Nuomonė 14/2026 dėl „Europrivacy“ sertifikavimo kriterijų patvirtinimo Valdyboje Europos duomenų apsaugos ženklui išduoti pagal BDAR 42 straipsnio 5 dalį

Priimta 2026 m. balandžio 15 d.

Translations proofread by EDPB Members.

This language version has not yet been proofread.

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) 63 straipsnį, 64 straipsnio 2 dalį ir 42 straipsnį,

atsižvelgdama į Europos ekonominės erdvės (toliau – 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 10 ir 22 straipsnius,

kadangi:

1. valstybės narės, priežiūros institucijos, Europos duomenų apsaugos valdyba (toliau – EDAV arba Valdyba) ir Europos Komisija skatina nustatyti – visų pirma Sąjungos lygmeniu – duomenų apsaugos sertifikavimo mechanizmus (toliau – sertifikavimo mechanizmai) ir duomenų apsaugos ženklus bei žymenis, kad būtų galima įrodyti, jog duomenų valdytojai ir duomenų tvarkytojai, vykdydami duomenų tvarkymo operacijas, laikosi BDAR, atsižvelgiant į konkrečius labai mažų, mažųjų ir vidutinių įmonių poreikius. Be to, sertifikavimo mechanizmų nustatymas gali padidinti skaidrumą ir leisti duomenų subjektams įvertinti konkrečių produktų ir paslaugų duomenų apsaugos lygį;
2. sertifikavimo kriterijai yra neatsiejama sertifikavimo mechanizmo dalis. Todėl pagal BDAR reikalaujama, kad nacionalinio sertifikavimo mechanizmo kriterijus patvirtintų kompetentinga priežiūros institucija (BDAR 42 straipsnio 5 dalis ir 43 straipsnio 2 dalies b punktas), o Europos duomenų apsaugos ženklo atveju – EDAV (BDAR 42 straipsnio 5 dalis ir 70 straipsnio 1 dalies o punktas);
3. kai priežiūros institucija (toliau – PI) ketina siūlyti, kad EDAV patvirtintų Europos duomenų apsaugos ženklą pagal BDAR 42 straipsnio 5 dalį, ji turėtų nurodyti sertifikavimo schemos savininko ketinimą pasiūlyti sertifikavimo mechanizmą visose valstybėse narėse. Šiuo atveju pagrindinis EDAV vaidmuo yra užtikrinti nuoseklų BDAR taikymą pasitelkiant nuoseklumo užtikrinimo mechanizmą, nurodytą BDAR 63, 64 ir 65 straipsniuose. Atsižvelgdama į tai ir remdamasi BDAR 64 straipsnio 2 dalimi, EDAV patvirtina sertifikavimo kriterijus;
4. šia nuomone siekiama užtikrinti nuoseklų BDAR taikymą, be kita ko, priežiūros institucijų, duomenų valdytojų ir duomenų tvarkytojų vykdomus taikymo veiksmus, atsižvelgiant į esminius elementus, kurie turi būti nustatyti sertifikavimo mechanizmais. Visų pirma, EDAV vertinimas atliekamas remiantis Sertifikavimo ir sertifikavimo kriterijų nustatymo pagal Reglamento 42 ir 43 straipsnius gairėmis Nr. 1/2018 (toliau – Gairės) ir jų Papildymu, kuriame pateikiamos Sertifikavimo kriterijų gairės (toliau – Papildymas), dėl kurio surengtų viešų konsultacijų laikotarpis baigėsi 2021 m. gegužės 26 d.;
5. EDAV atitinkamai pripažįsta, kad kiekvienas sertifikavimo mechanizmas turėtų būti vertinamas individualiai ir šio vertinimo rezultatai nedaro poveikio jokio kito sertifikavimo mechanizmo vertinimui;
6. sertifikavimo mechanizmais turėtų būti sudarytos sąlygos duomenų valdytojams ir duomenų tvarkytojams įrodyti, kad jie laikosi BDAR reikalavimų. Todėl jų kriterijai turėtų tinkamai atspindėti BDAR nustatytus asmens duomenų apsaugos reikalavimus ir principus ir padėti nuosekliai taikyti BDAR;

[1] Nuorodos į valstybes nares šiame dokumente turėtų būti suprantamos kaip nuorodos į EEE valstybes nares.

