustatytų tinkamas apsaugos priemones, taikytinas perduodant asmens duomenis į trečiąsias valstybes arba tarptautinėms organizacijoms. Tuo tikslu BDAR nurodytos įvairios tinkamos apsaugos priemonės, kurias pagal 46 straipsnį duomenų eksportuotojai gali taikyti ketindami perduoti duomenis į trečiąsias valstybes, be kita ko, nustatydami sertifikavimą kaip naują duomenų perdavimo mechanizmą (BDAR 42 straipsnio 2 dalis ir 46 straipsnio 2 dalies f punktas).

Šiose gairėse pateikiamos rekomendacijos dėl BDAR 46 straipsnio 2 dalies f punkto taikymo asmens duomenų perdavimui į trečiąsias valstybes arba tarptautinėms organizacijoms naudojant sertifikavimą. Šiame dokumente yra keturi skirsniai ir priedas.

Pirmoje šio dokumento dalyje („BENDROSIOS NUOSTATOS“) paaiškinama, kad gairėmis papildomos esamos Sertifikavimo bendrosios gairės Nr. 1/2018 ir aptariami konkretūs BDAR V skyriaus reikalavimai, kai sertifikavimas naudojamas kaip duomenų perdavimo priemonė. Pagal BDAR 44 straipsnį bet koks asmens duomenų perdavimas trečiosioms valstybėms arba tarptautinėms organizacijoms turi atitikti ne tik BDAR V skyriaus reikalavimus, bet ir kitų BDAR nuostatų sąlygas. Todėl pirmiausia turi būti užtikrintas bendrųjų BDAR nuostatų laikymasis, o antra, turi būti laikomasi BDAR V skyriaus nuostatų. Apibūdinami susiję subjektai ir jų pagrindiniai vaidmenys šioje srityje, ypatingą dėmesį skiriant duomenų importuotojo, kuriam bus suteiktas sertifikavimas, ir duomenų eksportuotojo, kuris naudosis juo kaip priemone jo vykdomam duomenų perdavimui, vaidmeniui (atsižvelgiant į tai, kad atsakomybė už duomenų tvarkymo reikalavimų laikymąsi ir toliau tenka duomenų eksportuotojui). Šiame kontekste sertifikavimas taip pat gali apimti priemones, kuriomis papildomos duomenų perdavimo priemonės, skirtos užtikrinti atitiktį ES asmens duomenų apsaugos lygiui. Pirmoje gairių dalyje taip pat pateikiama informacija apie sertifikavimo, kuris bus naudojamas kaip duomenų perdavimo priemonė, gavimo procesą.

Antroje šių gairių dalyje („AKREDITAVIMO REIKALAVIMŲ ĮGYVENDINIMO GAIRĖS“) primenama, kad sertifikavimo įstaigos akreditavimo reikalavimai nustatyti standarte ISO 17065, o BDAR 43 straipsnyje ir jo priede nurodytų sertifikavimo įstaigų akreditavimo gairės 4/2018 aiškinamos atsižvelgiant į V skyrių. Tačiau duomenų perdavimo atveju kai kurie sertifikavimo įstaigai taikytini akreditavimo reikalavimai šiose gairėse paaiškinami išsamiau.

Trečioje šių gairių dalyje („KONKRETŪS SERTIFIKAVIMO KRITERIJAI“) pateikiamos rekomendacijos dėl sertifikavimo kriterijų, jau išvardytų Gairėse Nr. 1/2018, ir nustatomi papildomi konkretūs kriterijai, kurie turėtų būti įtraukti į sertifikavimo mechanizmą, naudotiną kaip duomenų perdavimo trečiosioms valstybėms priemonė. Šie kriterijai apima trečiųjų valstybių teisės aktų vertinimą, bendrąsias duomenų eksportuotojų ir importuotojų pareigas, tolesnio duomenų perdavimo, teisių gynimo ir vykdymo užtikrinimo taisykles, procesą ir veiksmus, taikomus tais atvejais, kai nacionalinės teisės aktai ir praktika neleidžia laikytis įsipareigojimų, prisiimtų sertifikavimo procese, ir trečiųjų valstybių valdžios institucijų prašymus suteikti prieigą prie duomenų.

Šių gairių ketvirtoje dalyje („PRIVALOMI IR VYKDYTINI ĮSIPAREIGOJIMAI, KURIUOS REIKIA ĮGYVENDINTI“) pateikiami elementai, kurie turėtų būti įtraukti į privalomus ir vykdytinus įsipareigojimus, kuriuos turėtų prisiimti duomenų valdytojai arba duomenų tvarkytojai, kuriems netaikomas BDAR, kad būtų nustatytos tinkamos į trečiąsias valstybes perduodamų duomenų apsaugos priemonės. Šie įsipareigojimai, kurie gali būti nustatyti įvairiuose dokumentuose, įskaitant sutartis, visų pirma apima garantiją, kad duomenų importuotojas neturi pagrindo manyti, jog atitinkamam duomenų

tvarkymui taikomi trečiosios valstybės įstatymai ir praktika, įskaitant bet kokius reikalavimus atskleisti asmens duomenis arba priemones, kuriomis valdžios institucijoms leidžiama susipažinti su duomenimis, neleistų jam vykdyti sertifikavimo įsipareigojimų.

Šių gairių PRIEDE pateikiama keletas papildomų priemonių, atitinkančių Rekomendacijų Nr. 01/2020 (Rekomendacijos Nr. 01/2020 dėl priemonių duomenų perdavimo priemonėms papildyti, siekiant užtikrinti atitiktį ES asmens duomenų apsaugos lygiui) II priede išvardytas priemones, pavyzdžių, kai sertifikavimas naudojamas kaip duomenų perdavimo priemonė. Pavyzdžiai parinkti siekiant atkreipti dėmesį į kritines situacijas.

TURINYS

Informacija apie versijas **2**

SANTRAUKA **3**

1 BENDROSIOS NUOSTATOS **6**

1.1 Tikslas ir aprėptis 6

1.2 Tarptautiniam duomenų perdavimui taikomos bendrosios taisyklės 6

1.3 Kokie subjektai dalyvauja ir koks jų vaidmuo sertifikavimo kaip perdavimo priemonės procese? 8

1.4 Kokia yra sertifikavimo kaip duomenų perdavimo priemonės taikymo sritis ir objektas? 9

1.5 Koks turėtų būti eksportuotojo vaidmuo naudojant sertifikavimą kaip duomenų perdavimo priemonę? 9

1.6 Koks yra sertifikavimo kaip duomenų perdavimo priemonės procesas? 10

2 AKREDITAVIMO REIKALAVIMŲ GAIRIŲ ĮGYVENDINIMAS **12**

3 KONKRETŪS SERTIFIKAVIMO KRITERIJAI **12**

3.1 SERTIFIKAVIMO KRITERIJŲ GAIRIŲ ĮGYVENDINIMAS 12

3.2 PAPILDOMI KONKRETŪS SERTIFIKAVIMO KRITERIJAI 14

1. Trečiosios valstybės teisės aktų vertinimas 14

2. Duomenų eksportuotojų ir duomenų importuotojų bendrosios pareigos 14

3. Tolesnio duomenų perdavimo taisyklės 14

4. Teisių gynimas ir vykdymo užtikrinimas 15

5. Procesas ir veiksmai tais atvejais, kai nacionalinės teisės aktais užkertamas kelias laikytis įsipareigojimų, prisiimtų vykdant sertifikavimą 15

6. Trečiųjų valstybių institucijų prašymų susipažinti su duomenimis tvarkymas 15

7. Su duomenų eksportuotoju susijusios papildomos apsaugos priemonės 16

4 PRIVALOMI IR VYKDYTINI ĮSIPAREIGOJIMAI, KURIUOS REIKIA ĮGYVENDINTI **16**

PRIEDAS **19**

A. PAPILDOMŲ PRIEMONIŲ, KURIAS TURI ĮGYVENDINTI DUOMENŲ IMPORTUOTOJAS TUO ATVEJU, JEI Į SERTIFIKAVIMO TAIKYMO SRITĮ YRA ĮTRAUKTAS TRANZITAS, PAVYZDŽIAI 19

B. PAPILDOMŲ PRIEMONIŲ, TAIKOMŲ TUO ATVEJU, KAI TRANZITUI NETAIKOMAS SERTIFIKAVIMAS IR EKSPORTUOTOJAS TURI JAS UŽTIKRINTI, PAVYZDŽIAI 20

