Valdybos nuomonė (64 straipsnis)

Nuomonė 15/2020 dėl Vokietijos kompetentingų priežiūros institucijų sprendimo dėl sertifikavimo įstaigos akreditavimo reikalavimų patvirtinimo pagal BDAR 43 straipsnio 3 dalį projekto

Priimta 2020 m. gegužės 25 d.

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

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 Valdybos 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 (PI) 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 Bendrojo duomenų apsaugos reglamento (2016/679) 43 straipsnyje nurodytų sertifikavimo įstaigų akreditavimo gairėmis 4/2018 (toliau – Gairės) ir Gairėmis 1/2018 dėl sertifikavimo ir sertifikavimo kriterijų nustatymo pagal Bendrojo duomenų apsaugos reglamento 42 ir 43 straipsnius;

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

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

įsipareigojimais, susijusiais su sertifikavimo įstaigų akreditavimu, 43 straipsnyje pateikiama mažiau informacijos dėl akreditavimo reikalavimų, 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 43 straipsnio 1 dalies b punktą. Valdyba pažymi, kad 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 rinkinys yra išsamus. Atsižvelgiant į nagrinėjamo klausimo sudėtingumą, šį terminą pirmininko sprendimu galima pratęsti dar šešioms savaitėms,

PRIĖMĖ ŠIĄ NUOMONĘ:

1 FAKTŲ SANTRAUKA

1. Vokietijos federacinės ir žemių priežiūros institucijos (toliau – Vokietijos PI), vadovaudamosi 43 straipsnio 1 dalies b punktu, Valdybai pateikė akreditavimo reikalavimų projektą. 2020 m. vasario 13 d. paskelbta, kad dokumentų rinkinys yra išsamiai parengtas. Vokietijos nacionalinė akreditavimo įstaiga (toliau – NAĮ), DAkkS, akredituos sertifikavimo įstaigas pagal BDAR nustatytus sertifikavimo kriterijus. Tai reiškia, kad NAĮ, Valdybai priėmus nuomonę dėl akreditavimo reikalavimų projekto, akredituodama sertifikavimo įstaigas taikys ISO 17065 ir papildomus Vokietijos 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 Vokietijos priežiūros institucijos nusprendė, jog akreditavimą kartu vykdys nacionalinė akreditavimo įstaiga (NAĮ), DAkkS ir kompetentinga priežiūros institucija, kurios. vadovaudamosi Gairėmis, yra parengusios papildomus reikalavimus, taikytinus vykdant akreditavimo procedūras.

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

4. Vertinant Vokietijos priežiūros institucijos parengtus papildomus akreditavimo reikalavimus yra siekiama išnagrinėti jų skirtumus (ar yra papildomų ar pašalintų reikalavimų), palyginti su Gairėmis, ypač Gairių 1 priedu. Valdybos nuomonėje taip pat nagrinėjami visi aspektai, kurie gali daryti poveikį sertifikavimo įstaigų vykdomo akreditavimo nuoseklumui.

5. Reikėtų atkreipti dėmesį, kad Gairėmis dėl sertifikavimo įstaigų akreditavimo siekiama padėti PI, šioms rengiant 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 ir kompetentingoms PI, kai taikytina, 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 Vokietijos PI akreditavimo reikalavimų projekto skirsnių Nuomonėje pastabų nepateikta, vadinasi, Valdyba dėl jų pastabų neturi ir neprašo, kad Vokietijos PI imtųsi tolesnių veiksmų.