7. kita vertus, sertifikavimo schemos savininkas turėtų užtikrinti, kad sertifikavimo mechanizmas būtų suderinamas su visais įtrauktais ar naudojamais ISO standartais ir sertifikavimo praktika ir juos atitiktų;
8. todėl sertifikavimu turėtų būti sukurta pridėtinė vertė duomenų valdytojams ir duomenų tvarkytojams, padedant jiems įgyvendinti standartizuotas ir konkrečias organizacines ir technines priemones, kuriomis akivaizdžiai palengvinama ir pagerinama duomenų tvarkymo operacijų atitiktis BDAR, atsižvelgiant į konkrečiam sektoriui taikomus reikalavimus;
9. EDAV palankiai vertina sertifikavimo schemų savininkų pastangas tobulinti sertifikavimo mechanizmus – praktines ir potencialiai ekonomiškai efektyvias priemones, kuriomis užtikrinamas BDAR reikalavimų laikymasis ir stiprinama duomenų subjektų teisė į privatumą ir duomenų apsaugą didinant skaidrumą;
10. EDAV primena, kad sertifikavimas yra savanoriška atskaitomybės priemonė ir kad atitiktimi sertifikavimo mechanizmui nesumažinama duomenų valdytojų arba duomenų tvarkytojų atsakomybė laikytis BDAR ir netrukdoma priežiūros institucijoms vykdyti jų užduotis ir įgaliojimus pagal BDAR ir atitinkamus nacionalinius įstatymus;
11. šioje nuomonėje EDAV nagrinėja tokius klausimus kaip kriterijų taikymo sritis, jų taikomumas ir aktualumas visose valstybėse narėse;
12. šioje EDAV nuomonėje daugiausia dėmesio skiriama sertifikavimo kriterijams. EDAV gali pareikalauti aukšto lygio informacijos apie vertinimo metodus, kad ji galėtų nuodugniai įvertinti galimybę atlikti kriterijų auditą rengdama savo nuomonę šiuo klausimu. Tačiau ši nuomonė nereiškia jokio tokių vertinimo metodų patvirtinimo;
13. pagal BDAR 64 straipsnio 2 dalį, taikomą kartu su EDAV darbo tvarkos taisyklių 10 straipsnio 2 dalimi, EDAV nuomonė priimama per aštuonias savaites, skaičiuojant nuo pirmos darbo dienos, kai pirmininkas ir kompetentinga priežiūros institucija nusprendžia, kad dokumentų rinkinys yra išsamus. Atsižvelgiant į klausimo sudėtingumą, pirmininko sprendimu šis laikotarpis gali būti pratęstas dar šešioms savaitėms. Jei EDAV nuomonėje daroma išvada, kad nagrinėjamų kriterijų negalima patvirtinti, PI gali pakartotinai pateikti kriterijus tvirtinti po to, kai bus išspręsti pirminėje EDAV nuomonėje išsakyti susirūpinimą keliantys klausimai,

priėmė šią nuomonę:

1 Faktų santrauka

14. Vadovaudamasis BDAR 42 straipsnio 5 dalimi ir Gairėmis, Europos sertifikavimo ir privatumo centras (angl. *European Centre for Certification and Privacy*) (toliau – sertifikavimo schemos savininkas) parengė „Europrivacy“ sertifikavimo kriterijų 82-ą versiją (toliau – sertifikavimo kriterijai).
15. 2026 m. sausio 29 d. Liuksemburgo priežiūros institucija (toliau – LU PI) pateikė „Europrivacy“ sertifikavimo kriterijų 82-ą versiją EDAV patvirtinti pagal BDAR 64 straipsnio 2 dalį.
16. Sprendimas dėl dokumentų išsamumo buvo priimtas 2026 m. kovo 31 d.
17. EDAV primena, kad 2022 m. spalio 10 d. ji patvirtino „Europrivacy“ sertifikavimo kriterijų 60-ą versiją Europos duomenų apsaugos ženklui išduoti pagal BDAR 42 straipsnio 5 dalį, paskelbdama EDAV nuomonę 28/2022 (toliau – ankstesnė EDAV nuomonė).

18. Šioje nuomonėje nagrinėjama iš dalies pakeista „Europrivacy“ sertifikavimo kriterijų versija (82-a versija). Visų pirma Valdyba pažymi, kad pastarosios sertifikavimo kriterijų versijos, kuri šiuo metu pateikta EDAV, taikymo sritis buvo išplėsta įtraukiant pareiškėjus, kuriems taikoma BDAR 3 straipsnio 2 dalis, ir šiuo atžvilgiu įtrauktas kriterijus dėl galimos trečiosios valstybės teisės kolizijos. Be to, Valdyba pažymi, kad iš dalies pakeistoje „Europrivacy“ sertifikavimo kriterijų versijoje (82-oje versijoje) buvo pakoreguoti, patobulinti ir (arba) patikslinti kai kurie iš EDAV 2022 m. patvirtintų sertifikavimo kriterijų. Šie pakeitimai, visų pirma susiję su: atstovo paskyrimu EEE ir bendradarbiavimu nagrinėjant EEE kompetentingų duomenų apsaugos institucijų pateiktus prašymus; nacionalinių įsipareigojimų laikymosi vertinimo ataskaita (angl. *National Obligations Compliance Assessment Report*, NOCAR), tolesniu duomenų tvarkymu, apsaugos priemonėmis, taikomomis tvarkant specialių kategorijų asmens duomenis, pagalbinių duomenų tvarkytojų pasitelkimu, duomenų saugumo pažeidimų sprendimu, duomenų tvarkymo rizikos vertinimu ir saugumo politika bei reikalavimais.