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 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 savo Darbo tvarkos taisyklių 12 ir 22 straipsnius,

PRIĖMĖ ŠIAS GAIRES:

1 BENDROSIOS NUOSTATOS

1.1 Tikslas ir aprėptis

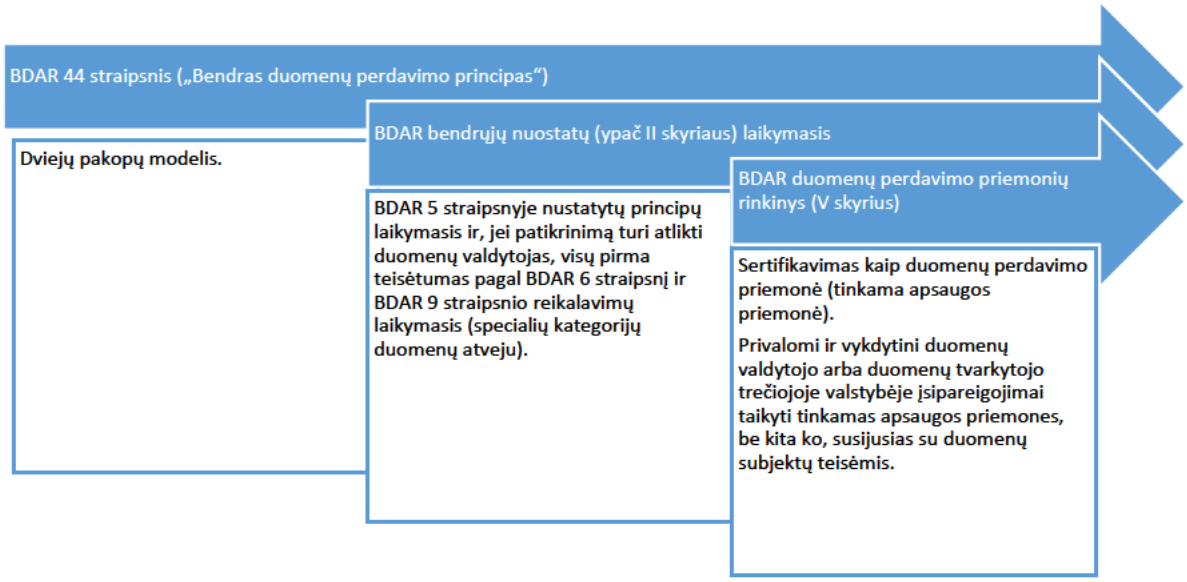
1. Šiuo dokumentu siekiama pateikti rekomendacijas dėl BDAR 46 straipsnio 2 dalies f punkto taikymo asmens duomenų perdavimui į trečiąsias valstybes arba tarptautinėms organizacijoms naudojant sertifikavimą. EDAV jau paskelbė bendrąsias gaires dėl sertifikavimo[2] ir akreditavimo[3] pagal BDAR. Todėl šiose naujose gairėse atsižvelgiama tik į konkrečius aspektus, susijusius su sertifikavimu kaip duomenų perdavimo priemone. Jose nurodoma, kaip taikomi BDAR 46 straipsnio 2 dalies f punktas ir 42 straipsnio 2 dalis, šiuo klausimu pateikiant praktinių rekomendacijų ir į jau paskelbtas gaires įtraukiant naujų elementų.

2. EDAV įvertins, kaip veikia šios gairės, atsižvelgdama į patirtį, įgytą jas taikant praktikoje, ir pateiks papildomų rekomendacijų, kad paaiškintų, kaip turėtų būti taikomi toliau išvardyti elementai, įskaitant sertifikavimo susitarimo vaidmenį, kiek tai susiję su BDAR 46 straipsnio 2 dalies f punkte nurodytais privalomais ir vykdytinais įsipareigojimais.

1.2 Tarptautiniam duomenų perdavimui taikomos bendrosios taisyklės

3. Pagal BDAR 44 straipsnį bet koks asmens duomenų perdavimas trečiosioms valstybėms[4] arba tarptautinėms organizacijoms turi atitikti ne tik BDAR V skyriaus reikalavimus, bet ir kitų BDAR nuostatų sąlygas. Taigi kiekvienas duomenų perdavimo veiksmas turi atitikti, *inter alia*, BDAR 5 straipsnyje nustatytus duomenų apsaugos principus, BDAR 6 straipsnyje nustatytus teisėtumo principus, o jei perduodami specialių kategorijų duomenys – BDAR 9 straipsnio nuostatas. Todėl turi būti taikomas dviejų pakopų kriterijus. Pirmiausia turi būti užtikrintas bendrųjų BDAR nuostatų laikymasis, o antra, turi būti laikomasi BDAR V skyriaus nuostatų.

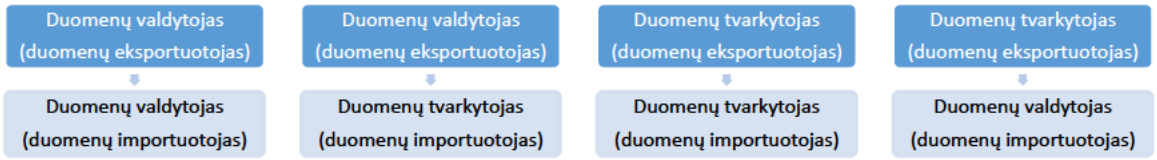
[1] Šiame dokumente daromos nuorodos į valstybes nares turėtų būti suprantamos kaip nuorodos į EEE valstybes nares.
[2] Sertifikavimo ir sertifikavimo kriterijų nustatymo pagal Reglamento (ES) 2016/679 42 ir 43 straipsnius gairės Nr. 1/2018.
[3] Bendrojo duomenų apsaugos reglamento (2016/679) 43 straipsnyje nurodytų sertifikavimo įstaigų akreditavimo gairės 4/2018.
[4] Gairės Nr. 05/2021 dėl BDAR 3 straipsnio ir nuostatų dėl tarptautinio duomenų perdavimo pagal BDAR V skyrių taikymo sąveikos, p. 4.



4. BDAR 46 straipsnyje nurodyta, kad „[j]eigu nėra priimtas sprendimas pagal 45 straipsnio 3 dalį, duomenų valdytojas arba duomenų tvarkytojas gali perduoti asmens duomenis į trečiąją valstybę arba tarptautinei organizacijai tik tuo atveju, jeigu duomenų valdytojas arba duomenų tvarkytojas yra nustatęs tinkamas apsaugos priemones, su sąlyga, kad suteikiama galimybė naudotis vykdytinomis duomenų subjektų teisėmis ir veiksmingomis duomenų subjektų teisių gynimo priemonėmis“. Pagal BDAR 46 straipsnio 2 dalies f punktą tokios tinkamos apsaugos priemonės gali būti nustatomos patvirtintu sertifikavimo mechanizmu kartu su privalomais ir vykdytinais duomenų valdytojo arba duomenų tvarkytojo trečiojoje valstybėje įsipareigojimais taikyti tinkamas apsaugos priemones, be kita ko, susijusias su duomenų subjektų teisėmis.

5. Todėl duomenų eksportuotojas gali nuspręsti remtis duomenų importuotojo gautu sertifikavimu kaip elementu, kuriuo įrodoma, jog jis vykdo savo pareigas, pvz., pagal BDAR 24 straipsnio 3 dalį arba 28 straipsnio 5 dalį. Duomenų importuotojas gali nuspręsti pateikti paraišką dėl sertifikavimo, kad įrodytų, jog taikomos tinkamos apsaugos priemonės.

6. Ir duomenų eksportuotojas, ir duomenų importuotojas gali atlikti skirtingus vaidmenis (pavyzdžiui, duomenų valdytojo arba duomenų tvarkytojo)[5], priklausomai nuo V skyriuje nurodyto duomenų tvarkymo, dėl kurio atsiranda skirtingos pareigos:



7. Be sertifikavimo ar kitų 45 ir 46 straipsniuose nurodytų duomenų perdavimo priemonių ar mechanizmų naudojimo, BDAR 49 straipsnyje nustatyta, kad tam tikrais konkrečiais atvejais tarptautinis duomenų

[5] Žr. toliau: SERTIFIKAVIMO KRITERIJŲ GAIRIŲ ĮGYVENDINIMAS.

perdavimas gali būti vykdomas, kai nesilaikoma jokio kito V skyriuje nustatyto mechanizmo[6]. Kita vertus, kaip paaiškinta ankstesnėse EDAV parengtose gairėse, BDAR 49 straipsnyje numatytos nukrypti leidžiančios nuostatos turi būti aiškinamos siaurai ir daugiausia susijusios su duomenų tvarkymo veikla, kuri yra nereguliari ir nepasikartojanti[7].