9. Vokietijos 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 Svarbiausi akreditavimo reikalavimuose nustatyti vertinimo dalykai (BDAR 43 straipsnio 2 dalis ir Valdybos gairių 1 priedas), kad būtų užtikrintas nuoseklus vertinimas:

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

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 pažymi, kad Vokietijos PI akreditavimo reikalavimų projekto 3 skyriuje („Apibrėžtys”) nustatyta, kokios sertifikavimo schemos yra leidžiamos, nurodant, kad jos turi atitikti standarto DIN EN ISO/IEC 17065 reikalavimus. Šiuo atžvilgiu reikėtų pažymėti, kad Valdybos gairių 5.1 ir 5.2 skirsniuose jau išsamiai išdėstyta, ką galima patvirtinti pagal BDAR. Todėl Valdyba pripažįsta, kad Vokietijos PI tikslas nėra apriboti Gairėse nurodytų dalykų ir kad Vokietijos PI akreditavimo reikalavimų projekto 3 skyriuje pateikti teiginiai turi būti laikomi taikytinais atsižvelgiant į šiuos akreditavimo reikalavimus.

2.2.3 BENDRO POBŪDŽIO PASTABOS

13. Valdyba pažymi, kad Vokietijos PI akreditavimo reikalavimų projekto „bendrųjų pastabų“ skirsnyje daroma nuoroda į Valdybos „leidimą“ taikyti sertifikavimo kriterijus „pagal BDAR 63 straipsnį ir 64 straipsnio 1 dalies c punktą“. Valdyba pažymi, kad BDAR nesuteikia Valdybai kompetencijos „leisti“ taikyti sertifikavimo kriterijus. Tačiau pagal pirmiau minėtus straipsnius Valdyba gali patvirtinti sertifikavimo kriterijus. Todėl Valdyba rekomenduoja Vokietijos PI išbraukti nuorodą į „Valdybos leidimą”, kad projektas atitiktų BDAR formuluotę.

2.2.4 BENDRIEJI AKREDITAVIMO REIKALAVIMAI (akreditavimo reikalavimų projekto 4 skyrius)

14. Dėl teisinės atsakomybės reikalavimo (Vokietijos PI akreditavimo reikalavimų projekto 4.1 punktas) Valdyba pažymi, kad patvirtinamajame dokumente Vokietijos PI paaiškina, jog tikimasi, kad sertifikavimo įstaigos procedūros bus atnaujintos ir todėl papildomų reikalavimų šiuo klausimu nereikia. Tačiau Valdyba mano, kad lūkesčiai neįpareigoja sertifikavimo įstaigų taikyti tokias procedūras. Kaip nustatyta Gairių priedo 4.1.1 punkte, sertifikavimo įstaigos turi turėti atnaujintas procedūras, kad įrodytų atitiktį akreditavimo sąlygose nustatytoms teisinėms pareigoms. Be to, sertifikavimo įstaiga turi sugebėti įrodyti, jog turi BDAR atitinkančias procedūras ir priemones, konkrečiai skirtas kliento organizacijos asmens duomenims valdyti ir tvarkyti sertifikavimo proceso metu. Todėl Valdyba rekomenduoja Vokietijos PA iš dalies pakeisti reikalavimų projektą, kad jis atitiktų Gaires.

15. Dėl Vokietijos PI akreditavimo reikalavimų projekto 4.1.2.2 punkto (toliau – sertifikavimo susitarimas) Valdyba pažymi, kad Vokietijos PI akreditavimo reikalavimų projekte nenumatyta prievolė užtikrinti visišką sertifikavimo procedūros, įskaitant konfidencialius sutartinius klausimus, skaidrumą kompetentingai PI. Be to, neminima pareiškėjo pareiga suteikti sertifikavimo įstaigai galimybę susipažinti su jo vykdoma tvarkymo veikla. Todėl Valdyba Vokietijos PI rekomenduoja tokias prievoles įtraukti į projektą.

16. Valdyba pažymi, kad Vokietijos PI akreditavimo reikalavimų projekto 4.1.2.2 punkte nėra aiškiai užsimenama apie kompetentingos PI užduotis ir įgaliojimus (priedo 4.1.2 punkto trečioji įtrauka). Valdyba mano, kad tokia nuoroda turėtų būti įtraukta į reikalavimų projektą, todėl ji rekomenduoja Vokietijos PI atitinkamai iš dalies pakeisti projektą.

