Valdybos nuomonė (64 straipsnis)

Nuomonė 14/2020 dėl Airijos kompetentingos priežiūros institucijos sprendimo dėl sertifikavimo įstaigos akreditavimo reikalavimų tvirtinimo pagal BDAR 43 straipsnio 3 dalį projekto

Priimta 2020 m. gegužės 25 d.

Priimta

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 1 dalies c punktą, 3–8 dalis ir 43 straipsnio 3 dalį;

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 2018 m. gegužės 25 d. Darbo tvarkos taisyklių 10 ir 22 straipsnius,

kadangi:

1) pagrindinis Europos duomenų apsaugos valdybos (toliau – Valdyba) vaidmuo – užtikrinti nuoseklų Reglamento 2016/679 (toliau – BDAR) taikymą visoje Europos ekonominėje erdvėje. Laikydamasi BDAR 64 straipsnio 1 dalies, Valdyba turi pateikti nuomonę, kai priežiūros institucija ketina patvirtinti sertifikavimo įstaigų akreditavimo reikalavimus pagal 43 straipsnį. Todėl šios nuomonės tikslas – nustatyti suderintą požiūrį į reikalavimus, kuriuos duomenų apsaugos priežiūros institucija arba nacionalinė akreditavimo įstaiga taikys akredituodama sertifikavimo įstaigą. Bendras akreditavimo reikalavimų rinkinys BDAR nenustatytas, tačiau raginama laikytis nuoseklumo. Valdyba, kad šis tikslas būtų pasiektas, pirmiausia savo nuomonėse priežiūros institucijas ragina parengti akreditavimo reikalavimus pagal Valdybos Sertifikavimo įstaigų akreditavimo gairių 4/2018 1 priede pateiktą struktūrą ir, antra, analizuoja jas pagal Valdybos pateiktą šabloną – pagal jį galima atlikti lyginamąją reikalavimų analizę (remiantis ISO 17065 ir Valdybos gairėmis dėl sertifikavimo įstaigų akreditavimo);

2) pagal BDAR 43 straipsnį kompetentingos priežiūros institucijos turi patvirtinti akreditavimo reikalavimus. Tačiau jos turi taikyti nuoseklumo mechanizmą, kad būtų galima pasitikėti sertifikavimo mechanizmu, ir visų pirma jos turi nustatyti aukšto lygio reikalavimus;

3) nors akreditavimo reikalavimams turi būti taikomas nuoseklumo mechanizmas, tai nereiškia, kad reikalavimai privalo būti identiški. Kompetentingos priežiūros institucijos turi tam tikrą veiksmų laisvę, susijusią su nacionalinėmis arba regioninėmis aplinkybėmis, ir turėtų atsižvelgti į savo vietos teisės aktus. Valdybos nuomonės tikslas nėra užtikrinti, kad būtų parengtas vienas ES reikalavimų rinkinys, veikiau jos tikslas – išvengti didelio nenuoseklumo, kuris gali daryti poveikį, pavyzdžiui, pasitikėjimui akredituotų sertifikavimo įstaigų nepriklausomumu arba kompetencija;

4) taikant nuoseklumo mechanizmą kaip orientyru bus remiamasi BDAR 43 straipsnyje nurodytų sertifikavimo įstaigų akreditavimo gairėmis 4/2018 (toliau – Gairės) ir Gairėmis 1/2018 dėl sertifikavimo ir sertifikavimo kriterijų nustatymo pagal BDAR 42 ir 43 straipsnius;

5) jeigu valstybė narė nustato, kad sertifikavimo įstaigas turi akredituoti priežiūros institucija, priežiūros institucija turėtų nustatyti akreditavimo reikalavimus, įskaitant BDAR 43 straipsnio 2 dalyje nurodytus reikalavimus, bet jais neapsiribojant. Palyginti su nacionalinių akreditavimo įstaigų įsipareigojimais, susijusiais su sertifikavimo įstaigų akreditavimu, BDAR 43 straipsnyje pateikiama

[1] Šioje nuomonėje daromos nuorodos į Sąjungą turėtų būti suprantamos kaip nuorodos į EEE.

mažiau informacijos apie akreditavimo reikalavimus, kai priežiūros institucija pati vykdo akreditavimą. Siekiant padėti laikytis darnaus požiūrio į akreditavimą, priežiūros institucijos taikomi akreditavimo reikalavimai turėtų būti grindžiami ISO/IEC 17065 ir papildomi reikalavimais, kuriuos priežiūros institucija nustato pagal BDAR 43 straipsnio 1 dalies b punktą. Valdyba pažymi, kad BDAR 43 straipsnio 2 dalies a–e punktai atitinka ir tiksliai nusako ISO 17065 reikalavimus, taip užtikrinant nuoseklumą[2];

6) Valdybos nuomonė turi būti priimta pagal BDAR 64 straipsnio 1 dalies c punktą, 3 ir 8 dalis, taikomas kartu su Valdybos 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.