19. EDAV pabrėžia, kad 2022 m. jau patvirtintų sertifikavimo kriterijų pakeitimas paveiks iki šiol jau išduotus sertifikatus ir tebevykstančius sertifikavimo procesus. Todėl reikėtų tinkamai ir skaidriai valdyti pereinamąjį laikotarpį nuo Europos duomenų apsaugos ženklų, suteiktų pagal sertifikavimo kriterijus, patvirtintus ankstesne EDAV nuomone (jų 60-ą versiją), iki Europos duomenų apsaugos ženklų, suteiktų pagal sertifikavimo kriterijus (jų 82-ą versiją), kurie vertinami šioje nuomonėje. Atsižvelgdama į tai, Valdyba, remdamasi sertifikavimo schemos savininko pateiktais dokumentais, supranta, kad visi tebevykstantys sertifikavimo procesai turi būti užbaigti iki 2026 m. pabaigos; po šio termino išduodant naujus sertifikatus nebebus naudojami sertifikavimo kriterijai, patvirtinti ankstesne EDAV nuomone (jų 60-a versija). Iki šiol išduoti sertifikatai galios iki jų trejų metų galiojimo pabaigos ir bus atnaujinti pagal sertifikavimo kriterijų 82-ą versiją. Todėl po 2029 m. pabaigos sertifikavimo kriterijai, patvirtinti ankstesne EDAV nuomone (jų 60-a versija), bus visiškai pakeisti sertifikavimo kriterijų 82-a versija. Be to, sertifikavimo schemos savininkas viešai paskelbs informaciją apie pereinamojo laikotarpio planą. Gali prireikti atitinkamai koreguoti sertifikavimo įstaigų akreditavimo apimtį, bet šioje nuomonėje šis klausimas nenagrinėjamas, kadangi jis nepriklauso EDAV kompetencijai.

20. Bendroji „Europrivacy“ sertifikavimo schema nėra skirta naudoti kaip duomenų perdavimo priemonė pagal BDAR 42 straipsnio 2 dalį ir 46 straipsnio f punktą. 2026 m. sausio 29 d. LU PI taip pat pateikė papildomą sertifikavimo kriterijų rinkinį („Europrivacy“ sertifikavimo schemos taikymo srities išplėtimas, skirtas duomenų importuotojams sertifikuoti pagal 46 straipsnį) EDAV tvirtinti pagal BDAR 64 straipsnio 2 dalį; šio rinkinio taikymo sritis apima duomenų valdytojus ir duomenų tvarkytojus, įsisteigusius ne EEE, kuriems BDAR tiesiogiai netaikomas pagal BDAR 3 straipsnio 2 dalį, bet kurie tvarko asmens duomenis, gautus iš kito duomenų valdytojo ar duomenų tvarkytojo, kuriam BDAR taikomas. Dėl šio sertifikavimo kriterijų rinkinio, kuris yra skirtas naudoti kaip duomenų perdavimo priemonė pagal BDAR 46 straipsnio 2 dalies f punktą, EDAV priėmė Nuomonę 15/2026.

2 Vertinimas

21. EDAV atliko sertifikavimo kriterijų vertinimą, kad jie būtų patvirtinti pagal BDAR 42 straipsnio 5 dalį, vadovaudamasi Gairių 2 priede (toliau – Priedas) ir jų Papildyme numatyta struktūra.

22. Kad parengtų šią nuomonę ir patvirtintų sertifikavimo kriterijus, EDAV įvertino aprašus „Vertinimo taikymas ir objektas. Pirminės patikros ir kontrolės priemonės“ (A), „*Europrivacy* BDAR pagrindiniai kriterijai“ (G), „Techninių ir organizacinių priemonių patikros ir kontrolės priemonės“ (T), kurie buvo pateikti kartu su sertifikavimo kriterijais.

23. Be to, šiuo klausimu Valdyba pažymi, kad su sertifikavimo kriterijais, patvirtintais ankstesne EDAV nuomone (jų 60-a versija) pateiktos „papildomos kontekstinės patikros ir kontrolės priemonės“ [2], kuriomis siekiama užtikrinti, kad su vertinimo objektu susijęs duomenų tvarkymas atitiktų konkrečiai sričiai ir technologijoms keliamus reikalavimus [3], nebuvo patvirtintos ankstesne EDAV nuomone ir kad tokios „papildomos kontekstinės patikros ir kontrolės priemonės“ nebėra įtrauktos į atnaujintų dokumentų rinkinį, kuris buvo pateiktas šiai nuomonei parengti.

24. Atsižvelgdama į patikslintas sertifikavimo schemos apibrėžtis, Valdyba pažymi, kad nuorodos į kompetentingas duomenų apsaugos institucijas visoje sertifikavimo schemoje reiškia EEE duomenų apsaugos institucijas[4].

25. Kalbant apie trečiosios valstybės teisę, Valdyba supranta, kad ji reiškia pareiškėjui ir (arba) su vertinimo objektu susijusiems tvarkomiems asmens duomenims taikytiną teisę tiek, kiek tokia teise neapribojamos duomenų apsaugos teisės viršijant tai, kas būtina ir proporcinga demokratinėje visuomenėje siekiant apsaugoti vieną iš BDAR 23 straipsnio 1 dalyje išvardytų tikslų, yra proporcinga siekiamam tikslui, ja gerbiama teisė į duomenų apsaugą ir numatyta tinkamų bei konkrečių priemonių duomenų subjektų pagrindinėms teisėms ir interesams apsaugoti.

2.1 Sertifikavimo mechanizmo taikymo sritis ir vertinimo objektas

26. EDAV primena[5], kad „Europrivacy“ sertifikavimo mechanizmas yra bendroji sertifikavimo schema, nes ji skirta įvairioms duomenų tvarkymo operacijoms, kurias atlieka įvairių veiklos sektorių duomenų valdytojai ir duomenų tvarkytojai.