1.3 Kokie subjektai dalyvauja ir koks jų vaidmuo sertifikavimo kaip perdavimo priemonės procese?

8. Siekiant užtikrinti nuoseklumą, **Europos duomenų apsaugos valdyba (EDAV)** yra įgaliota patvirtinti EEE masto sertifikavimo kriterijus (Europos duomenų apsaugos ženklą) ir teikti nuomones dėl priežiūros institucijų sprendimų dėl sertifikavimo įstaigoms taikomų sertifikavimo kriterijų ir akreditavimo reikalavimų projektų. Ji taip pat yra kompetentinga įtraukti į registrą visus sertifikavimo mechanizmus ir duomenų apsaugos ženklus bei žymenis ir padaryti juos viešai prieinamus[8].

9. **Priežiūros institucijos** tvirtina sertifikavimo kriterijus, kai sertifikavimo mechanizmas nėra Europos duomenų apsaugos ženklas[9]. Jos taip pat gali akredituoti sertifikavimo įstaigą, parengti sertifikavimo kriterijus ir suteikti sertifikavimą, jei tai nustatyta jų valstybės narės nacionalinės teisės aktuose[10].

10. **Nacionalinė akreditavimo įstaiga** gali akredituoti trečiųjų šalių sertifikavimo įstaigas taikydama ISO 17065 ir priežiūros institucijų papildomus akreditavimo reikalavimus, kurie turėtų atitikti šių gairių 2 skirsnį. Kai kuriose valstybėse narėse akreditaciją gali suteikti ir kompetentinga priežiūros institucija, taip pat ją gali atlikti nacionalinė akreditavimo įstaiga arba abi šios institucijos.

11. **Schemos savininkas** – tai organizacija, kuri nustatė sertifikavimo kriterijus ir metodikos reikalavimus, pagal kuriuos bus vertinama atitiktis. Vertinimus gali atlikti ta pati organizacija, kuri sukūrė schemą ir kurios savininkė ji yra, tačiau gali būti ir tokia tvarka, pagal kurią schemos savininkė yra viena organizacija, o vertinimus kaip sertifikavimo įstaiga atlieka kita organizacija (arba kelios organizacijos).

12. Priklausomai nuo nacionalinės teisės, vietoj priežiūros institucijų, sertifikavimą gali suteikti **sertifikavimo įstaiga**, akredituota, kaip nurodyta pirmiau[11]. Ji gali parengti sertifikavimo kriterijus, taigi ir būti schemos savininkė (žr. 11 punktą). Ji turi būti įsisteigusi EEE, visų pirma tam, kad galėtų veiksmingai naudotis BDAR 58 straipsnio 2 dalies f punkte įtvirtintais įgaliojimais imtis taisomųjų veiksmų. Tačiau sertifikavimo įstaiga gali sudaryti subrangos sutartis su vietos ekspertais ar už EEE ribų esančiomis įstaigomis, kurie jos vardu atliks audito veiklą[12]. Nepaisant to, sertifikavimo įstaiga negali sudaryti subrangos sutarčių dėl sprendimo suteikti sertifikavimą arba jo nesuteikti.

13. **Duomenų importuotojas** yra trečiosios valstybės subjektas (duomenų valdytojas arba duomenų tvarkytojas), gaunantis duomenis iš duomenų eksportuotojo.

---

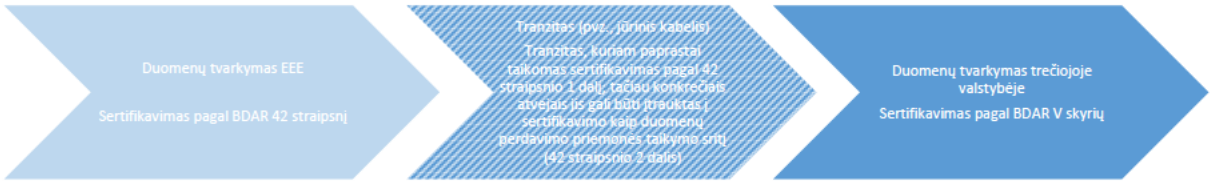
[6] Išsamesnė informacija apie 49 straipsnį ir jo sąveiką su 46 straipsniu apskritai pateikiama Gairėse Nr. 2/2018 dėl nukrypti leidžiančių nuostatų pagal Reglamento (ES) 2016/679 49 straipsnį.
[7] Gairių Nr. 2/2018 dėl nukrypti leidžiančių nuostatų pagal Reglamento (ES) 2016/679 49 straipsnį, p. 5.
[8] BDAR 42 straipsnio 8 dalis.
[9] Sertifikavimo ir sertifikavimo kriterijų nustatymo pagal Reglamento (ES) 2016/679 42 ir 43 straipsnius gairės Nr. 1/2018, 2.2 punktas.
[10] BDAR 42 straipsnio 5 dalis ir 43 straipsnio 1 dalis.
[11] BDAR 42 straipsnio 5 dalis.
[12] Sertifikavimo įstaigos turi įvertinti savo vietos ekspertus pagal ISO 17065 ir papildomus akreditavimo reikalavimus, kuriuos nustatė priežiūros institucija (BDAR 43 straipsnio 1 dalies b punktas).

14. **Duomenų eksportuotojas** yra subjektas (duomenų valdytojas arba duomenų tvarkytojas), perduodantis duomenis iš EEE duomenų importuotojui. Duomenų eksportuotojas turi užtikrinti, kad būtų laikomasi V skyriaus reikalavimų.

1.4 Kokia yra sertifikavimo kaip duomenų perdavimo priemonės taikymo sritis ir objektas?

15. Sertifikavimo mechanizmu kaip duomenų perdavimo priemone pagal 42 straipsnio 2 dalį turi būti siekiama užtikrinti tinkamas asmens duomenų tvarkymo pagal 46 straipsnio 2 dalies f punkto sąlygas apsaugos priemones. Sertifikavimu įrodoma, kad duomenų valdytojai arba duomenų tvarkytojai, kurie yra už EEE ribų arba kurie yra tarptautinė organizacija, gaunanti duomenis iš EEE duomenų valdytojų ar duomenų tvarkytojų, taiko tinkamas apsaugos priemones, kad būtų pašalinta konkreti su asmens duomenų perdavimu susijusi rizika.

16. Apskritai asmens duomenų perdavimo iš valstybės narės į trečiąją valstybę veiksmas savaime yra asmens duomenų tvarkymas, kaip tai suprantama pagal BDAR 4 straipsnio 2 punktą, atliekamas valstybėje narėje[13] ir todėl gali būti sertifikuojamas pagal BDAR 42 straipsnio 1 dalį. Tačiau kai kuriose situacijose, priklausomai nuo aplinkybių, į sertifikavimo kaip duomenų perdavimo priemonės taikymo sritį gali būti įtrauktas tranzitas. Todėl sertifikavimo objektas, kuris sertifikavimo metu sutampa su vertinimo objektu[14], paprastai turėtų būti duomenų, kuriuos iš EEE gavo duomenų importuotojas trečiojoje valstybėje, tvarkymas ir jų tranzitas, jei jį kontroliuoja importuotojas.



17. Sertifikavimo objektas gali būti viena duomenų tvarkymo operacija arba operacijų seka. Jos gali apimti valdymo procesus, t. y. organizacines priemones, kaip duomenų tvarkymo operacijos sudedamąsias dalis[15].

18. Todėl paraišką teikiantis subjektas jo sertifikavimo objekto atžvilgiu būtų duomenų importuotojas trečiojoje valstybėje.