PRIĖMĖ ŠIĄ NUOMONĘ:

1 FAKTŲ SANTRAUKA

1. Airijos priežiūros institucija (toliau – Airijos PI), vadovaudamasi 43 straipsnio 1 dalies b punktu, Valdybai pateikė akreditavimo reikalavimų projektą. 2020 m. vasario 13 d. paskelbta, kad byla yra išsamiai parengta. Airijos nacionalinė akreditavimo įstaiga (toliau – Airijos NAĮ) akredituos sertifikavimo įstaigas pagal BDAR nustatytus sertifikavimo kriterijus. Tai reiškia, kad Airijos NAĮ, Valdybai priėmus nuomonę dėl akreditavimo reikalavimų projekto, akredituodama sertifikavimo įstaigas taikys ISO 17065 ir papildomus Airijos PI nustatytus reikalavimus (kai PI juos patvirtins).

2. Vadovaudamasis Valdybos darbo tvarkos taisyklių 10 straipsnio 2 dalimi ir atsižvelgdamas į nagrinėjamo klausimo sudėtingumą, pirmininkas nusprendė pradinį aštuonių savaičių terminą nuomonei priimti pratęsti šešiomis savaitėmis.

2 VERTINIMAS

2.1 Bendros Valdybos pastabos dėl pateikto sprendimo projekto

3. Šios nuomonės tikslas – įvertinti PI parengtus akreditavimo reikalavimus, lyginant juos su ISO 17065 arba visu reikalavimų rinkiniu, kad nacionalinė akreditavimo įstaiga arba PI pagal BDAR 43 straipsnio 1 dalį galėtų akredituoti sertifikavimo įstaigą, atsakingą už sertifikatų pagal BDAR 42 straipsnį išdavimą ir atnaujinimą. Tai nedaro poveikio kompetentingos PI užduotims ir įgaliojimams. Šiuo konkrečiu atveju Valdyba pažymi, kad Airijos PI nusprendė, jog akreditavimą vykdys nacionalinė akreditavimo įstaiga (NAĮ), ir kad PI, vadovaudamasi Gairėmis, yra parengusi papildomus reikalavimus, kuriais NAĮ vadovausis vykdydama akreditavimo procedūras.

[2] Bendrojo duomenų apsaugos reglamento 43 straipsnyje nurodytų sertifikavimo įstaigų akreditavimo gairės 4/2018, 39 punktas. Skelbiama adresu https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-42018-accreditation-certification-bodies-under_lt.

4. Vertinant Airijos PI parengtus akreditavimo reikalavimus yra siekiama išnagrinėti jų skirtumus, palyginti su Gairėmis, ypač Gairių 1 priedu (ar yra papildomų reikalavimų arba ar kai kurie reikalavimai nėra išbraukti). Valdybos nuomonėje taip pat nagrinėjami visi aspektai, kurie gali daryti poveikį sertifikavimo įstaigų vykdomo akreditavimo nuoseklumui.

5. Reikėtų atkreipti dėmesį, kad Sertifikavimo įstaigų akreditavimo gairėmis siekiama padėti priežiūros institucijoms, rengiančioms savo akreditavimo reikalavimus. Gairių priedas pats savaime nėra akreditavimo reikalavimai. Todėl sertifikavimo įstaigų akreditavimo reikalavimus PI turi apibrėžti taip, kad juos būtų galima praktiškai ir nuosekliai taikyti atsižvelgiant į PI aplinkybes.

6. Atsižvelgdama į savo patirtį, Valdyba pripažįsta, kad apibrėžiant tam tikras specialiąsias taikytinų akreditavimo reikalavimų nuostatas NAĮ turi būti suteikta tam tikra veiksmų laisvė. Tačiau, Valdybos nuomone, būtina pabrėžti, kad tais atvejais, kai nustatomi papildomi reikalavimai, jie turėtų būti suformuluoti taip, kad juos būtų galima praktiškai ir nuosekliai taikyti, o prireikus – koreguoti.

7. Valdyba pažymi, kad ISO standartai, ypač ISO 17065, yra intelektinės nuosavybės teisių objektas, todėl Valdyba šioje nuomonėje atitinkamo dokumento teksto nepateikia. Atsižvelgdama į tai, Valdyba nusprendė, prireikus, pateikti nuorodas į konkrečius ISO standarto skirsnius, tačiau paties jų teksto necituoti.