17. Be to, Vokietijos reikalavimų projekto nuostatose dėl sertifikavimo susitarimo nėra įpareigojimo leisti sertifikavimo įstaigai atskleisti visą informaciją, reikalingą sertifikavimui pagal BDAR 42 straipsnio 8 dalį ir 43 straipsnio 5 dalį (priedo 4.1.2 punkto 7 įtrauka). Nors šis įpareigojimas įtrauktas į Vokietijos PI akreditavimo reikalavimų projekto proceso valdymo skirsnį, Valdyba mano, kad jis turėtų būti įtrauktas į sertifikavimo susitarimą, kad būtų sustiprintas jo privalomas pobūdis. Todėl Valdyba rekomenduoja Vokietijos PI įtraukti pirmiau minėtą įpareigojimą kaip sertifikavimo susitarimo dalį.

18. Pagal priedą pareiškėjas turi informuoti sertifikavimo įstaigą apie reikšmingus faktinės ar teisinės padėties ir sertifikuojamų jo produktų, procesų ir paslaugų pokyčius (priedo 4.1.2 punkto dešimta įtrauka). Tačiau Vokietijos PI akreditavimo reikalavimų projekto 4.1.2.2 punkto 6 įtrauka apima tik įpareigojimą informuoti sertifikavimo įstaigą apie reikšmingus faktinių ar teisinių aplinkybių pasikeitimus, tačiau joje aiškiai neminimi produktai, procesai ir paslaugos. Valdyba rekomenduoja Vokietijos PI traukti tokią nuorodą pagal priedo reikalavimus.

19. Dėl Vokietijos PI akreditavimo reikalavimų projekto 4.2.7 punkto („Nešališkumo valdymas”) Valdyba rekomenduoja sugriežtinti sertifikavimo įstaigoms, kurios priklauso atskiram juridiniam asmeniui arba yra jo kontroliuojamos, taikomus kriterijus, kad būtų atsižvelgta į tai, jog bet kokie ekonominiai sertifikavimo įstaigos ir juridinio asmens santykiai, priklausomai nuo jų savybių, gali turėti įtakos sertifikavimo veiklos nešališkumui.

20. Dėl Vokietijos PI akreditavimo reikalavimų projekto 4.6 punkto („viešai skelbiama informacija”) Valdyba pažymi, kad jame nėra užsimenama apie priimtų kriterijų ir sertifikavimo procedūrų visų versijų paskelbimą. Todėl Valdyba ragina Vokietijos PI iš dalies pakeisti akreditavimo reikalavimų projektą, kad būtų aiškiai nurodyta, jog skelbiamos visos patvirtintų kriterijų ir sertifikavimo procedūrų versijos. Be to, Valdyba pažymi, kad 4.6 punkto antroje pastraipoje teigiama, jog „sertifikavimo

schemos, kurias naudoja sertifikavimo įstaiga, kriterijai, patvirtinti pagal BDAR 42 straipsnio 5 dalį, nurodantys leistiną taikymo trukmę, *paprastai turėtų būti skelbiami*." Kad būtų išvengta dviprasmybių, Valdyba ragina Vokietijos PI išbraukti žodį „paprastai" ir įrašyti jungtuką „ir" tarp žodžių „įstaiga" ir „kriterijai".

2.2.5 REIKALAVIMAI DĖL IŠTEKLIŲ (akreditavimo reikalavimų projekto 6 skyrius)

21. Dėl kompetencijos reikalavimų ir konkrečiai Vokietijos PI akreditacijos reikalavimų projekto 6.1.2.1 punkto („Žmogiškųjų išteklių kompetencija") Valdyba pažymi, kad reikalavimuose dėl žinių turėjimo išvardytose srityse nenurodyta, kad žinios turi būti reikiamos ir tinkamos. Siekdama užtikrinti suderinamumą su priede reikalaujamu kompetencijos lygiu, Valdyba rekomenduoja Vokietijos PI suderinti formuluotę su Gairėmis, reikalaujant, kad žinios būtų reikiamos ir tinkamos.