1.5 Koks turėtų būti eksportuotojo vaidmuo naudojant sertifikavimą kaip duomenų perdavimo priemonę?

19. Duomenų eksportuotojo atliekamas duomenų perdavimas paprastai tiesiogiai patenka į BDAR taikymo sritį. Tai reiškia, kad duomenų eksportuotojas privalo laikytis savo pareigų pagal BDAR ir visų pirma užtikrinti, kad duomenys būtų perduodami saugiai pagal 32 straipsnį ir V skyrių, siekiant užtikrinti, kad

---

[13] Europos Sąjungos Teisingumo Teismo sprendimas *Data Protection Commissioner / Facebook Ireland Ltd ir Maximillian Schrems*, C-311/18, Nr. 83.
[14] Sertifikavimo ir sertifikavimo kriterijų nustatymo pagal Reglamento (ES) 2016/679 42 ir 43 straipsnius gairės Nr. 1/2018, p. 17.
[15] Sertifikavimo ir sertifikavimo kriterijų nustatymo pagal Reglamento (ES) 2016/679 42 ir 43 straipsnius gairės Nr. 1/2018, p. 16 (pvz., skundų nagrinėjimo mechanizmas).

nebūtų pakenkta tuo reglamentu garantuojamam fizinių asmenų apsaugos lygiui (BDAR 44 straipsnis)[16]. Žinoma, tai gali būti sertifikuojama pagal 42 straipsnio 1 dalį.

20. Be to, duomenų eksportuotojas, norintis naudoti sertifikavimą kaip tinkamą apsaugos priemonę pagal BDAR 46 straipsnio 2 dalies f punktą, visų pirma privalo patikrinti, ar sertifikavimas, kuriuo jis ketina remtis, yra veiksmingas atsižvelgiant į numatomo duomenų tvarkymo savybes. Tuo tikslu duomenų eksportuotojas turi patikrinti suteiktą sertifikavimą, kad patikrintų, ar sertifikatas galioja ir ar nėra pasibaigęs jo galiojimo laikas, ar jis apima konkretų vykdytiną duomenų perdavimą ir ar į sertifikavimo taikymo sritį yra įtrauktas asmens duomenų tranzitas, taip pat ar bus vykdomas tolesnis duomenų perdavimas ir ar pateikti atitinkami su juo susiję dokumentai. Be to, duomenų eksportuotojas turi patikrinti, ar sertifikavimą suteikianti sertifikavimo įstaiga yra akredituota nacionalinės akreditavimo įstaigos arba kompetentingos priežiūros institucijos. Be to, duomenų eksportuotojas turėtų nurodyti sertifikavimo kaip duomenų perdavimo priemonės naudojimą duomenų tvarkymo sutartyje pagal BDAR 28 straipsnį tais atvejais, kai duomenų valdytojas perduoda duomenis duomenų tvarkytojui, arba dalijimosi duomenimis sutartyje su duomenų importuotoju, kai vienas duomenų valdytojas perduoda duomenis kitam.

21. Atsižvelgiant į tai, kad duomenų eksportuotojas yra atsakingas už visų V skyriaus nuostatų taikymą, jis taip pat turi įvertinti, ar sertifikavimas, kuriuo jis ketina remtis kaip perdavimo priemone, yra veiksmingas atsižvelgiant į trečiojoje valstybėje galiojančius teisės aktus ir praktiką, kurie yra svarbūs atitinkamam duomenų perdavimui. Šiam vertinimui atlikti duomenų eksportuotojas, norėdamas įrodyti, kad laikosi savo atsakomybės, gali remtis sertifikavimo įstaigos atliekamu duomenų importuotojo dokumentais patvirtinto trečiosios valstybės įstatymų ir praktikos vertinimo patikrinimu.

22. Jeigu įvertinus duomenų importuotoją paaiškėja, kad jam ir (arba) duomenų eksportuotojui gali reikėti imtis papildomų sertifikavimo procese numatytų priemonių, kad būtų užtikrintas iš esmės lygiavertis apsaugos lygis, kaip numatytasis EEE, duomenų eksportuotojas privalo patikrinti papildomas priemones, kurias taiko sertifikavimą įgijęs duomenų importuotojas, ir ar jis gali atsakyti į technines ir (jei yra) papildomas priemones, kurių prašo duomenų importuotojas.

23. Jei šių nuostatų nesilaikoma, duomenų eksportuotojas turės reikalauti, kad duomenų importuotojas pats imtųsi pritaikytų papildomų priemonių arba jas nustatytų.

1.6 Koks yra sertifikavimo kaip duomenų perdavimo priemonės procesas?

24. Sertifikavimas yra savanoriškas, tačiau, kai prašoma, jis turi būti suteikiamas taikant skaidrų procesą, grindžiamą privalomomis taisyklėmis. Pagal BDAR labai pasitikima privačiais sertifikavimo mechanizmais kaip „reguliuojamu savireguliavimu“. Todėl tais mechanizmais turi būti užtikrinama, kad sertifikatai iš esmės atitiktų reikalavimus dėl tinkamų apsaugos priemonių, kaip apibrėžta BDAR 46 straipsnyje.

[16] Šiuo atžvilgiu svarbu pažymėti, kad BDAR 44 straipsnyje aiškiai numatyta, kad duomenis gali perduoti ne tik duomenų valdytojas, bet ir duomenų tvarkytojas. Todėl duomenų perdavimas įvyksta, kai duomenų valdytojo nurodymu duomenų tvarkytojas duomenis siunčia kitam duomenų tvarkytojui ar net duomenų valdytojui trečiojoje valstybėje (BDAR 28 straipsnio 3 dalies a punktas). Tokiais atvejais duomenų tvarkytojas veikia kaip duomenų eksportuotojas duomenų valdytojo vardu ir turi užtikrinti, kad pagal duomenų valdytojo nurodymus perduodant duomenis būtų laikomasi V skyriaus nuostatų, be kita ko, kad būtų naudojama tinkama duomenų perdavimo priemonė. Atsižvelgiant į tai, kad duomenų perdavimas yra duomenų tvarkymo veiksmas, vykdomas duomenų valdytojo vardu, duomenų valdytojas taip pat yra atsakingas ir jam gali tekti atsakomybė pagal V skyrių, jis taip pat turi užtikrinti, kad duomenų tvarkytojas pateiktų pakankamas garantijas pagal 28 straipsnį.

25. Todėl sertifikavimas turi būti grindžiamas sertifikavimo kriterijų vertinimu pagal privalomą audito metodiką. Tuos kriterijus patvirtins nacionalinės priežiūros institucijos arba EDAV, kaip aprašyta BDAR 42 straipsnio 5 dalyje. Sertifikavimo kriterijai apima duomenų importuotojo atliekamo duomenų tvarkymo, įskaitant tolesnį duomenų perdavimą, ir atitinkamos trečiosios valstybės teisinės sistemos vertinimo reikalavimus, siekiant užtikrinti, kad trečiosios valstybės taisyklės ir praktika netrukdytų duomenų importuotojui vykdyti su sertifikavimu susijusias pareigas.

26. Sertifikavimo proceso metu vertinimo objektą pagal sertifikavimo kriterijus tikrina nacionalinės akreditavimo įstaigos arba kompetentingos priežiūros institucijos akredituota sertifikavimo įstaiga[17].

27. Pagal BDAR 43 straipsnio 1 dalį sertifikavimo įstaigos, turinčios tinkamo lygio ekspertinių žinių duomenų apsaugos srityje, informavusios priežiūros instituciją, kad ji prireikus galėtų pasinaudoti savo įgaliojimais pagal BDAR 58 straipsnio 2 dalies h punktą, išduoda ir atnaujina sertifikatus.

28. Pagal BDAR 43 straipsnio 5 dalį sertifikavimo įstaigos kompetentingoms priežiūros institucijoms nurodo priežastis, kodėl prašomas sertifikavimas buvo suteiktas arba panaikintas. Tai nereiškia, kad sertifikavimo įstaiga turi gauti priežiūros institucijos leidimą, kad galėtų išduoti sertifikatą. Sertifikavimo įstaiga stebės, ar jos klientai laikosi sertifikavimo kriterijų.

29. Priežiūros institucija yra įgaliota imtis taisomųjų veiksmų – atšaukti sertifikatą arba nurodyti sertifikavimo įstaigai atšaukti pagal BDAR 42 ir 43 straipsnius išduotą sertifikatą, arba nurodyti sertifikavimo įstaigai neišduoti sertifikato, jei nevykdomi arba nebevykdomi sertifikavimo reikalavimai.

30. Europos duomenų apsaugos ženklas tarptautiniam duomenų perdavimui gali būti naudojamas kaip priemonė, kartu su privalomais ir vykdytinais įsipareigojimais apimanti duomenų perdavimą į trečiąsias valstybes[18].

