

Valdybos nuomonė (64 straipsnis)



Nuomonė 19/2024 dėl „EuroPriSe“ sertifikavimo kriterijų patvirtinimo Valdyboje Europos duomenų apsaugos ženklui išduoti pagal 42 straipsnio 5 dalį (BDAR)

Priimta 2024 m. liepos 16 d.

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

Turinys

1. FAKTŲ SANTRAUKA	5
2. VERTINIMAS	6
2.1 Sertifikavimo mechanizmo taikymo sritis ir vertinimo objektas.....	6
2.2 Duomenų tvarkymo operacijos	6
2.3 Duomenų tvarkymo teisėtumas ir principai	7
2.4 Bendrosios duomenų valdytojų ir duomenų tvarkytojų prievolės	7
2.5 Duomenų subjektų teisės	7
2.6 Pavojus teisėms ir laisvei	7
2.7 Techninės ir organizacinės apsaugos užtikrinimo priemonės	7
2.8 Kriterijai, kuriais siekiama įrodyti, kad yra tinkamos asmens duomenų perdavimo apsaugos priemonės	8
3. PAPILDOMI EUROPOS DUOMENŲ APSAUGOS ŽENKLO KRITERIJAI	8
IŠVADOS / REKOMENDACIJOS	8
BAIGIAMOSIOS PASTABOS	8

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. 154/2018¹,

atsižvelgdama į savo Darbo tvarkos taisyklių 10 ir 22 straipsnius.

- (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 poreikius². Be to, nustačius sertifikavimo mechanizmus galima padidinti skaidrumą ir leisti duomenų subjektams įvertinti konkrečių produktų ir paslaugų duomenų apsaugos lygį³.
- (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 ketina siūlyti, kad EDAV patvirtintų Europos duomenų apsaugos ženklą pagal BDAR 42 straipsnio 5 dalį, ji turėtų nurodyti schemas savininko ketinimą siūlyti sertifikavimo mechanizmą visose valstybėse narėse. Šiuo atveju pagrindinis EDAV vaidmuo – užtikrinti nuoseklų BDAR taikymą taikant BDAR 63, 64 ir 65 straipsniuose nurodytą nuoseklumo užtikrinimo mechanizmą. Atsižvelgdama į tai, pagal BDAR 64 straipsnio 2 dalį EDAV tvirtina sertifikavimo kriterijus.
- (4) Šia nuomone siekiama užtikrinti nuoseklų BDAR taikymą, įskaitant priežiūros institucijų, duomenų valdytojų ir duomenų tvarkytojų nuoseklų taikymą, atsižvelgiant į pagrindinius elementus, kurie turi būti sukurti sertifikavimo mechanizmuose. 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 vertinimo gairės (toliau – papildymas), dėl kurių viešųjų konsultacijų laikotarpis baigėsi 2021 m. gegužės 26 d.
- (5) Todėl EDAV pripažįsta, kad kiekvienas sertifikavimo mechanizmas turėtų būti nagrinėjamas atskirai ir tai neturi įtakos bet kurio kito sertifikavimo mechanizmo vertinimui.
- (6) Sertifikavimo mechanizmai turėtų sudaryti sąlygas duomenų valdytojams ir duomenų tvarkytojams įrodyti, kad jie laikosi BDAR. Todėl jų kriterijai turėtų tinkamai atspindėti BDAR nustatytus asmens duomenų apsaugos reikalavimus ir principus ir padėti nuosekliai taikyti BDAR.

¹ Šioje nuomonėje minimos valstybės narės – tai EEE valstybės narės.

² BDAR 42 straipsnio 1 dalis.

³ BDAR 100 konstatuojamoji dalis.