27. Valdyba palankiai vertina tai, kad su šios sertifikavimo schemos taikymo sritimi susijusiuose dokumentuose, kuriuos pateikė LU PI, pakeista „Europrivacy“ sertifikavimo schema taikoma: **i)** duomenų valdytojams ir duomenų tvarkytojams, įsisteigusiems Europos Sąjungoje (ES) arba Europos ekonominėje erdvėje (EEE); **ii)** duomenų valdytojams ir duomenų tvarkytojams, įsisteigusiems ne EEE, kuriems BDAR taikomas pagal BDAR 3 straipsnio 2 dalį, nes jie siūlo prekes ar paslaugas EEE duomenų subjektams arba jie stebi EEE duomenų subjektų elgseną[6]. Kriterijų taikomumas priklauso nuo pareiškėjo vaidmens ir atsakomybės.

28. Kalbant apie trečiojoje valstybėje įsisteigusius pareiškėjus pagal BDAR 3 straipsnio 2 dalį, kuriems netaikomas sprendimas dėl tinkamumo, apimantis vertinimo objektą, A.2.1.6 kriterijumi apibrėžtos sąlygos, kurių būtina laikytis nustatant vertinimo objektą, kai peržiūrima jų sertifikavimo paraiška. Visų pirma, prieš planuodama sertifikavimo auditą, sertifikavimo įstaiga turi patikrinti, ar pareiškėjas geba įrodyti, kad trečiosios valstybės nacionalinė teisė ir

[2] EDAV savo ankstesne nuomone nepatvirtinto „papildomų kontekstinių patikros ir kontrolės priemonių“.
[3] Ankstesnė EDAV nuomonė, 7 ir 8 punktai.
[4] Žr. „Europrivacy“ kriterijuose nurodytą kompetentingos PI apibrėžtį: „*Kompetentinga duomenų apsaugos institucija reiškia EEE duomenų apsaugos institucijas. Apskritai tai yra nacionalinės duomenų apsaugos institucijos, įgaliotos užtikrinti, kad su vertinimo objektu susijęs asmens duomenų tvarkymas atitiktų reikalavimus. BDAR sertifikato išdavimo duomenų importuotojui pagal BDAR 46 straipsnį tikslais kompetentinga duomenų apsaugos institucija yra EEE duomenų eksportuotojo vietos kompetentinga duomenų apsaugos institucija, išskyrus skundų pateikimo atvejus, kai kompetentinga yra bet kuri EEE institucija*“.
[5] Ankstesnė EDAV nuomonė, 6 punktas.
[6] Žr. 2019 m. lapkričio 12 d. priimtų EDAV gairių dėl BDAR (3 straipsnio) teritorinės taikymo srities (2.1 versija) 2 dalį.

praktika netrukdo pareiškėjui laikytis sertifikavimo reikalavimų. Priešingu atveju sertifikavimo procesas sustabdomas paraiškos peržiūros etape.

29. Valdyba pažymi, kad duomenų valdytojas „Europrivacy“ sertifikavimo procesui gali pateikti vertinimo objektą, kuriam taikomas bendras duomenų valdymas (A.2.1.5 kriterijus). Jei vertinimo objektui taikomas bendras duomenų valdymas, Valdyba norėtų pabrėžti, kad akredituota sertifikavimo įstaiga turės atidžiai vykdyti paraiškos peržiūros procesą, kad užtikrintų, jog vertinimo objektas yra prasmingas ir kad pareiškėjas yra visiškai atsakingas už vertinimo objekto atitiktį visoms BDAR nustatytoms prievolėms, kurių laikymąsi siekiama įrodyti sertifikavimo schema. Todėl pareiškėjo ir kitų bendrų duomenų valdytojų, susijusių su vertinimo objektu, sudarytas susitarimas dėl jų atitinkamos atsakomybės už prievolių pagal BDAR laikymąsi gali, priklausomai nuo su vertinimo objektu susijusių duomenų tvarkymo veiksmų konteksto, trukdyti pareiškėjui atitikti sertifikavimo kriterijus.

2.2 Duomenų tvarkymo operacijos

30. Kaip EDAV pažymėjo savo ankstesnėje nuomonėje, sertifikavimo kriterijais atsižvelgiama į atitinkamus duomenų tvarkymo operacijų komponentus (duomenis, sistemas ir tvarkymą), atsižvelgiant į bendrą sertifikavimo schemos taikymo sritį. Visų pirma pagal kriterijus galima nustatyti specialias duomenų kategorijas, apibrėžtas BDAR 9 straipsnyje (kriterijų G.2 skirsnis „Specialus duomenų tvarkymas“).

2.3 Duomenų tvarkymo teisėtumas

31. Kaip EDAV pažymėjo savo ankstesnėje nuomonėje dėl jau patvirtintų sertifikavimo kriterijų (jų 60-os versijos), pagal kriterijus būtina patikrinti duomenų tvarkymo teisėtumą atliekant kiekvieną atskirą duomenų tvarkymo operaciją vertinimo objekto atžvilgiu ir patikrinti teisinio pagrindo reikalavimus, apibrėžtus BDAR 6 straipsnyje (kriterijų G.1 skirsnis „Duomenų tvarkymo teisėtumas“). Visų pirma Valdyba palankiai vertina atnaujintų sertifikavimo kriterijų reikalavimą, kad duomenų subjektų sutikimas apimtų kiekvieną tikslą, kuriuo duomenys tvarkomi, ir kad sutikimo atšaukimas neturi sukelti neigiamų pasekmių duomenų subjektui.