31. Vis dėlto sertifikavimas, kuris turi būti naudojami kaip duomenų perdavimo priemonė, taip pat gali būti suteikiamas pagal patvirtintas EEE valstybių nacionalines sertifikavimo schemas. Todėl jis galioja tik tuo atveju, kai duomenis trečiosioms valstybėms perduoda EEE valstybės narės, kurioje patvirtinta sertifikavimo schema, duomenų eksportuotojai, nes skirtingų EEE valstybių sertifikatų tarpusavio pripažinimo nėra. Tačiau skirtingose EEE valstybėse veikiančios priežiūros institucijos gali patvirtinti tą patį duomenų perdavimo sertifikavimo mechanizmą[19].

---

[17] Bendrojo duomenų apsaugos reglamento (2016/679) 43 straipsnyje nurodytų sertifikavimo įstaigų akreditavimo gairės 4/2018, p. 9.

[18] Žr. BDAR 42 straipsnio 5 dalį ir EDAV sertifikavimo ir sertifikavimo kriterijų nustatymo pagal Reglamento 42 ir 43 straipsnius gairių Nr. 1/2018 35 punktą.

[19] Jei priežiūros institucija vadovauja X sertifikavimo kriterijaus priėmimui pagal savo nacionalinę iniciatyvą, o vėliau, atsižvelgdamos į schemos kriterijus ir taikytinus konkrečius nacionalinės teisės aktus, kitos valstybės nori priimti tuos pačius sertifikavimo kriterijus, jos gali juos priimti EDAV nepriimant nuomonės pagal BDAR 64 straipsnį ir remdamosi pirmajai priežiūros institucijai pateikta nuomone pagal BDAR 64 straipsnio 3 dalį (šiuo klausimu žr. nuorodą į gairių papildymą (Sertifikavimo ir sertifikavimo kriterijų nustatymo pagal Reglamento 42 ir 43 straipsnius gairių Nr. 1/2018 priedas), 66 punktas).

2 AKREDITAVIMO REIKALAVIMŲ GAIRIŲ ĮGYVENDINIMAS

32. Sertifikavimo įstaigos akreditavimo reikalavimai, susiję su sertifikavimu kaip duomenų perdavimo priemone, nustatyti standarte ISO 17065 ir aiškinant Gaires 4/201820 atsižvelgiant į V skyrių, kaip paaiškinta toliau.

33. EDAV nuomone, papildomi akreditavimo reikalavimai, parengti remiantis Gairėmis 4/2018 ir ISO 17065 ir priimti pagal BDAR 64 straipsnio 1 dalies c punktą, jau apima konkrečius sertifikavimo įstaigos akreditavimo reikalavimus, susijusius su sertifikavimu kaip duomenų perdavimo priemone. Tačiau perduodant duomenis kai kuriuos reikalavimus reikia šiek tiek patikslinti pateikiant aiškinamųjų pastabų ir paaiškinimų.

34. Kalbant apie reikalingus išteklius (žr. Gairių 4/2018 1 priedo 6 reikalavimą), sertifikavimo įstaiga užtikrina, kad ji turėtų išteklius, būtinus, kad galėtų patikrinti, ar duomenų importuotojas tinkamai ir teisingai atliko būtiną trečiosios (-iųjų) valstybės (-ių), kurioje (-iose) jis yra įsisteigęs arba vykdo veiklą, teisinės padėties ir praktikos vertinimą[21]. Šis vertinimas turėtų būti atliekamas atsižvelgiant į duomenų tvarkymo veiklą, kuri turi būti sertifikuojama kaip vertinimo objekto dalis, atsižvelgiant į tinkamas apsaugos priemones pagal BDAR 46 straipsnį, ir prireikus turėtų apimti duomenų importuotojo nustatytas ir įgyvendinamas papildomas priemones. Tai taip pat apima, pvz., svarbių vietos teisės aktų ir praktikos išmanymą ir tinkamus trečiosios (-iųjų) valstybės (-ių) kalbos (-ų) mokėjimo įgūdžius.

35. Kalbant apie procedūrinius reikalavimus (žr. Gairių 4/2018 1 priedo 7 reikalavimą), sertifikavimo įstaiga užtikrina, kad sertifikavimo procesas galėtų būti paremtas galimais auditais vietoje ir būtų susijęs su duomenų tvarkymu, kuris bus vykdomas trečiojoje (-iosiose) valstybėje (-ėse), ir kad vertinimas taip pat apimtų praktinį esamų trečiosios (-iųjų) valstybės (-ių) teisės aktų ir politikos įgyvendinimą.

36. Kalbant apie reikalavimus, susijusius su pakeitimais, turinčiais įtakos sertifikavimui (žr. Gairių 4/2018 1 priedo 7.10 reikalavimą), sertifikavimo įstaiga stebi trečiųjų valstybių teisės aktų ir (arba) jurisprudencijos pakeitimus, galinčius turėti įtakos duomenų tvarkymui, kuris yra vertinimo objekto dalis.

3 KONKRETŪS SERTIFIKAVIMO KRITERIJAI

37. Kalbant apie konkrečius sertifikavimo kriterijus, šios gairės grindžiamos Sertifikavimo ir sertifikavimo kriterijų nustatymo pagal Reglamento 42 ir 43 straipsnius gairėmis Nr. 1/2018 (3.0 versija), atitinkamu 2 priedu dėl sertifikavimo kriterijų peržiūros ir vertinimo pagal 42 straipsnio 5 dalį ir Sertifikavimo kriterijų vertinimo gairių papildymu.

38. EDAV nuomone, sertifikavimo kriterijai, parengti remiantis Gairių Nr. 1/2018 2 priedu ir Sertifikavimo kriterijų vertinimo gairių papildymu, jau apima daugumą sertifikavimo kriterijų, į kuriuos reikia atsižvelgti rengiant sertifikavimo schemą, kuri būtų naudojama kaip duomenų perdavimo priemonė. Tačiau kai kuriuos iš šių esamų kriterijų gali prireikti patikslinti, kad jie būtų pritaikyti konkrečiam duomenų perdavimo scenarijui (žr. 3.1 punktą). Be to, gali prireikti suformuluoti papildomus kriterijus, kad būtų galima taikyti tinkamas apsaugos priemones, be kita ko, susijusias su duomenų subjektų teisėmis (žr. 3.2 punktą).

3.1 SERTIFIKAVIMO KRITERIJŲ GAIRIŲ ĮGYVENDINIMAS

20 BDAR 43 straipsnyje ir priede nurodytų sertifikavimo įstaigų akreditavimo gairės 4/2018.
[21] Žr. 12 punktą.

39. Sertifikavimo mechanizmo taikymo sritis ir vertinimo objektas (žr. 2 priedo 2 skirsnio a punktą) turėtų būti aiškiai aprašyti atitinkamuose dokumentuose, be kita ko, kiek tai susiję su asmens duomenų perdavimu trečiajai valstybei, ar tai, ar ketinama įtraukti ir jų tranzitą.

40. Kalbant apie sertifikavimo mechanizmo taikymo sritį ir vertinimo objektą (žr. 2 priedo 2 skirsnio b punktą), atitinkamuose dokumentuose turėtų būti konkrečiai aprašyta, kokios rūšies subjektams (pvz., duomenų valdytojams ir (arba) duomenų tvarkytojams) taikomas sertifikavimo mechanizmas.

41. Kalbant apie sertifikavimo mechanizmo taikymo sritį ir vertinimo objektą (žr. 2 priedo 2 skirsnio f punktą), pagal kriterijus turėtų būti reikalaujama, kad vertinimo objektas būtų konkrečiai apibrėžtas, kad būtų išvengta nesusipratimų. Tai turėtų apimti bent:

42. duomenų tvarkymo operaciją (-as), įskaitant atvejus, kai numatomas tolesnis duomenų perdavimas:

    a) tikslą,

    b) subjekto rūšį (pvz., duomenų valdytojas ir (arba) duomenų tvarkytojas),

    c) perduodamų duomenų rūšį, atsižvelgiant į tai, ar įtraukiami specialių kategorijų asmens duomenys, kaip apibrėžta BDAR 9 straipsnyje,

    d) duomenų subjektų kategorijas,

    e) valstybes, kuriose tvarkomi duomenys.