22. Be to, Valdyba pažymi, kad už sprendimų priėmimą atsakingi techninę kompetenciją turintys darbuotojai turi turėti ne trumpesnę kaip 7 metų profesinę patirtį arba 5 metų profesinę patirtį techninės duomenų apsaugos srityje, atsižvelgiant į jų išsilavinimo lygį, o už vertinimus atsakingi darbuotojai turi turėti 4 metų profesinę patirtį arba 2 metų profesinę patirtį techninės duomenų apsaugos srityje ir bandymų procedūros patirtį, atsižvelgiant į jų išsilavinimo lygį. Analogiškai, sprendimus priimantys teisinę kompetenciją turintys darbuotojai privalo turėti bent 5 metų duomenų apsaugos teisės profesinę patirtį, o už vertinimus atsakingi darbuotojai – bent 2 metų patirtį duomenų apsaugos teisės ir audito procedūrų srityse. 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 vertintojams ir sprendimus priimantiems asmenims keliami kompetencijos reikalavimai turėtų būti pritaikyti atsižvelgiant į skirtingas jų atliekamas užduotis, o ne į patirties metų skaičių. 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 visapusiškos patirties, taip pat su duomenų apsauga susijusios profesinės patirties. Atsižvelgdama į tai, Valdyba Vokietijos PI rekomenduoja labiau akcentuoti skirtingas esmines vertintojų ir sprendimų priėmėjų žinias ir (arba) patirtį, bei sumažinti iš jų reikalaujamų patirties metų skaičiaus skirtumus.

23. Be to, Valdyba mano, kad su sertifikavimo sritimi susijusių valdymo sistemų žinios turėtų apimti ir standartą ISO/IEC 27701:2019 „Saugumo metodai – ISO/IEC 27001 ir ISO/IEC 27002 papildymas dėl privatumo valdymo – reikalavimai ir gairės", ir ragina Vokietijos PI įtraukti tokią nuorodą.

24. Galiausiai dėl techninio personalo išsilavinimo reikalavimų Valdyba mano, kad dalykų sąrašas jau parengtas atsižvelgiant į techninę kompetenciją, kurios reikalaujama priede. Todėl Valdyba ragina Vokietijos PI iš dalykų, susijusių su techninio personalo universitetiniu švietimu, sąrašo išbraukti „gamtos mokslus".

2.2.6 PROCEDŪRINIAI REIKALAVIMAI (akreditavimo reikalavimų projekto 7 skyrius)

25. Valdyba pažymi, kad Vokietijos PI akreditavimo reikalavimų projekto 7 skyriuje keletą kartų paminėti „jos kriterijai" (pvz., 7.4, 7.6, 7.11 ir 7.13 punktuose). Siekdama išvengti bet kokių dviprasmybių, Valdyba ragina Vokietijos PI patikslinti tokio termino reikšmę, pavyzdžiui, pridedant paaiškinimą 1 priede (Žodynėlis).

26. Dėl Vokietijos PI akreditavimo reikalavimų projekto 7.1 punkto („Bendroji informacija”) Valdyba pažymi, kad nėra aiškiai nurodyta sertifikavimo įstaigos pareiga laikytis papildomų reikalavimų. Nors toks įpareigojimas galėtų būti numanomas pagal reikalavimų projekto tekstą, Valdyba mano, kad tokią pareigą reikėtų aiškiai nurodyti. Todėl Valdyba rekomenduoja Vokietijos PI projektą atitinkamai iš dalies pakeisti.