32. Be to, kaip nurodyta ankstesnėje EDAV nuomonėje, sertifikavimo kriterijais reikalaujama patikrinti konkrečius reikalavimus dėl sąlygų, kurioms esant pagal BDAR 9 straipsnio 2 dalį leidžiama tvarkyti specialių kategorijų asmens duomenis (kriterijų G.2.1 skirsnis „Specialus duomenų tvarkymas“), ir užtikrinti papildomus apribojimus ir apsaugos priemones duomenų subjekto teisėms ir laisvėms apginti. Pagal sertifikavimo kriterijus taip pat reikalaujama patikrinti reikalavimus dėl sąlygų, apibrėžtų BDAR 10 straipsnyje, susijusių su asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymą (kriterijų G.2.2 skirsnis), kai taikoma. Šiuo klausimu Valdyba taip pat palankiai vertina atnaujintų sertifikavimo kriterijų (G.2.1.3 kriterijus dėl papildomų apsaugos priemonių, taikomų tvarkant specialių kategorijų asmens duomenis) reikalavimą, kad pareiškėjas taikytų papildomus apribojimus ir apsaugos priemones, kurie pritaikyti pagal konkretų duomenų pobūdį ir susijusius pavojus, kai tvarkomi specialių kategorijų asmens duomenys.

33. Be to, kalbant apie pareiškėjus pagal BDAR 3 straipsnio 2 dalį, įsisteigusius trečiojoje valstybėje, kuriems netaikomas sprendimas dėl tinkamumo, apimantis vertinimo objektą, atnaujintais sertifikavimo kriterijais reikalaujama, kad pareiškėjas pateiktų teisės specialisto parengtą ataskaitą, kurioje būtų įvertinta, ar trečiosios valstybės nacionalinė teisė ir praktika netrukdo jam vykdyti duomenų apsaugos įsipareigojimų pagal BDAR. Panašiai šiuo vertinimu patikrinama, ar trečiosios valstybės nacionalinė teisė neapriboja duomenų apsaugos teisių viršijant tai, kas būtina ir proporcinga demokratinėje visuomenėje siekiant apsaugoti vieną iš BDAR 23 straipsnio 1 dalyje išvardytų tikslų, yra proporcinga siekiamam tikslui, joje gerbiama

teisė į duomenų apsaugą ir numatytos tinkamos bei konkrečios priemonės duomenų subjektų pagrindinėms teisėms ir interesams apsaugoti. Be to, jį reikia peržiūrėti kiekvieną kartą, kai reguliavimo ar organizaciniai pokyčiai gali trukdyti laikytis kriterijų arba turėti įtakos vertinimo objektui ar duomenų subjektų teisėms, ir apie tai turėtų būti informuota sertifikavimo įstaiga (G.1.1.5 kriterijus).

34. Atsižvelgiant į tai, atnaujintų sertifikavimo kriterijų naudojimo vadove paaiškinta, kad „kai pareiškėjui, kuris yra įsisteigęs ne EEE, taikomas sprendimas dėl tinkamumo, apimantis su vertinimo objektu susijusį duomenų tvarkymą, atitiktis šiam reikalavimui gali būti įrodoma pateikiant supaprastintą ataskaitą“. Pagal tuos kriterijus, tokioje ataskaitoje turėtų būti įvertinta, ar sprendimas dėl tinkamumo galioja, ir dokumentuotos priežastys, kodėl vertinimo objektas patenka į to sprendimo dėl tinkamumo taikymo sritį (G.1.1.5 kriterijaus F punktas).

2.4 Duomenų tvarkymo principai

35. EDAV primena, kad kriterijais tinkamai atsižvelgiama į duomenų apsaugos principus pagal BDAR 5 straipsnį. Visų pirma atnaujintuose sertifikavimo kriterijuose išplėstas ir labiau detalizuotas tikslo apribojimo principas, įtraukiant specialų kriterijų, pagal kurį reikalaujama įrodyti, kad asmens duomenys toliau nėra tvarkomi su šiais tikslais nesuderinamu būdu, kad bet koks tolesnio duomenų tvarkymo teisėtumas turėtų būti įvertintas atskirai ir kad siekiant toliau tvarkyti duomenis, atliekamas tikslų suderinamumo vertinimas, kuris tinkamai dokumentuojamas (G.1.1.6 kriterijus).

2.5 Bendrosios duomenų valdytojų ir duomenų tvarkytojų prievolės

36. EDAV primena, kad sertifikavimo kriterijais[7] atspindimos duomenų valdytojo prievolės pagal BDAR 24 straipsnį (kriterijų G.4 skirsnis „Duomenų valdytojo atsakomybė“) ir reikalaujama įvertinti duomenų tvarkytojo ir duomenų valdytojo sutartinius susitarimus pagal BDAR 28 straipsnį (kriterijų G.5 skirsnis „Duomenų tvarkytojai arba pagalbiniai duomenų tvarkytojai“).