43. Kalbant apie skaidrumą ir duomenų subjektų teises (žr. 2 priedo 8 skirsnį), pagal sertifikavimo kriterijus turėtų būti reikalaujama, kad:

    a) duomenų subjektams būtų teikiama informacija apie duomenų tvarkymo veiksmus, įskaitant, kai aktualu, apie asmens duomenų perdavimą trečiajai valstybei arba tarptautinei organizacijai (žr. BDAR 12, 13, 14 straipsnius);

    b) duomenų subjektams būtų garantuojamos teisės susipažinti su duomenimis, juos ištaisyti, ištrinti, apriboti, pranešti apie ištaisymą, ištrynimą ar apribojimą, nesutikti, kad duomenys būti tvarkomi arba būtų taikomi tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiami sprendimai, iš esmės lygiavertės numatytosioms BDAR 15–19, 21 ir 22 straipsniuose;
    c) sertifikatą turintis duomenų importuotojas nustatytų tinkamą skundų nagrinėjimo procedūrą, kad būtų užtikrintas veiksmingas duomenų subjekto teisių įgyvendinimas;
    d) būtų įvertinama, ar ir kokiu mastu šios duomenų subjektų teisės yra vykdytinos atitinkamoje trečiojoje valstybėje, ir bet kokios papildomos tinkamos priemonės, kurių gali prireikti siekiant užtikrinti jų vykdymą, pvz., reikalaujant, kad duomenų importuotojas sutiktų priklausyti duomenų eksportuotojo (-ų) kompetentingos priežiūros institucijos jurisdikcijai ir su ja bendradarbiautų vykdant procedūras, kuriomis siekiama užtikrinti, kad būtų laikomasi šių teisių, ir visų pirma, kad jis sutiktų atsakyti į užklausas, leisti atlikti auditą ir laikytis minėtos priežiūros institucijos priimtų priemonių, įskaitant taisomąsias ir kompensacines priemones.

44. Kalbant apie technines ir organizacines apsaugos priemones (2 priedo 10 skirsnio q punktas), pagal sertifikavimo kriterijus turėtų būti reikalaujama, kad duomenų importuotojas informuotų duomenų eksportuotoją ir, jei duomenų importuotojas veikia kaip duomenų valdytojas, informuotų už duomenų eksportuotoją (-us) atsakingą EEE esančią priežiūros instituciją apie duomenų saugumo pažeidimus ir apie juos praneštų duomenų subjektams, jei dėl pažeidimo gali kilti didelis pavojus jų teisėms ir laisvėms, laikantis BDAR 34 straipsnio reikalavimų.

3.2 PAPILDOMI KONKRETŪS SERTIFIKAVIMO KRITERIJAI

45. Atsižvelgdama į apsaugos priemones, nustatytas kitoms duomenų perdavimo priemonėms pagal BDAR 46 straipsnį (pvz., įmonėms privalomas taisykles arba elgesio kodeksus), ir siekdama užtikrinti nuoseklų apsaugos lygį, taip pat atsižvelgdama į ESTT sprendimą *Schrems II*, EDAV mano, kad sertifikavimo mechanizmas, naudotinas kaip duomenų perdavimo į trečiąsias valstybes priemonė, taip pat turėtų apimti toliau išvardytus kriterijus.

1. Trečiosios valstybės teisės aktų vertinimas

a) Ar pagal kriterijus reikalaujama, kad duomenų importuotojas būtų įvertinęs trečiosios valstybės, kurioje jis vykdo veiklą, taisykles bei praktiką ir ar jos trukdo duomenų importuotojui laikytis su sertifikavimu susijusių savo įsipareigojimų?

b) Ar pagal kriterijus reikalaujama, kad duomenų importuotojas trečiosios valstybės, kurioje jis vykdo veiklą, taisyklių ir praktikos vertinimą dokumentuotų ir galėtų tuos dokumentus suteikti sertifikavimo įstaigai ir paprašius EEE esančiai priežiūros institucijai, kurios kompetencijai priklauso duomenų eksportuotojas, ir duomenų eksportuotojui?

c) Ar pagal kriterijus reikalaujama, kad duomenų importuotojas būtų nustatęs ir įgyvendinęs organizacines ir technines priemones, kad užtikrintų tinkamas apsaugos priemones pagal BDAR 46 straipsnį, atsižvelgdamas į Rekomendacijas Nr. 01/2020 dėl priemonių duomenų perdavimo priemonėms papildyti, siekiant užtikrinti atitiktį ES asmens duomenų apsaugos lygiui?

d) Ar pagal kriterijus reikalaujama, kad duomenų importuotojas dokumentuotų veiksmingai įgyvendintas organizacines ir technines priemones, kad būtų užtikrintos tinkamos apsaugos priemonės pagal BDAR 46 straipsnį, ir galėtų tuos dokumentus suteikti sertifikavimo įstaigai ir paprašius kompetentingoms duomenų apsaugos institucijoms ir duomenų eksportuotojui?

e) Ar pagal kriterijus reikalaujama, kad duomenų importuotojas nustatytų ir įgyvendintų organizacines ir technines priemones perduotų asmens duomenų saugumui užtikrinti, atsižvelgiant į Rekomendacijas Nr. 01/2020 dėl priemonių duomenų perdavimo priemonėms papildyti, siekiant užtikrinti atitiktį ES asmens duomenų apsaugos lygiui, jei į sertifikavimo kaip duomenų perdavimo priemonės taikymo sritį įtrauktas tranzitas?

f) Ar pagal kriterijus reikalaujama sertifikavimo įstaigai ir duomenų eksportuotojui garantuoti, kad duomenų importuotojas neturi pagrindo manyti, jog jam taikytini teisės aktai ir praktika gali sutrukdyti jam įvykdyti su sertifikavimu susijusias jo pareigas?

2. Duomenų eksportuotojų ir duomenų importuotojų bendrosios pareigos

a) Ar pagal kriterijus reikalaujama duomenų eksportuotojų ir duomenų importuotojų sutartyse (pvz., esamoje paslaugų sutartyje) nustatyti konkretaus duomenų perdavimo, kuriam taikomas sertifikavimas, aprašymą ir kad atitinkamiems duomenų subjektams būtų pripažįstamos trečiųjų šalių naudos gavėjų teisės?

b) Jei pagal kriterijus reikalaujama pateikti konkretų šių sutarčių ar priemonių turinį ir pateikiamas šablonas, ar pagal kriterijus reikalaujama, kad jie taip pat būtų vertinami?

3. Tolesnio duomenų perdavimo taisyklės

a) Ar pagal kriterijus reikalaujama, kad tolesniam duomenų perdavimui būtų taikomos specialios apsaugos priemonės pagal BDAR V skyriaus reikalavimus, siekiant užtikrinti, kad nebūtų pakenkta EEE užtikrinamam apsaugos lygiui, ir ar pagal kriterijus reikalaujama, kad

sertifikavimo įstaigai ir EEE esančiai priežiūros institucijai, kurios kompetencijai priklauso duomenų eksportuotojas (-ai), ir duomenų eksportuotojui paprašius būtų suteikiami atitinkami dokumentai?

4. Teisių gynimas ir vykdymo užtikrinimas

a) Ar pagal kriterijus numatyta, kad duomenų subjektai gali užtikrinti savo, kaip trečiųjų šalių naudos gavėjų, teises duomenų importuotojo atžvilgiu duomenų subjekto įprastinės gyvenamosios vietos EEE teisme arba tarptautinėje organizacijoje, įskaitant kompensaciją už duomenų subjekto patirtą žalą, jei duomenų importuotojas nesilaiko atitinkamos sertifikavimo schemos?
b) Ar pagal kriterijus galima tinkamai įvertinti, ar duomenų importuotojas EEE yra atsakingas už duomenų subjekto patirtą žalą, jei nesilaikoma atitinkamos sertifikavimo schemos?
c) Ar pagal kriterijus reikalaujama, kad duomenų subjektai galėtų pateikti skundą dėl duomenų importuotojo EEE esančiai priežiūros institucijai, visų pirma EEE valstybėje, kurioje yra jo įprastinė gyvenamoji vieta ar darbo vieta arba kuri yra kompetentinga duomenų eksportuotojo (-ų) atžvilgiu?
d) Ar pagal kriterijus reikalaujama, kad duomenų importuotojas bendradarbiautų su EEE esančia priežiūros institucija, kompetentinga už duomenų eksportuotoją (-us), ir sutiktų, kad jis būtų jos audituojamas ir tikrinamas, atsižvelgti į jos rekomendacijas ir laikytis jos sprendimų?