27. Valdyba pažymi, kad Vokietijos PI papildomų reikalavimų projekte neminimas patvirtinto Europos duomenų apsaugos ženklo naudojimas, kaip nurodyta priedo 7.1.2 punkte. Valdyba mano, kad apie tai turėtų būti nurodyta, ypač atsižvelgiant į tai, kad sertifikavimo įstaigos, suteikiančios Europos duomenų apsaugos ženklus, akreditavimas gali būti atliekamas kiekvienoje valstybėje narėje, kurioje įsisteigusi sertifikavimo įstaiga[3]. Todėl Valdyba rekomenduoja Vokietijos PI minėto ženklo naudojimą paminėti. Pavyzdžiui, reikalavimų projekte galėtų būti nurodyta: *„Kompetentingą PI informuojama prieš sertifikavimo įstaigai pradedant naudoti patvirtintą Europos duomenų apsaugos ženklą jos padalinyje naujoje valstybėje narėje".*

28. Valdyba pažymi, kad Vokietijos PI akreditavimo reikalavimų projekto 7.2 punkte („Paraiška”) numatyta situacija, kai duomenų tvarkytojai naudojami duomenų tvarkymo operacijoms atlikti pagal Gairių priedą. Tačiau Valdyba pažymi, kad kai naudojami duomenų tvarkytojai, paraiškoje pateikiama atitinkama (-os) duomenų valdytojo (tvarkytojo) sutartis (-ys), kaip nurodyta priede. Todėl Valdyba rekomenduoja Vokietijos PI suderinti formuluotę su gairėmis įtraukiant nuorodą į duomenų valdytojo (tvarkytojo) sutartį (-is). Be to, Valdyba ragina Vokietijos PI apsvarstyti, ar šiuo atveju taip pat reikėtų nuorodos į bendrus duomenų valdytojus ir jų konkrečius susitarimus.

29. Valdyba pažymi, kad Vokietijos PI akreditavimo reikalavimų projekto 7.2 punkte nurodyta, kad „duomenų valdytojas ir duomenų tvarkytojas turi teisę kreiptis dėl sertifikavimo”. Duomenų valdytojų galimybė kreiptis dėl sertifikavimo priklausys nuo konkrečios sertifikavimo schemos. Todėl, siekdama išvengti painiavos, Valdyba ragina Vokietijos PI išbraukti pirmiau minėtą nuorodą arba paaiškinti, kad duomenų tvarkytojų sertifikavimo galimybės priklausys nuo sertifikavimo schemos taikymo srities.

30. Dėl Vokietijos PI akreditavimo reikalavimų projekto 7.3 punkto („Vertinimo paraiškos”) Valdyba pažymi, kad Vokietijos PI akreditavimo reikalavimų projekte teigiama, jog „planuojami vertinimo metodai yra numatyti sutartyje <... >”. Idant būtų aišku, kad tai yra reikalavimas, Valdyba skatina Vokietijos PI performuluoti pirmąją pastraipą, kad būtų aišku, jog vertinimo metodai turi būti įtraukti į sertifikavimo susitarimą, pvz., šią nuostatą suformuluoti taip: „planuojami vertinimo metodai turi būti nustatyti sutartyje [...]”. Be to, Valdyba ragina Vokietijos PI pakeisti nuorodą į standarto ISO 17065 7.3.1.b punktą nuoroda į standarto ISO 17065 7.3 punktą, siekiant suderinti formuluotę su priedu. Be to, Valdyba pažymi, kad ketvirtoje pastraipoje kalbama apie tinkamą techninę ir teisinę kompetenciją. Aiškumo dėlei Valdyba skatina Vokietijos PI pridėti frazę „duomenų apsaugos srityje”.

31. Valdyba pastebi, kad Vokietijos PI akreditacijos reikalavimų projekto 7.4 punkte („vertinimo metodai”) nenumatyta sertifikavimo įstaigos pareiga aprašyti pakankamus vertinimo metodus, kad būtų galima įvertinti duomenų tvarkymo operacijos (-ų) atitiktį sertifikavimo kriterijams. Valdyba rekomenduoja Vokietijos PI iš dalies pakeisti reikalavimų projektą, kad jame būtų nurodyta minėta pareiga. Pavyzdžiui, galima naudoti tokią formuluotę: *„Sertifikavimo įstaiga užtikrina, kad sertifikavimo mechanizmuose būtų aprašyti pakankami vertinimo metodai, skirti įvertinti, ar duomenų tvarkymo operacija (-os) atitinka sertifikavimo kriterijus*". Be to, kalbant apie pirmąją sritį, kuriai bus taikomi vertinimo metodai, Valdyba mano, kad būtinybė ir proporcingumas turi būti vertinami ir atitinkamų