8. Galiausiai pažymėtina, kad atlikdama vertinimą Valdyba rėmėsi Gairių 1 priede (toliau – priedas) nustatyta struktūra. Jeigu dėl kurių nors Airijos PI akreditavimo reikalavimų projekto skirsnių Nuomonėje pastabų nepateikta, vadinasi, Valdyba dėl jų pastabų neturi ir neprašo, kad Airijos PI imtųsi tolesnių veiksmų.

9. Airijos PI pateikta informacija, nepatenkanti į BDAR 43 straipsnio 2 dalies taikymo sritį, pavyzdžiui, nuorodos į nacionalinės teisės aktus, šioje nuomonėje nenagrinėjama. Tačiau Valdyba pažymi, kad, kai to reikalaujama, nacionalinės teisės aktai turėtų atitikti BDAR.

2.2 Pagrindiniai vertinami aspektai (BDAR 43 straipsnio 2 dalis ir Valdybos gairių 1 priedas), įtraukti į akreditavimo reikalavimus, kad būtų galima nuosekliai įvertinti:

1) dėmesys visoms pagrindinėms sritims, pabrėžtoms Gairių priede, ir tikrinimas, ar nenukrypta nuo Priedo;

2) sertifikavimo įstaigos nepriklausomumas;

3) sertifikavimo įstaigos interesų konfliktai;

4) sertifikavimo įstaigos kompetencija;

5) tinkamos apsaugos priemonės siekiant užtikrinti, kad sertifikavimo įstaiga tinkamai taikytų BDAR sertifikavimo kriterijus;

6) pagal BDAR išduodamo sertifikato išdavimas, periodinis peržiūrėjimas ir panaikinimas;

7) skaidrus skundų dėl sertifikavimo pažeidimų nagrinėjimas.

10. Atsižvelgdama į tai, kad:

a. BDAR 43 straipsnio 2 dalyje išvardytos akreditavimo sritys, kurias sertifikavimo įstaiga turi apimti, kad būtų akredituota;

b. BDAR 43 straipsnio 3 dalyje nustatyta, kad sertifikavimo įstaigų akreditavimo reikalavimai turi būti patvirtinti kompetentingos priežiūros institucijos;

c. BDAR 57 straipsnio 1 dalies p ir q punktuose nustatyta, kad kompetentinga priežiūros institucija turi parengti ir paskelbti sertifikavimo įstaigų akreditavimo reikalavimus ir gali nuspręsti pati atlikti sertifikavimo įstaigų akreditavimą;

d. BDAR 64 straipsnio 1 dalies c punkte nustatyta, kad Valdyba turi pateikti nuomonę, kai priežiūros institucija ketina tvirtinti sertifikavimo įstaigos akreditavimo reikalavimus pagal 43 straipsnio 3 dalį,

e. jeigu akreditavimą pagal ISO/IEC 17065/2012 vykdo nacionalinė akreditavimo įstaiga, taip pat turi būti taikomi kompetentingos priežiūros institucijos nustatyti papildomi reikalavimai;

f. Sertifikavimo įstaigų akreditavimo gairių 1 priede pasiūlyta, kokius reikalavimus duomenų apsaugos priežiūros institucija turi parengti, o nacionalinė akreditavimo įstaiga taikyti akredituodama sertifikavimo įstaigas.

Valdyba laikosi tokios nuomonės:

2.2.1 ĮŽANGA (Airijos PI akreditavimo reikalavimų projekto 0 skyrius)

11. Valdyba pripažįsta, kad bendradarbiavimo sąlygos, kuriomis apibrėžiamas nacionalinės akreditavimo įstaigos ir jos duomenų apsaugos priežiūros institucijos ryšys, *per se* nėra sertifikavimo įstaigų akreditavimo reikalavimas. Tačiau Valdyba mano, kad dėl išsamumo ir skaidrumo bendradarbiavimo sąlygas, jei jos nustatomos, reikia paskelbti PI nuomone tinkamu formatu.

2.2.2 TERMINAI IR APIBRĖŽTYS

12. Valdyba atkreipia dėmesį, kad akreditavimo gairių nuoroda yra neatnaujinta (nurodyta „WP 261“). Valdyba patvirtino BDAR 43 straipsnyje nurodytų sertifikavimo įstaigų akreditavimo gaires 4/2018. Todėl Valdyba Airijos priežiūros instituciją ragina iš dalies pakeisti formuluotę ir nurodyti Gaires 4/2018.