- (7) Kartu schemos savininkas turėtų užtikrinti sertifikavimo mechanizmo suderinamumą ir atitiktį visiems įtrauktiems arba naudojamiems ISO standartams ir sertifikavimo praktikai.
- (8) Todėl sertifikavimas turėtų suteikti pridėtinės vertės duomenų valdytojams ir duomenų tvarkytojams, nes jis padeda 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 schemos savininkų pastangas parengti sertifikavimo mechanizmus, kurie yra praktinės ir potencialiai ekonomiškai efektyvios priemonės, kuriomis užtikrinamas geresnis BDAR reikalavimų laikymasis ir skatinama duomenų subjektų teisė į privatumą ir duomenų apsaugą didinant skaidrumą.
- (10) EDAV primena, kad sertifikavimas yra savanoriška atskaitomybės priemonė ir kad sertifikavimo mechanizmo reikalavimų laikymasis nesumažina duomenų valdytojų ar duomenų tvarkytojų atsakomybės už BDAR laikymąsi ir netrukdo priežiūros institucijoms vykdyti savo užduotis ir įgaliojimus pagal BDAR ir atitinkamus nacionalinės teisės aktus.
- (11) Šioje nuomonėje EDAV nagrinėja tokius klausimus, kaip kriterijų taikymo sritis, kriterijų pritaikomumas ir aktualumas visose valstybėse narėse.
- (12) Šioje nuomonėje daugiausia dėmesio skiriama sertifikavimo kriterijams. Jei EDAV reikalauja aukšto lygio informacijos apie vertinimo metodus, kad galėtų nuodugniai įvertinti galimybę atlikti kriterijų auditą savo nuomonės kontekste, pastaroji neapima jokio tokių vertinimo metodų patvirtinimo.
- (13) EDAV nuomonė priimama pagal BDAR 64 straipsnio 2 dalį, taikomą kartu su EDAV darbo tvarkos taisyklių 10 straipsnio 2 dalimi, per aštuonias savaites, skaičiuojant nuo pirmos darbo dienos, pirmininkui ir kompetentingai priežiūros institucijai priėmus sprendimą, kad dokumentų byla yra išsami. Atsižvelgiant į nagrinėjamo klausimo sudėtingumą, šį terminą pirmininko sprendimu galima pratęsti dar šešioms savaitėms. Jei EDAV nuomonėje daroma išvada, kad kriterijai negali būti patvirtinti, priežiūros institucija gali dar kartą pateikti kriterijus tvirtinti, kai bus išspręstos pirminėje EDAV nuomonėje išreikštos abejonės.

PRIĖMĖ ŠIĄ NUOMONĘ:

1. FAKTŲ SANTRAUKA

1. Pagal BDAR 42 straipsnio 5 dalį ir gaires „EuroPriSe“ duomenų tvarkytojų atliekamų duomenų tvarkymo operacijų sertifikavimo kriterijų katalogo (taikymo sritis – ES) v1.5“ (angl. *EuroPriSe Criteria Catalogue for the certification of processing operations by processors (scope: EU) v1.5*) projektą (toliau – sertifikavimo kriterijų projektas, sertifikavimo kriterijai arba kriterijai) parengė Vokietijos juridinis asmuo „EuroPriSe Cert GmbH“ (toliau – schemos savininkas) ir pateikė juos Vokietijos Šiaurės Reino-Vestfalijos kompetentingai priežiūros institucijai „Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen“ (toliau – DE-NRW priežiūros institucija).
2. 2024 m. balandžio 29 d. Vokietijos priežiūros institucija (toliau – Vokietijos PI) pateikė sertifikavimo kriterijų projektą EDAV patvirtinti pagal BDAR 64 straipsnio 2 dalį. 2024 m. gegužės 29 d. buvo priimtas sprendimas dėl dokumentų rinkinio išsamumo.

3. „EuroPriSe“ sertifikavimo mechanizmas nėra sertifikavimas pagal BDAR 46 straipsnio 2 dalies f punktą, skirtas tarptautiniam asmens duomenų perdavimui, todėl juo neužtikrinamos tinkamos apsaugos priemonės perduodant asmens duomenis į trečiąsias valstybes ar tarptautinėms organizacijoms pagal 46 straipsnio 2 dalies f punkte nurodytas sąlygas. Iš tiesų bet koks asmens duomenų perdavimas į trečiąją valstybę arba tarptautinei organizacijai gali būti vykdomas tik tuo atveju, jei laikomasi BDAR V skyriaus nuostatų.

2. VERTINIMAS

4. 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.