37. Be to, Valdyba palankiai vertina papildytą sertifikavimo kriterijų reikalavimą, kad pareiškėjas pagal BDAR 3 straipsnio 2 dalį įsteigtų biurą arba paskirtų atstovą EEE, kaip numatyta BDAR 27 straipsnyje, ir šio biuro arba atstovo kontaktiniai duomenys būtų skelbiami pareiškėjo internetinėje svetainėje (G.4.1.4 kriterijus). Valdyba atkreipia dėmesį į šiuos sertifikavimo kriterijus ir primena, kad šis reikalavimas nėra visada privaloma duomenų valdytojų ir duomenų tvarkytojų pareiga pagal BDAR, todėl reikia atsižvelgti į BDAR 27 straipsnyje nurodytas sąlygas.

38. Be to, EDAV pažymi, kad, kaip nurodyta ankstesnėje nuomonėje, pagal kriterijus reikalaujama, kad visi pareiškėjai paskirtų duomenų apsaugos pareigūną (toliau – DAP), net ir tuo atveju, kai pagal BDAR 37 straipsnį pareiškėjas neprivalo paskirti DAP. Pagal kriterijus tikrinama, ar DAP atitinka 37–39 straipsnių reikalavimus (kriterijų G.9 skirsnis „Duomenų apsaugos pareigūnas“).

39. Pagal sertifikavimo kriterijus taip pat tikrinamas duomenų tvarkymo veiklos įrašų turinys pagal BDAR 30 straipsnį (kriterijų G.5.3 skirsnis „Duomenų tvarkymo veiklos įrašai“). Šiuo atžvilgiu Valdyba palankiai vertina tai, kad atnaujintais sertifikavimo kriterijais reikalaujama, kad

[7] Ankstesnė EDAV nuomonė, 15 punktas.

pareiškėjai pagal BDAR 3 straipsnio 2 dalį bendradarbiautų nagrinėjant EEE kompetentingų DAP prašymus ir prireikus pateiktų jiems duomenų tvarkymo veiklos įrašus (G.5.3.5 kriterijus).

40. Be to, EDAV pažymi, kad buvo įtraukti tam tikri papildomi sertifikavimo kriterijai dėl pagalbinių duomenų tvarkytojų pasitelkimo, taikomi pareiškėjams, kurie atlieka duomenų valdytojų ar duomenų tvarkytojų vaidmenį (G.5.1.2 skirsnis „Pagalbinių duomenų tvarkytojų pasitelkimas“). Toks išskyrimas leidžia geriau atskirti duomenų tvarkymo grandinės dalyvių vaidmenis ir atsakomybę.

2.6 Duomenų subjektų teisės

41. Kaip nurodyta ankstesnėje nuomonėje, EDAV primena, kad sertifikavimo kriterijais tinkamai atsižvelgiama į duomenų subjekto teisę į informaciją pagal BDAR III skyrių ir reikalaujama imtis atitinkamų priemonių[8]. Sertifikavimo kriterijais taip pat reikalaujama, kad būtų įdiegtos priemonės, kuriomis numatoma galimybė įsikišti į duomenų tvarkymo operaciją, kad būtų užtikrintos duomenų subjektų teisės ir sudarytos sąlygos ištaisyti, ištrinti duomenis ar apriboti jų tvarkymą (kriterijų G.3 skirsnis „Duomenų subjektų teisės“).

42. Be to, EDAV palankiai vertina sertifikavimo kriterijų patobulinimus dėl duomenų subjektams teiktinos informacijos (G 3.2 skirsnis „Informacija, kuri turi būti pateikta, kai asmens duomenys renkami iš duomenų subjekto“ ir G.3.3 skirsnis „Informacija, kuri turi būti pateikta, kai asmens duomenys yra gauti ne iš duomenų subjekto“), duomenų subjektų informavimo[9] ir naudojimosi duomenų subjektų teisėmis sąlygų[10] (G 3.1 skirsnis „Skaidrus informavimas, pranešimas ir naudojimosi duomenų subjektų teisėmis sąlygos“), taip pat dėl teisės susipažinti su duomenimis (G 3.4 skirsnis „Duomenų subjekto teisė susipažinti su asmens duomenimis“), reikalauti ištrinti duomenis (G.3.6 skirsnis „Teisė reikalauti ištrinti duomenis (teisė būti pamirštam)“) ir apriboti duomenų tvarkymą (G 3.7.1 kriterijus dėl teisės apriboti duomenų tvarkymą), dėl prievolės pranešti apie asmens duomenų ištaisymą ar ištrynimą arba duomenų tvarkymo apribojimą (G.3.8.2 kriterijus dėl prievolės informuoti duomenų subjektus apie gavėjus, jei to paprašoma), dėl teisės nesutikti (G.3.10 skirsnis „Teisė nesutikti“) ir teisės, kad nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas (G.3.11 skirsnis „Teisė, kad nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas“).