2.2.3 BENDRO POBŪDŽIO PASTABOS

13. Valdyba atkreipia dėmesį, kad Airijos PI reikalavimų projekte pakartotinai nurodoma „kompetentinga priežiūros institucija“. Kadangi šiuo atveju kompetentinga PI yra Airijos PI, Valdyba Airijos priežiūros instituciją ragina šią nuorodą pakeisti ir vartoti „DAK“ (duomenų apsaugos koordinatorius) arba „Airijos PI“, kad būtų išvengta painiavos.

14. Valdyba palankiai vertina tai, kad Airijos PI reikalavimų projekte yra terminų ir apibrėžčių skyrius. Tačiau keli terminai dokumente vartojami nenuosekliai (pvz., „object of evaluation“ ir „ToE“). Kad būtų išvengta painiavos, Valdyba Airijos priežiūros instituciją ragina reikalavimų projekte vartoti vienodus terminus.

2.2.4 BENDRIEJI AKREDITAVIMO REIKALAVIMAI (papildomų akreditavimo reikalavimų projekto 4 skyrius)

15. Kalbant apie Airijos PI akreditavimo reikalavimų projekto 4.1.2 skirsnio 7 punktą, Valdyba mano, kad jo formuluotė šiek tiek neaiški, t. y. neaišku, kam nurodomos sertifikavimo patvirtinimo priežastys. Be to, taip pat neaišku, ką reiškia „palengvinti“ (angl. *facilitating*) registrą. Todėl Valdyba Airijos priežiūros instituciją ragina pakeisti formuluotę taip, kad ji būtų aiškesnė.

2.2.5 STRUKTŪRINIAI REIKALAVIMAI (akreditavimo reikalavimų projekto 5 skyrius)

16. Valdyba atkreipia dėmesį, kad Airijos PI akreditavimo reikalavimų projekte nurodyta, jog skiriamas „tinkamo vyresnumo asmuo, atsakingas už priežiūrą, kaip laikomasi duomenų apsaugos ir informacijos valdymo reikalavimų“. „Tinkamas vyresnumas“ turėtų būti aiškiau įvardytas – nurodant patirtį ir įgaliojimų apimtį. Be to, atrodo, kad šio asmens funkcijos yra panašios į duomenų apsaugos pareigūno funkcijas. Valdyba Airijos priežiūros instituciją ragina aiškiai nustatyti šio asmens funkcijas ir nurodyti reikiamą patirtį.

2.2.6 REIKALAVIMAI DĖL IŠTEKLIŲ (akreditavimo reikalavimų projekto 6 skyrius)

17. Kalbant apie sertifikavimo įstaigos darbuotojus (6.1 skirsnis), Valdyba atkreipia dėmesį, kad techninės kompetencijos darbuotojų, atsakingų už sprendimų priėmimą, reikalavimai apima bent 5 metų profesinę patirtį, susijusią su sertifikavimo dalyku, o darbuotojai, atsakingi vertinimą, turėtų turėti bent 2 metų profesinę patirtį. Panašiai, teisinės kompetencijos darbuotojai, priimantys sprendimus, privalo turėti bent 5 metų profesinę patirtį, o už vertinimus atsakingi darbuotojai – bent 2 metų patirtį. Valdyba atkreipia dėmesį, kad reikalaujama mažiausia darbuotojų, atsakingų už sprendimų priėmimą, ir darbuotojų, atsakingų už vertinimą, profesinė patirtis, nurodoma metais, labai skiriasi. Šiuo atžvilgiu Valdyba mano, kad turėtų būti pabrėžiama skirtingos rūšies kompetencija, o ne profesinė patirtis, nurodoma metų skaičiumi. Valdybos nuomone, vertintojai turėtų turėti labiau specializuotos patirties, taip pat su techninėmis procedūromis susijusios profesinės patirties (pvz., audito ir sertifikavimo), o sprendimų priėmėjai turėtų turėti bendresnės ir išsamesnės patirties, taip pat su duomenų apsauga susijusios profesinės patirties. Atsižvelgdama į tai Valdyba Airijos priežiūros institucijai rekomenduoja labiau akcentuoti skirtingas esmines vertintojų ir sprendimų priėmėjų žinias ir (arba) patirtį, bei sumažinti iš jų reikalaujamos patirties metų skirtumą.