5. Procesas ir veiksmai tais atvejais, kai nacionalinės teisės aktais užkertamas kelias laikytis įsipareigojimų, prisiimtų vykdant sertifikavimą

a) Ar pagal kriterijus reikalaujama įsipareigoti, kad tais atvejais, kai duomenų importuotojas į trečiąją valstybę arba tarptautinę organizaciją turi pagrindo manyti, jog dėl jam taikomų teisės aktų ir praktikos pakeitimų jam gali būti užkirstas kelias įvykdyti su sertifikavimu susijusias pareigas, jis nedelsiant apie tai praneš sertifikavimo įstaigai ir duomenų eksportuotojui, kad pastarasis galėtų įvertinti, ar būtina nedelsiant sustabdyti duomenų perdavimą?
b) Ar pagal kriterijus reikalaujama aprašyti veiksmus, kurių reikia imtis (įskaitant pranešimą EEE esančiam duomenų eksportuotojui ir atitinkamų papildomų priemonių taikymą), jei duomenų importuotojas sužino apie trečiosios valstybės teisės aktus ar praktiką, kuriais užkertamas kelias laikytis su sertifikavimu susijusių pareigų, taip pat priemones, kurių reikia imtis, kai trečiosios valstybės valdžios institucijos prašo informacijos (įskaitant pareigą įvertinti ir prireikus užginčyti prašymo teisėtumą ir kuo labiau sumažinti atskleidžiamos informacijos kiekį)?

6. Trečiųjų valstybių institucijų prašymų susipažinti su duomenimis tvarkymas

a) Ar pagal kriterijus reikalaujama, kad duomenų importuotojas nedelsdamas informuotų duomenų eksportuotoją, jei trečiosios valstybės institucijos pateiktų prašymus susipažinti su duomenimis, ir imtųsi tinkamų papildomų priemonių?
b) Ar pagal kriterijus reikalaujama, kad duomenų perdavimas nebūtų vykdomas dėl neproporcingų trečiųjų valstybių valdžios institucijų prašymų susipažinti su duomenimis, visų pirma prašymų, kuriais reikalaujama masiškai ir nediferencijuotai perduoti asmens duomenis?

7. Su duomenų eksportuotoju susijusios papildomos apsaugos priemonės

46. Ar pagal kriterijus reikalaujama, kad, jei taip numatyta, duomenų importuotojas, be kita ko, nustatydamas atitinkamus privalomus reikalavimus duomenų eksportuotojui, užtikrintų, kad jam nustačius papildomas priemones duomenų eksportuotojas taip pat nustatytų atitinkamas papildomas priemones, atsižvelgiant į EDAV rekomendacijas Nr. 01/2020 ir naudojimo atvejus, siekiant užtikrinti veiksmingą duomenų importuotojo papildomų priemonių įgyvendinimą?

4 PRIVALOMI IR VYKDYTINI ĮSIPAREIGOJIMAI, KURIUOS REIKIA ĮGYVENDINTI

47. BDAR 42 straipsnio 2 dalyje reikalaujama, kad duomenų valdytojai ir duomenų tvarkytojai, kuriems netaikomas BDAR ir kurie laikosi duomenų perdavimui skirto sertifikavimo mechanizmo, be kita ko, sutartinėmis arba kitomis teisiškai privalomomis priemonėmis[22] prisiimtų privalomus ir vykdytinus įsipareigojimus taikyti sertifikavimo mechanizmu numatytas tinkamas apsaugos priemones, be kita ko, susijusias su duomenų subjektų teisėmis.

48. Kaip nurodyta BDAR, tokie įsipareigojimai gali būti prisiimami sudarant sutartį ir tai atrodo paprasčiausias sprendimas. Taip pat galėtų būti taikomos kitos priemonės, su sąlyga, kad sertifikavimo mechanizmo besilaikantys duomenų valdytojai ir (arba) duomenų tvarkytojai galėtų įrodyti, kad tokios kitos priemonės yra privalomos ir vykdytinos.

49. Bet kuriuo atveju privalomas ir vykdytinas pobūdis turi būti užtikrintas pagal ES teisę, o įsipareigojimai taip pat turėtų būti privalomi ir vykdytini duomenų subjektų kaip trečiųjų šalių naudos gavėjų.

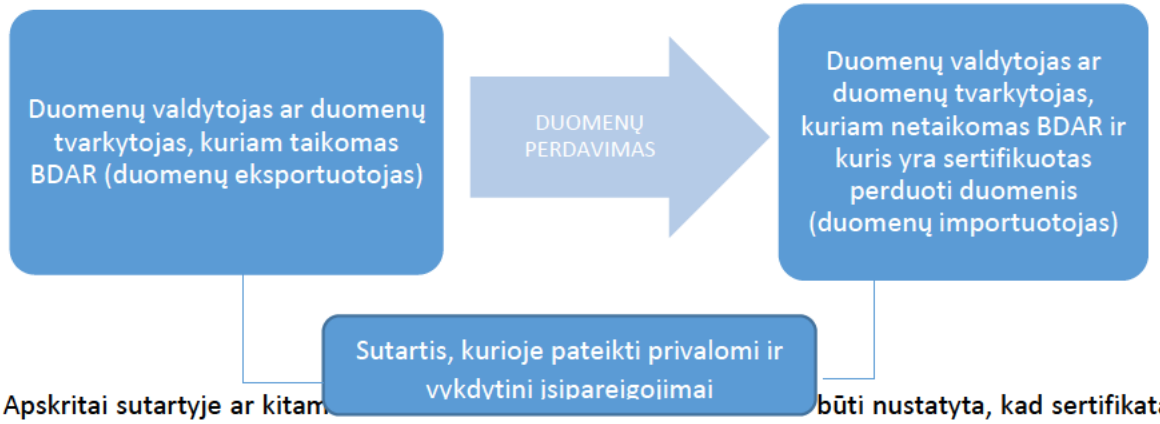
50. Tiesioginis išankstinis sprendimas būtų įtraukti privalomus ir vykdytinus įsipareigojimus į duomenų eksportuotojo ir duomenų importuotojo sutartį. Praktiškai šalys galėtų vadovautis esama sutartimi (pvz., duomenų eksportuotojo ir duomenų importuotojo paslaugų susitarimu, duomenų valdytojų ir duomenų tvarkytojų susitarimu dėl duomenų tvarkymo pagal BDAR 28 straipsnį arba pavienių duomenų valdytojų dalijimosi duomenimis susitarimu), į kurią būtų galima įtraukti privalomus ir vykdytinus įsipareigojimus. Šie įsipareigojimai turėtų būti aiškiai atskirti nuo visų kitų sąlygų. Kita galimybė galėtų būti remtis atskira sutartimi, pavyzdžiui, prie duomenų perdavimui skirto sertifikavimo mechanizmo pridedant pavyzdinę sutartį, kurią tuomet turėtų pasirašyti trečiosios valstybės duomenų valdytojai ir (arba) duomenų tvarkytojai ir visi jos duomenų eksportuotojai.

51. Atsižvelgiant į konkrečią padėtį, turėtų būti galima lanksčiai pasirinkti tinkamiausią variantą.

52. Kai duomenų tvarkytojas turi naudoti sertifikavimo mechanizmą duomenų perdavimui ir tolesniam perdavimui pagalbiniams duomenų tvarkytojams, nuoroda į sertifikavimo mechanizmą ir dokumentą, kuriame numatyti privalomi ir vykdytini įsipareigojimai, taip pat turėtų būti pateikta duomenų tvarkytojo ir jo duomenų valdytojo pasirašytame susitarime.

Privalomų ir vykdytinų įsipareigojimų, įtrauktų į duomenų eksportuotojo ir duomenų importuotojo sutartį, pavyzdys:

[22] Ši teisiškai privaloma priemonė negali būti dar viena V skyriaus priemonė (pvz., SCC), nes 46 straipsnio 2 dalies f punkte nurodyti privalomi ir vykdytini įsipareigojimai turi būti parengti taip, kad būtų užtikrinta, kad duomenų importuotojas laikytųsi sertifikavimo kriterijų.



53. Apskritai sutartyje ar kitam… būti nustatyta, kad sertifikatą turintis duomenų valdytojas ir (arba) duomenų tvarkytojas, veikiantis kaip duomenų importuotojas, įsipareigoja laikytis duomenų perdavimui skirtame sertifikate nurodytų taisyklių, kai tvarkomi atitinkami iš EEE gauti duomenys, ir patikina, kad jis neturi pagrindo manyti, jog atitinkamam duomenų tvarkymui taikytini trečiosios valstybės įstatymai ir praktika, įskaitant bet kokius asmens duomenų atskleidimo reikalavimus arba priemones, leidžiančias valdžios institucijoms susipažinti su duomenimis, neleidžia jam vykdyti su sertifikavimu susijusių įsipareigojimų, ir kad jis informuos eksportuotoją apie visus atitinkamus teisės aktų ar praktikos pakeitimus šioje srityje.