[3] Šiuo klausimu žr. Gairių Nr. 1/2018 44 punktą.

duomenų subjektų atžvilgiu, kai taikytina. Galiausiai Valdyba pažymi, kad nėra paminėtas metodų ir išvadų dokumentavimas. Valdyba ragina Vokietijos PI iš dalies pakeisti reikalavimų projektą, kad tai būtų aiškiai nurodyta.

32. Dėl esamų sertifikatų (Vokietijos PI akreditavimo reikalavimų projekto 7.4 punktas) Valdyba mano, kad 13 puslapyje esanti 4 įtrauka kelia painiavą, nes neaišku, koks ryšys tarp dabartinio ir ankstesnio sertifikavimo galiojimo laikotarpių ir kaip jie derėtų tarpusavyje. Be to, vargu, ar praktiškai įmanoma kelti klausimą dėl kitos akredituotos sertifikavimo įstaigos anksčiau išduoto sertifikavimo galiojimo. Apibendrinant galima teigti, kad pastraipoje reikėtų daugiau aiškumo dėl įvairių paminėtų elementų santykio. Valdyba rekomenduoja Vokietijos PI iš dalies pakeisti projektą, visų pirma paaiškinant, kad BDAR numatyto sertifikato galiojimo trukmė neturi priklausyti nuo kitų tipų sertifikatų galiojimo.

33. Kalbant apie Vokietijos PI akreditavimo reikalavimų projekto 7.5 punktą („Vertinimas"), Valdyba ragina Vokietijos PI pakeisti jo pavadinimą į „Peržiūra".

34. Dėl sertifikavimui įtakos turinčių pakeitimų (Vokietijos PI akreditavimo reikalavimų projekto 7.10 punktas) Valdyba pažymi, kad Vokietijos PI akreditavimo reikalavimų projekte nustatyta, kad „klientas laiku informuojamas apie jam įtakos turinčius teisinės sistemos pakeitimus". Atsižvelgdama į poreikį išsaugoti sertifikavimo įstaigos nešališkumą, Valdyba ragina Vokietijos PI performuluoti sakinį, kad būtų aišku, jog klientui laiku pateikiama bendra informacija apie pokyčius, kurie jam gali turėti įtakos. Tačiau siekiant užtikrinti, kad būtų aišku, ką reiškia „Europos duomenų apsaugos valdybos sprendimai", Valdyba ragina Vokietijos PI šį žodžių junginį patikslinti. Pavyzdžiui, būtų galima rašyti „Europos duomenų apsaugos valdybos priimti dokumentai".

35. Valdyba atkreipia dėmesį, kad Vokietijos PI akreditavimo reikalavimų projekto 7.11 punkte („Sertifikato galiojimo nutraukimas, apribojimas, sustabdymas arba panaikinimas") nenustatyta sertifikavimo įstaigos prievolė sutikti su Vokietijos sprendimais ir nurodymais panaikinti sertifikatą arba neišduoti sertifikato pareiškėjui, jeigu nesilaikoma arba nebesilaikoma sertifikavimo reikalavimų. Todėl Valdyba Vokietijos priežiūros institucijai rekomenduoja tokią prievolę įtraukti. Be to, Valdyba skatina Vokietijos PI punkto antraštėje žodį „apribojimas" pakeisti žodžiu „sutrumpinimas", remiantis Gairių priedu.

2.2.7 KITI PAPILDOMI REIKALAVIMAI

36. Dėl Vokietijos PI akreditavimo reikalavimų 8.11.3 punkto („Skundų nagrinėjimas"), Valdyba ragina Vokietijos PI siekiant aiškumo vietoj sąvokos „pateisinami (angl. *justified*) skundai" vartoti sąvoką „pagrįsti (angl. *substantiated*) skundai".