2.7 Pavojus teisėms ir laisvei

43. Savo ankstesnėje nuomonėje EDAV jau nurodė, kad pagal sertifikavimo kriterijus reikalaujama įvertinti su vertinimo objektu susijusio duomenų tvarkymo keliamą pavojų fizinių asmenų teisėms ir laisvėms pagal BDAR 35 straipsnį (kriterijų G.8 skirsnis „Pareiga įvertinti, ar reikalingas poveikio duomenų apsaugai vertinimas (PDAV)“)[11].

44. EDAV palankiai vertina sertifikavimo kriterijų pakeitimus, kuriais siekiama užtikrinti, kad „pareiškėjas, taikydamas pakartotinai pritaikomą metodiką, įvertino duomenų tvarkymo

[8] Ankstesnė EDAV nuomonė, 19 punktas.
[9] Pavyzdžiui, G.3.1.1 kriterijumi dėl pareigos informuoti vartojant aiškią kalbą plačiau paaiškinta informacija apie duomenų tvarkymą, kurią pareiškėjas pateikia duomenų subjektui, dabar nurodant, kad i) informacija turėtų būti pateikiama raštu arba kitomis priemonėmis, ii) informacija turėtų būti prieinama pareiškėjo oficialiaja (-iosiomis) kalba (-omis) ir iii) tikslinių duomenų subjektų kalba.
[10] Pavyzdžiui, G.3.1.3 kriterijumi dėl tinkamo duomenų subjektų teisių valdymo ir registravimo užtikrinimo dabar reikalaujama, kad pareiškėjas būtų įdiegęs procedūrą ar mechanizmą, kad galėtų, be kita ko, patvirtinti prašymo gavimą duomenų subjektui ir valdyti, be kita ko, duomenų subjekto prašymų įrašus, įskaitant gavimo datą.
[11] Ankstesnė EDAV nuomonė, 20 punktas.

keliamą riziką, kuri gali turėti įtakos fizinių asmenų teisėms ir laisvėms“ (G.6.2.4 skirsnis „Duomenų tvarkymo rizikos vertinimas“).

45. Be to, EDAV palankiai vertina kitus papildymus ir detales, numatytus sertifikavimo kriterijuose. Pavyzdžiui, EDAV atkreipia dėmesį į PDAV proceso papildymą, kuriuo atsižvelgiama į aplinkybes, kai pareiškėjas neprivalo atlikti PDAV (G.8.2.1 skirsnis „PDAV proceso reikalavimai“).

2.8 Techninės ir organizacinės apsaugos užtikrinimo priemonės

46. Kaip nurodyta ankstesnėje EDAV nuomonėje, pagal sertifikavimo kriterijus reikalaujama taikyti technines ir organizacines priemones, kuriomis užtikrinamas duomenų tvarkymo operacijų konfidencialumas, vientisumas ir prieinamumas. Kriterijais taip pat reikalaujama taikyti technines priemones, kad būtų įgyvendinta pritaikytoji ir standartizuotoji duomenų apsauga pagal BDAR 25 ir 32 straipsnius (kriterijų G.6 skirsnis „Pritaikytoji ir standartizuotoji duomenų apsauga ir duomenų tvarkymo saugumas“, kriterijų skirsnis G.6.2 „Duomenų tvarkymo saugumas“ ir T kriterijų skirsnis)[12]. Šiuo atžvilgiu Valdyba palankiai vertina tai, kad pakeistais sertifikavimo kriterijais išsamiau paaiškintos (G.6.1.2 skirsnis „Standartizuotasis duomenų kiekio mažinimas“) taisyklės ir procedūros, kurias pareiškėjas turi taikyti siekdamas atitikties šiems kriterijams.

47. Kaip pabrėžiama ankstesnėje EDAV nuomonėje, sertifikavimo kriterijais reikalaujama taikyti priemones, kuriomis užtikrinama, kad pareigos pranešti apie asmens duomenų saugumo pažeidimus būtų vykdomos laiku ir tinkama apimtimi pagal BDAR 33 ir 34 straipsnius (kriterijų G.7 skirsnis „Duomenų saugumo pažeidimų valdymas“).

48. Šiuo atžvilgiu Valdyba pažymi, kad sertifikavimo kriterijai buvo dar patobulinti ir detaliau išdėstyti. Konkrečiau, dabar sertifikavimo kriterijuose pateiktas išsamesnis sąrašas (G.7.1.1 skirsnis „Pareiga dokumentuoti duomenų saugumo pažeidimus“), susijęs su informacija, kurią pareiškėjas turi pagrįsti dokumentais įvykus duomenų saugumo pažeidimui (pvz., paveiktų arba galimai paveiktų asmens duomenų kategorijos, apytikris paveiktų arba galimai paveiktų duomenų subjektų skaičius, susijusių ar galimai susijusių asmens duomenų įrašų kategorijos ir apytikris skaičius, tikėtinos asmens duomenų saugumo pažeidimo pasekmės).

2.9 Kriterijai, kuriais siekiama įrodyti, kad yra tinkamų asmens duomenų perdavimo apsaugos priemonių

49. Kaip Valdyba patvirtino savo ankstesnėje nuomonėje, pagal sertifikavimo kriterijus reikalaujama nurodyti visus asmens duomenų perdavimo į trečiąsias valstybes ir tarptautinėms organizacijoms veiksmus, susijusius su vertinimo objektu, ir pagrįsti pasirinkimą dėl duomenų perdavimo mechanizmo, kuriuo numatomos tinkamos apsaugos priemonės pagal BDAR V skyrių (kriterijų G.10 skirsnis „Asmens duomenų perdavimas į trečiąsias valstybes arba tarptautinėms organizacijoms“).