54. Sutartimi ar kita priemone taip pat numatomi mechanizmai, leidžiantys užtikrinti tokių įsipareigojimų vykdymą tais atvejais, kai duomenų valdytojas ir (arba) duomenų tvarkytojas, veikiantis kaip duomenų importuotojas, nesilaiko su sertifikavimu susijusių taisyklių, visų pirma dėl duomenų subjektų, kurių duomenys bus perduodami pagal sertifikavimą, teisių.

55. Konkrečiau, sutartis ar kita priemonė turėtų apimti:

- tai, kad duomenų subjektai, kurių duomenys perduodami pagal sertifikavimo procedūrą, kaip trečiosios šalys naudos gavėjai, turi teisę užtikrinti sertifikuoto duomenų importuotojo prisiimtų su sertifikavimu susijusių įsipareigojimų vykdymą;

- atsakomybės už duomenų importuotojo, sertifikuoto už EEE ribų, sertifikavimo taisyklių nesilaikymą klausimą. Tuo atveju, kai duomenų importuotojas, sertifikuotas už EEE ribų, nesilaiko sertifikavimo taisyklių, duomenų subjektai, pasinaudodami savo, kaip trečiosios šalies naudos gavėjo, teise, įskaitant teisę gauti kompensaciją, turi turėti galimybę pareikšti tam subjektui ieškinį EEE esančioje priežiūros institucijoje ir EEE teisme valstybėje, kurioje yra duomenų subjekto įprastinė gyvenamoji vieta. Sertifikatą turintis duomenų importuotojas sutinka su duomenų subjekto sprendimu tai padaryti. Kai dėl to, kad duomenų importuotojas nesilaiko taisyklių, duomenų eksportuotojui gali kilti atsakomybė, duomenų subjektai taip pat turi turėti galimybę duomenų eksportuotojui pareikšti bet kokį ieškinį priežiūros institucijoje arba teisme valstybėje, kurioje yra įsisteigęs duomenų eksportuotojas arba kurioje yra duomenų subjekto įprastinė gyvenamoji vieta[23]. Duomenų importuotojas ir duomenų eksportuotojas taip pat turėtų sutikti, kad duomenų subjektui BDAR 80 straipsnio 1 dalyje nustatytomis sąlygomis galėtų atstovauti ne pelno įstaiga, organizacija ar asociacija;

[23] Ši atsakomybė neturėtų daryti poveikio mechanizmams, kurie turi būti įgyvendinti sertifikavimo tikslais, ir sertifikavimo įstaigai, kuri pagal sertifikavimo procedūrą taip pat gali imtis priemonių prieš sertifikuotus duomenų valdytojus ir (arba) duomenų tvarkytojus, nustatydama taisomuosius veiksmus.

- duomenų eksportuotojo teisę reikalauti, kad sertifikatą turinčiam duomenų importuotojui būtų taikomos sertifikavimo taisyklės kaip trečiajai šaliai naudos gavėjai;
- sertifikatą turinčio duomenų importuotojo pareigą pranešti duomenų eksportuotojui ir duomenų eksportuotojo priežiūros institucijai apie visas priemones, kurių ėmėsi sertifikavimo įstaiga, reaguodama į nustatytą to paties duomenų importuotojo sertifikavimo taisyklių nesilaikymą.

PRIEDAS

A. PAPILDOMŲ PRIEMONIŲ, KURIAS TURI ĮGYVENDINTI DUOMENŲ IMPORTUOTOJAS TUO ATVEJU, JEI Į SERTIFIKAVIMO TAIKYMO SRITĮ YRA ĮTRAUKTAS TRANZITAS, PAVYZDŽIAI

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

Turi būti nustatyti kriterijai, susiję su šifravimo standartais ir iššifravimo rakto saugumu, visų pirma kriterijai, susiję su teisine padėtimi trečiojoje valstybėje. Jei duomenų importuotojas gali būti priverstas perduoti iššifravimo raktus, papildoma priemonė negali būti laikoma veiksminga[24].

Naudojimo atvejis Nr. 2. Pseudoniminių duomenų perdavimas

Pseudoniminių duomenų atveju nustatomi papildomos informacijos, būtinos perduodamiems duomenims priskirti asmeniui, kurio tapatybė nustatyta arba gali būti nustatyta, saugumo kriterijai, visų pirma:

– kriterijai, susiję su teisine padėtimi trečiojoje valstybėje. Jei duomenų importuotojas gali būti priverstas susipažinti su papildomais duomenimis arba juos naudoti, kad jie būtų priskirti asmeniui, kurio tapatybė nustatyta arba gali būti nustatyta, priemonė negali būti laikoma veiksminga[25];

– kriterijai, susiję su papildomos informacijos, kurią turi trečiųjų valstybių institucijos ir kurios gali pakakti norint priskirti duomenis asmeniui, kurio tapatybė yra nustatyta arba gali būti nustatyta, apibrėžtimi.

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

Šifruotų duomenų atveju turi būti įtraukti visi saugaus tranzito kriterijai. Jei duomenų importuotojas gali būti priverstas perduoti kriptografinius raktus iššifravimui ar tapatumui nustatyti arba pakeisti tranzitui naudojamą komponentą taip, kad būtų pakenkta jo saugumo savybėms, papildoma priemonė negali būti laikoma veiksminga[26].

Naudojimo atvejis Nr. 4. Apsaugotas gavėjas

Apsaugotų gavėjų atveju turi būti apibrėžti konfidencialumo ribų kriterijai. Tvarkant duomenis turi būti laikomasi teisinio konfidencialumo ribų. Tai taip pat taikoma (pagalbinių) duomenų tvarkytojų atliekamam duomenų tvarkymui ir tolesniam duomenų perdavimui; tokių duomenų gavėjams taip pat turi būti taikomas konfidencialumas[27].

---

[24] 2 priedas, Rekomendacijos Nr. 01/2020 dėl priemonių duomenų perdavimo priemonėms papildyti, siekiant užtikrinti atitiktį ES asmens duomenų apsaugos lygiui, 2.0 versija. Naudojimo atvejis Nr. 1. Duomenų saugojimas atsarginei kopijai ir kitiems tikslams, kuriems nereikia prieigos prie nešifruotų duomenų, p. 85; https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_lt.pdf.

[25] Žr. 86–89 punktus.

[26] Žr. 90 punktą.

[27] Žr. 91 punktą.

B. PAPILDOMŲ PRIEMONIŲ, TAIKOMŲ TUO ATVEJU, KAI TRANZITUI NETAIKOMAS SERTIFIKAVIMAS IR EKSPORTUOTOJAS TURI JAS UŽTIKRINTI, PAVYZDŽIAI

Naudojimo atvejis Nr. 2. Pseudoniminių duomenų perdavimas

Turi būti numatyti kriterijai, susiję nėra pateikiama su papildoma informacija, kurią turi trečiųjų valstybių institucijos ir kurios gali pakakti norint priskirti duomenis asmeniui, kurio tapatybė yra nustatyta arba gali būti nustatyta.

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

Turi būti numatyti kriterijai, susiję su viešojo rakto sertifikavimo institucijos ar naudojamos infrastruktūros patikimumu, tapatumo nustatymui arba iššifravimui naudojamų kriptografinių raktų saugumu ir raktų valdymo patikimumu, taip pat tinkamai prižiūrimos programinės įrangos be žinomų trūkumų naudojimu.

Jei duomenų importuotojas gali būti priverstas atskleisti kriptografinius raktus iššifravimui ar tapatumui nustatyti arba pakeisti tranzitui naudojamą komponentą taip, kad būtų pakenkta jo saugumo savybėms, priemonė negali būti laikoma veiksminga[28].

Naudojimo atvejis Nr. 4. Apsaugotas gavėjas

Apsaugotų gavėjų atveju turi būti apibrėžti konfidencialumo ribų kriterijai. Tvarkant duomenis turi būti laikomasi teisinio konfidencialumo ribų. Tai taip pat taikoma (pagalbinių) duomenų tvarkytojų atliekamam duomenų tvarkymui ir tolesniam duomenų perdavimui; tokių duomenų gavėjams taip pat turi būti taikomas konfidencialumas[29].

[28] Žr. rekomendacijų 90 punktą.
[29] Žr. rekomendacijų 91 punktą.