2.2.7 PROCESO REIKALAVIMAI (akreditavimo reikalavimų projekto 7 skyrius)

18. Kalbant apie Airijos PI akreditavimo reikalavimų projekto 7.10 skirsnį („Pakeitimai, darantys poveikį sertifikavimui“), Valdyba atkreipia dėmesį, kad nenurodytos pakeitimų procedūros, dėl kurių reikia susitarti, remiantis priedo 7.10 skirsniu). Valdyba Airijos priežiūros instituciją ragina įtraukti tokią nuorodą ir paminėti kelias procedūras, kurias būtų galima įdiegti (pvz., pereinamieji laikotarpiai, tvirtinimo kompetentingoje PI procesas ir pan.). Be to, Valdyba mano, kad pažangiausių metodų pakeitimai taip pat aktualūs ir gali daryti poveikį sertifikavimui. Todėl Valdyba Airijos priežiūros instituciją ragina šią galimybę įtraukti į pakeitimų, darančių poveikį sertifikavimui, sąrašą. Galiausiai, Valdyba palankiai vertina tai, kad į pakeitimų, galinčių daryti poveikį sertifikavimui, sąrašą įtraukti asmens duomenų saugumo pažeidimai, taip pat BDAR pažeidimai. Tačiau, aiškumui užtikrinti Valdyba Airijos priežiūros instituciją ragina nurodyti, kad į duomenų saugumo pažeidimus arba BDAR pažeidimus atsižvelgiama tik tiek, kiek jie susiję su sertifikavimu.

19. Kalbant apie pakeitimus, darančius poveikį sertifikavimui (Airijos PI reikalavimų projekto 7.10 skirsnis), ir visų pirma apie penktą įtrauką, Valdyba atkreipia dėmesį, kad Airijos PI nurodo „taikytinus privalomus Europos duomenų apsaugos valdybos sprendimus“ ir taip pat Valdybos darbo tvarkos taisyklių 39 straipsnį – jame nurodyta „visi galutiniai EDAV patvirtinti dokumentai“. Kad būtų aišku, ką reiškia „Europos duomenų apsaugos valdybos sprendimai“, Valdyba Airijos priežiūros instituciją ragina šį žodžių junginį patikslinti. Pavyzdžiui, būtų galima rašyti „Europos duomenų apsaugos valdybos priimti dokumentai“ (angl. *documents adopted by the European Data Protection Board*).

20. Valdyba atkreipia dėmesį, kad Airijos priežiūros institucijos reikalavimų projekto 7.11 skirsnyje (sertifikato galiojimo nutraukimas, sutrumpinimas, sustabdymas arba panaikinimas) nenustatyta sertifikavimo įstaigos prievolė sutikti su Airijos PI sprendimais ir nurodymais panaikinti sertifikatą arba pareiškėjui neišduoti sertifikato, jeigu nesilaikoma arba nebesilaikoma sertifikavimo reikalavimų. Todėl Valdyba Airijos priežiūros institucijai rekomenduoja tokią prievolę įtraukti.

3 IŠVADOS IR (ARBA) REKOMENDACIJOS

21. Taikant Airijos priežiūros institucijos parengtus akreditavimo reikalavimus gali atsirasti sertifikavimo įstaigų akreditavimo nuoseklumo spragų, tad reikalingi toliau nurodyti pakeitimai.

22. Kalbant apie su procesu susijusius reikalavimus, Valdyba Airijos priežiūros institucijai rekomenduoja:

1) 7.11 skirsnyje nustatyti sertifikavimo įstaigos prievolę sutikti su Airijos PI sprendimais ir nurodymais panaikinti sertifikatą arba pareiškėjui neišduoti sertifikato, jeigu nesilaikoma arba nebesilaikoma sertifikavimo reikalavimų.

4 BAIGIAMOSIOS PASTABOS

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

24. Pagal BDAR 64 straipsnio 7 ir 8 dalis priežiūros institucija elektroninėmis priemonėmis per dvi savaites nuo nuomonės gavimo praneša pirmininkui, ar iš dalies pakeis sąrašo projektą, ar paliks jį nepakeistą. Per tą patį laikotarpį ji pateikia iš dalies pakeistą sąrašo projektą arba, jeigu neketina atsižvelgti į Valdybos nuomonę, nurodo atitinkamą pagrindą, kodėl neketina laikytis nuomonės ar jos dalies.

25. Airijos priežiūros institucija perduoda galutinį sprendimą Valdybai, kad jis būtų įtrauktas į sprendimų, kuriems taikomas nuoseklumo mechanizmas, registrą, kaip nustatyta BDAR 70 straipsnio 1 dalies y punkte.

Europos duomenų apsaugos valdybos vardu

Pirmininkė

(Andrea Jelinek)

Priimta