2.1 Sertifikavimo mechanizmo taikymo sritis ir vertinimo objektas

5. „EuroPriSe“ sertifikavimo mechanizme nustatyti ES masto duomenų tvarkytojų vykdomo duomenų tvarkymo sertifikavimo schemos sertifikavimo kriterijai. Sertifikavimo objektas, kuriam taikomas kriterijų katalogas, yra duomenų tvarkymo operacijos, atliekamos su produktais, procesais ir paslaugomis arba naudojantis (taip pat keliais) produktais ir paslaugomis, kurių atžvilgiu sertifikavimo pareiškėjas veikia kaip duomenų tvarkytojas. Pagrindiniai šio sertifikavimo mechanizmo kriterijai yra suskirstyti į tris reikalavimų grupes: teisiniu požiūriu (1 rinkinys), techninių ir organizacinių priemonių požiūriu (2 rinkinys) ir duomenų subjektų teisių požiūriu (3 rinkinys).
6. Pareiškėjai, norintys gauti sertifikatą pagal šią schemą, turi būti duomenų tvarkytojai. Tai apima duomenų tvarkytojus, kuriems duomenų valdytojas tiesiogiai pavedė tvarkyti asmens duomenis, kaip tai suprantama pagal BDAR 4 straipsnio 7 dalį. Tačiau sertifikavimo pareiškėjai taip pat gali būti duomenų tvarkytojai, kaip tai suprantama pagal BDAR 28 straipsnio 2 ir 4 dalis (pagalbiniai duomenų tvarkytojai).
7. Kai duomenų tvarkytojas, sertifikuotas pagal „EuroPriSe“ sertifikavimo sistemą, naudoja pagalbinio duomenų tvarkytojo paslaugomis, pastarasis negali teigti, kad jis buvo sertifikuotas pagal „EuroPriSe“ sertifikavimo sistemą. Tokiu atveju sertifikatas taikomas tik duomenų tvarkymo operacijoms, kurias atlieka pirminis sertifikuotas duomenų tvarkytojas. Visgi pagalbiniai duomenų tvarkytojai taip pat gali teikti sertifikavimo paraišką, o tai reikštų, kad atliekama atskira nepriklausoma procedūra.
8. Su sertifikavimo mechanizmo taikymo sritimi susijusiuose Vokietijos priežiūros institucijos pateiktuose dokumentuose Valdyba pažymi, kad „EuroPriSe“ schema taikoma Europos Sąjungoje (ES) arba Europos ekonominėje erdvėje (EEE) įsisteigusiems duomenų tvarkytojams.

2.2 Duomenų tvarkymo operacijos

9. Šie kriterijai taikomi ne tik tam tikrų rūšių duomenų tvarkymo operacijoms. Tai greičiau metodika, kuria grindžiamas „EuroPriSe“ vertinimas, leidžiantis duomenų tvarkytojams sertifikuoti bet kokias duomenų tvarkymo operacijas. Todėl tai yra universalus metodinis požiūris, kuriuo remiantis galima sertifikuoti daugybę labai skirtingų duomenų tvarkymo operacijų. Taigi labai svarbu, kad būtų laikomasi metodinių reikalavimų, nes tai vienintelis būdas užtikrinti vienodą sertifikavimo kriterijų taikymą ir panašų bandymų lygį įvairiose sertifikavimo procedūrose. Taip siekiama užtikrinti išduodamų sertifikatų ir jų rezultatų palyginamumą ir atkuriamumą.

2.3 Duomenų tvarkymo teisėtumas ir principai

10. Kriterijais reikalaujama patikrinti, ar sertifikuojamos duomenų tvarkymo operacijos atitinka pritaikytosios ir standartizuotosios duomenų apsaugos principus (kriterijų 1.5 skirsnis), o tai reiškia, kad pareiškėjas dalyvauja padedant duomenų valdytojui įgyvendinti šiuos principus. Tai leidžia įvertinti, kaip laikomasi BDAR 25 straipsnio, siejamo su BDAR 5 straipsniu. Nors nėra kriterijų, kuriais būtų tiesiogiai siekiama užtikrinti atitiktį BDAR 6 straipsniui, atsižvelgiant į tai, kad duomenų valdytojas yra atsakingas už duomenų tvarkymo teisėtumą, kriterijais siekiama užtikrinti, kad duomenų tvarkytojai pareiškėjai parengtų sertifikuojamas duomenų tvarkymo operacijas taip, kad duomenų valdytojams būtų lengviau įgyvendinti BDAR 5 straipsnio duomenų apsaugos principus, įskaitant duomenų tvarkymo teisėtumo principą.

2.4 Bendrosios duomenų valdytojų ir duomenų tvarkytojų prievolės

11. Kriterijai atspindi duomenų tvarkytojo ir duomenų valdytojo santykius. Visų pirma kriterijuose numatyta duomenų tvarkytojo pareiga parengti duomenų tvarkymo susitarimo su duomenų valdytoju šabloną, į kurį būtų įtraukti visi BDAR 28 straipsnio reikalavimai (kriterijų 1.2 skirsnis).
12. Kriterijais reikalaujama, kad pareiškėjai paskirtų duomenų apsaugos pareigūną (toliau – DAP) pagal BDAR 37 straipsnį ir pateiktų DAP paskyrimo įrodymą (pvz., paskyrimo pažymėjimą). Pagal kriterijus tikrinama, ar DAP atitinka 37–39 straipsnių reikalavimus (kriterijų 1.1 skirsnio 1 rinkinys).
13. Pagal BDAR 30 straipsnį kriterijais tikrinamas veiklos duomenų tvarkymo įrašų turinys (kriterijų 1.1 skirsnio 1 rinkinys).