[12] Ankstesnė EDAV nuomonė, 21 punktas.

50. EDAV pripažįsta, kad pareiškėjams pagal BDAR 3 straipsnio 2 dalį šie sertifikavimo kriterijai bus taikomi atliekant su vertinimo objektu susijusius duomenų perdavimo veiksmus, kai asmens duomenys perduodami subjektams, įsisteigusiems pareiškėjo trečiojoje valstybėje, ir subjektams, įsisteigusiems kitoje trečiojoje valstybėje.

51. Be to, Valdyba palankiai vertina tai, kad sertifikavimo kriterijai dėl asmens duomenų perdavimo labiau detalizuoti ir juose aiškiau išdėstytos pareiškėjo pareigos šiuo klausimu (kriterijų G.10.1 skirsnis „Asmens duomenų perdavimas į trečiąsias valstybes arba tarptautinėms organizacijoms“).

3 Papildomi Europos duomenų apsaugos ženklo kriterijai

52. Gairėse nustatyta, kad vertinant reikia atsakyti į klausimą, „ar kriterijai suteikia galimybę atsižvelgti į valstybių narių duomenų apsaugos teisę arba scenarijus“. Kaip patvirtinta ankstesnėje EDAV ataskaitoje, sertifikavimo kriterijų G.1.1.3 skirsnyje reikalaujama, kad pareiškėjas tokį vertinimą pateiktų nacionalinių įsipareigojimų laikymosi vertinimo ataskaitoje (angl. *National Obligations Compliance Assessment Report,* NOCAR). Tokioje ataskaitoje turi būti nagrinėjami vertinimo objektui taikomi nacionaliniai įsipareigojimai, nurodomos priemonės, kurių pareiškėjas ėmėsi, kad laikytųsi taikomų taisyklių, ir galbūt tuo metu vykdomi taisomieji veiksmai. Pareiškėjas negali naudotis sertifikavimo schemos savininko pateiktu pagrindinių papildomų nacionalinių reikalavimų sąrašu kiekvienai valstybei kaip baigtiniu nacionalinių įsipareigojimų, susijusių su vertinimo objektu, sąrašu. Pagal šią nuomonę, sertifikavimo schemos savininko pateiktas orientacinis būtiniausių papildomų patikrų ir kontrolės priemonių reikalavimų sąrašas nėra sertifikavimo kriterijus.

53. Valdyba palankiai vertina atnaujintuose kriterijuose padarytus pakeitimus, susijusius su NOCAR (G.1.1.3 skirsnis „Nacionalinių įsipareigojimų laikymosi vertinimo ataskaita“). Visų pirma, dabar juose paaiškinta, kad pareiškėjas Nacionalinių įsipareigojimų laikymosi vertinimo ataskaitoje (NOCAR) turėtų pateikti atliktą vertinimą, kurio metu tikrinama, ar duomenų tvarkymas atitinka „*pareiškėjui taikomus papildomus EEE nacionalinius įsipareigojimus dėl asmens duomenų apsaugos*“. Nacionalinių įsipareigojimų laikymosi vertinimo ataskaitoje turėtų būti nurodytas, be kita ko, aiškiai identifikuotas įvertintas vertinimo objektas, nustatytų vertinimo objektui taikomų papildomų EEE nacionalinių įsipareigojimų dėl asmens duomenų apsaugos sąrašas, taip pat vertinimo objekto atitikties nustatytiems papildomiems EEE nacionaliniams įsipareigojimams dėl asmens duomenų apsaugos įvertinimas. Valdyba mano, kad pareiškėjo, kuris yra įsisteigęs ne EEE, ir kuriam taikoma BDAR 3 straipsnio 2 dalis, atveju vertinimo objektui taikomi papildomi EEE nacionaliniai įsipareigojimai dėl asmens duomenų apsaugos turi būti nustatyti remiantis duomenų subjektų, kuriems pareiškėjas siūlo prekes ar paslaugas arba kurių elgseną jis stebi, buvimo vieta.

4 Išvados / rekomendacijos

54. Apibendrindama EDAV mano, kad „Europrivacy“ sertifikavimo kriterijai atitinka BDAR, ir patvirtina juos vadovaudamasi BDAR 70 straipsnio 1 dalies o punkte apibrėžta Valdybos užduotimi, todėl išduodamas bendras sertifikatas (Europos duomenų apsaugos ženklas).

55. EDAV mano, kad sertifikavimo kriterijai yra neatsiejama sertifikavimo schemos dalis, ir užregistruos „Europrivacy“ sertifikavimo schemą viešame sertifikavimo mechanizmų ir

duomenų apsaugos ženklų bei žymenų registre, taip pat viešai juos paskelbs pagal BDAR 42 straipsnio 8 dalį.

5 Baigiamosios pastabos

56. Ši nuomonė yra skirta Liuksemburgo priežiūros institucijai ir bus paviešinta pagal BDAR 64 straipsnio 5 dalies b punktą.

Europos duomenų apsaugos valdybos vardu

Pirmininkė

Anu Talus