3 IŠVADOS (REKOMENDACIJOS)

37. Taikant Vokietijos federacinių ir žemių priežiūros institucijų parengtus akreditavimo reikalavimus, gali atsirasti sertifikavimo įstaigų akreditavimo nuoseklumo spragų, tad reikalingi toliau nurodyti pakeitimai.

38. Kalbant apie bendro pobūdžio pastabas, Valdyba Vokietijos PI rekomenduoja:

    1) išbraukti nuorodą į „Valdybos leidimą", kad projektas atitiktų BDAR formuluotę.

39. Kalbant apie „bendro pobūdžio akreditavimo reikalavimus", Valdyba Vokietijos PI rekomenduoja:

1) iš dalies pakeisti reikalavimus dėl teisinės atsakomybės (4.1 punktas), kad jie atitiktų gaires;

2) iš dalies pakeisti 4.1.2.2 punktą, į sertifikavimo susitarimą įtraukiant įpareigojimą užtikrinti visišką sertifikavimo procedūros skaidrumą Vokietijos PI ir suteikti sertifikavimo įstaigai galimybę susipažinti su pareiškėjo duomenų tvarkymo veikla;

3) 4.1.2.2 punkte aiškiai nurodyti kompetentingos PI užduotis ir įgaliojimus pagal priedą;

4) be kitų sertifikavimo susitarimo elementų įtraukti įpareigojimą leisti sertifikavimo įstaigai atskleisti visą informaciją, reikalingą sertifikavimui pagal BDAR 42 straipsnio 8 dalį ir 43 straipsnio 5 dalį;

5) 4.1.2.2 punkto 6 įtraukoje aiškiai paminėti „sertifikuojamus produktus, procesus ir paslaugas";

6) 4.2.7 punkte sugriežtinti sertifikavimo įstaigoms, kurios priklauso atskiram juridiniam asmeniui arba yra jo kontroliuojamos, taikomus kriterijus, kad būtų atsižvelgta į tai, jog bet kokie ekonominiai sertifikavimo įstaigos ir juridinio asmens santykiai, priklausomai nuo jų savybių, gali turėti įtakos sertifikavimo veiklos nešališkumui.

40. Kalbant apie „reikalingus išteklius", Valdyba Vokietijos PI rekomenduoja:

1) suderinti 6.1.2.1 punkto formuluotę su gairėmis, reikalaujant, kad žinios būtų reikiamos ir tinkamos.

41. Kalbant apie procedūrinius reikalavimus, Valdyba Vokietijos PI rekomenduoja:

1) iš dalies pakeisti 7.1 punktą, aiškiai nurodant sertifikavimo įstaigos pareigą laikytis papildomų reikalavimų;

2) paminėti patvirtinto Europos duomenų apsaugos ženklo naudojimą;

3) suderinti 7.2 punkto formuluotę su gairėmis įtraukiant nuorodą į duomenų valdytojo (tvarkytojo) sutartį (-is);

4) į 7.4 punktą įtraukti sertifikavimo įstaigos pareigą aprašyti vertinimo metodus, kurių turi pakakti siekiant įvertinti, ar tvarkymo operacija (-os) atitinka sertifikavimo kriterijus;

5) 7.4 punkte patikslinti, kad BDAR numatyto sertifikato galiojimo trukmė neturi priklausyti nuo kitų tipų sertifikatų galiojimo;

6) 7.11 punkte nustatyti sertifikavimo įstaigos prievolę sutikti su Vokietijos PI sprendimais ir nurodymais panaikinti sertifikatą arba pareiškėjui neišduoti sertifikato, jeigu nebesilaikoma sertifikavimo reikalavimų.

4 BAIGIAMOSIOS PASTABOS

42. Ši nuomonė yra skirta Vokietijos federacinėms ir žemių priežiūros institucijoms ir bus paviešinta pagal BDAR 64 straipsnio 5 dalies b punktą.

Priimta

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

44. Vokietijos PI 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)