2.5 Duomenų subjektų teisės

14. Kriterijais tinkamai atsižvelgiama į duomenų subjekto teisę gauti informaciją pagal BDAR III skyrių ir reikalaujama parengti atitinkamas priemones. Kriterijais taip pat reikalaujama, kad būtų įdiegtos priemonės, numatančios galimybę įsikišti į duomenų tvarkymo operaciją, kad būtų užtikrintos duomenų subjektų teisės ir sudarytos sąlygos ištaisyti, ištrinti duomenis ar apriboti jų naudojimą (kriterijų 3 rinkinys).

2.6 Pavojus teisėms ir laisvei

15. Kriterijais reikalaujama, kad duomenų tvarkytojas žinotų apie galimą pavojų fizinių asmenų teisėms ir laisvėms, susijusį su atliekamu vertinimo objekto duomenų tvarkymu. Jei dėl asmens duomenų tvarkymo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, keliais kriterijais užtikrinama, kad pareiškėjas įrodytų, jog jis atitinka BDAR 35 straipsnio reikalavimus pagal BDAR 35 straipsnį (kriterijų 1.2.2 skirsnio 6 reikalavimas, kriterijų 1.3.2 skirsnis, kriterijų 1.3.3 skirsnis, kriterijų 2.1.5.1 skirsnis, kriterijų 2.1.5.9 skirsnis).

2.7 Techninės ir organizacinės apsaugos užtikrinimo priemonės

16. Pagal kriterijus reikalaujama taikyti technines ir organizacines priemones, užtikrinančias duomenų tvarkymo operacijų konfidencialumą, vientisumą ir prieinamumą. Kriterijais taip pat reikalaujama taikyti technines priemones, skirtas pritaikytosios ir standartizuotosios duomenų apsaugos įgyvendinimui pagal BDAR 25 ir 32 straipsnius (kriterijų 1.5 skirsnis, kriterijų 2.1 skirsnis / kiti dokumentai).

17. Kriterijais reikalaujama taikyti priemonę, kuria užtikrinama, kad pareigos pranešti apie asmens duomenų saugumo pažeidimus būtų vykdomos laiku ir tinkama apimtimi pagal BDAR 33 straipsnį (kriterijų 1.2.2 skirsnio 6 reikalavimas).

2.8 Kriterijai, kuriais siekiama įrodyti, kad yra tinkamos asmens duomenų perdavimo apsaugos priemonės

18. Kriterijais reikalaujama nurodyti visus asmens duomenų perdavimus į trečiąsias valstybes ir tarptautinėms organizacijoms, susijusioms su vertinimo objektu, ir pagrįsti pasirinkimą dėl duomenų perdavimo mechanizmo, kuriuo numatomos tinkamos apsaugos priemonės pagal BDAR V skyrių (kriterijų 1.4 skirsnis).

3. PAPILDOMI EUROPOS DUOMENŲ APSAUGOS ŽENKLO KRITERIJAI

19. Gairėse nustatyta, kad vertinant reikia atsakyti į klausimą, „ar kriterijais galima atsižvelgti į valstybės narės duomenų apsaugos įstatymus arba scenarijus“. Kriterijų 4 skirsnyje reikalaujama, kad pareiškėjas laikytųsi duomenų apsaugos srityje taikomų atitinkamų konkreitiems sektoriams skirtų nacionalinės teisės aktų. Be to, Valdyba supranta, kad „atitikties nacionalinei teisei ataskaitą“, kurioje visų pirma vertinama, ar vertinimo objektas atitinka taikomus nacionalinės duomenų apsaugos teisės reikalavimus, rengia teisės ekspertai, jei šie ekspertai įrodė, kad turi reikiamą kompetencijos lygį taikytinos nacionalinės teisės srityje.

IŠVADOS / REKOMENDACIJOS

20. Apibendrindama EDAV mano, kad sertifikavimo kriterijų projektas atitinka BDAR, ir patvirtina juos vadovaudamasi BDAR 70 straipsnio 1 dalies o punkte apibrėžta Valdybos užduotimi, todėl išduodamas bendras sertifikatas (Europos duomenų apsaugos ženklas).
21. EDAV užregistruoja „„EuroPriSe“ duomenų tvarkytojų atliekamų duomenų tvarkymo operacijų sertifikavimo kriterijų katalogo“ sertifikavimo mechanizmą viešame sertifikavimo mechanizme ir duomenų apsaugos ženklų bei žymenų registre pagal 42 straipsnio 8 dalį.

BAIGIAMOSIOS PASTABOS

22. Ši nuomonė yra skirta Vokietijos Šiaurės Reino-Vestfalijos priežiūros institucijai ir bus paviėšinta pagal BDAR 64 straipsnio 5 dalies b punktą.

Europos duomenų apsaugos valdybos vardu

Pirmininkė
Anu Talus