Gairės

# Bendrojo duomenų apsaugos reglamento (2016/679) 43 straipsnyje nurodytų sertifikavimo įstaigų akreditavimo gairės 4/2018

**3.0 redakcija**

**2019 m. birželio 4 d.**

Priimtos

# Ankstesnės redakcijos

| | | |
|---|---|---|
| 3.0 redakcija | 2019 m. birželio 4 d. | Į gaires įtraukiamas 1 priedas (t. y. jo 2.0 redakcija, priimta 2019 m. birželio 4 d. pasibaigus viešoms konsultacijoms) |
| 2.0 redakcija | 2018 m. gruodžio 4 d. | Gairės, kurios priimamos pasibaigus viešoms konsultacijoms. Tą pačią dieną priimamas viešoms konsultacijoms skirtas 1 priedas (jo 1.0 redakcija). |
| 1.0 redakcija | 2018 m. vasario 6 d. | Gairės, kurias priėmė 29 straipsnio darbo grupė (viešoms konsultacijoms skirta redakcija). 2018 m. gegužės 25 d. šią redakciją patvirtino Europos duomenų apsaugos valdyba. |

# Turinys

**Europos duomenų apsaugos valdyba,**

atsižvelgdama į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679/ES dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB 70 straipsnio 1 dalies e punktą,

atsižvelgusi į 2018 m. vasario mėn. vykusių viešų konsultacijų dėl gairių ir į 2018 m. gruodžio 14 d.–2019 m. vasario 1 d. vykusių viešų konsultacijų dėl jų priedo rezultatus, kaip nustatyta Bendrojo duomenų apsaugos reglamento (BDAR) 70 straipsnio 4 dalyje,

**PRIĖMĖ ŠIAS GAIRES.**

# 1 ĮVADAS

1. 2018 m. gegužės 25 d. įsigaliojusiu Bendruoju duomenų apsaugos reglamentu (Reglamentas (ES) 2016/679) (toliau – BDAR) Europoje užtikrinama šiuolaikinė duomenų apsaugos reikalavimų laikymosi sistema, pagrįsta atskaitomybe ir pagrindinėmis teisėmis. Šioje naujoje sistemoje numatytos įvairios priemonės, skirtos padėti užtikrinti BDAR nuostatų laikymąsi. Šios priemonės apima privalomus reikalavimus konkrečiomis aplinkybėmis (įskaitant duomenų apsaugos pareigūnų skyrimą ir poveikio duomenų apsaugai vertinimą) ir savanoriškas priemones, kaip antai elgesio kodeksus ir sertifikavimo mechanizmus.
2. Nustatant sertifikavimo mechanizmus ir duomenų apsaugos ženklus ir žymenis, valstybės narės pagal BDAR 43 straipsnio 1 dalį privalo užtikrinti, kad pagal BDAR 42 straipsnio 1 dalį sertifikatus išduodančios sertifikavimo įstaigos būtų akredituotos kompetentingos priežiūros institucijos arba nacionalinės akreditavimo įstaigos arba jų abiejų. Jeigu nacionalinė akreditavimo įstaiga akreditavimą atlieka pagal ISO/IEC 17065/2012, taip pat turi būti taikomi kompetentingos priežiūros institucijos nustatyti papildomi reikalavimai.
3. Prasmingi sertifikavimo mechanizmai gali padėti užtikrinti geresnį BDAR nuostatų laikymąsi ir didesnį skaidrumą duomenų subjektams ir plėtojant verslas verslui (B2B) santykius, pavyzdžiui, bendradarbiavimą tarp duomenų valdytojų ir duomenų tvarkytojų. Duomenų valdytojams ir duomenų tvarkytojams bus naudingas nepriklausomos trečiosios šalies patvirtinimas, kad jų duomenų tvarkymo operacijos atitinka reikalavimus[1].
4. Atsižvelgdama į visa tai, Europos duomenų apsaugos valdyba (toliau – EDAV) pripažįsta, kad būtina sukurti akreditavimo gaires. Akreditavimas ypač vertingas ir tikslingas dėl to, kad juo patikimai patvirtinama sertifikavimo įstaigų kompetencija, taip suteikiant pagrindą pasitikėti sertifikavimo mechanizmu.

[1] BDAR 100 konstatuojamojoje dalyje teigiama, kad siekiant didesnio skaidrumo ir geresnio šio reglamento laikymosi, reikėtų skatinti nustatyti sertifikavimo mechanizmus, kad duomenų subjektai galėtų įvertinti konkrečių produktų ar paslaugų duomenų apsaugos lygį.

5. Šių gairių tikslas – nurodyti, kaip turėtų būti aiškinamos ir įgyvendinamos BDAR 43 straipsnio nuostatos. Visų pirma jomis siekiama padėti valstybėms narėms, priežiūros institucijoms ir nacionalinėms akreditavimo įstaigoms nustatyti nuoseklų ir suderintą sertifikavimo įstaigų, kurios teiks sertifikavimo pagal BDAR paslaugas, akreditavimo pagrindą.

# 2 GAIRIŲ TAIKYMO SRITIS

6. Šiose gairėse:

- nustatomas akreditavimo pagal BDAR tikslas;
- paaiškinami sertifikavimo įstaigų akreditavimo pagal 43 straipsnio 1 dalį būdai ir nurodomi pagrindiniai svarstytini klausimai;
- pateikiama sistema, pagal kurią gali būti nustatomi papildomi akreditavimo reikalavimai, kai akreditavimą atlieka nacionalinė akreditavimo įstaiga ir
- sistema, pagal kurią gali būti nustatomi akreditavimo reikalavimai, kai akreditavimą atlieka priežiūros institucija.

7. Gairės nėra sertifikavimo įstaigų akreditavimo pagal BDAR procedūrinis vadovas. Jomis nekuriamas naujas sertifikavimo įstaigų akreditavimo pagal BDAR techninis standartas.

8. Gairės skirtos:

- valstybėms narėms, kurios turi užtikrinti, kad sertifikavimo įstaigos būtų akredituotos priežiūros institucijos ir (arba) nacionalinės akreditavimo įstaigos;
- nacionalinėms akreditavimo įstaigoms, kurios sertifikavimo įstaigas akredituoja pagal 43 straipsnio 1 dalies b punktą;
- kompetentingoms priežiūros institucijoms, nustatančioms standartą ISO/IEC 17065/2012[2] papildančius reikalavimus, kai akreditavimą atlieka nacionalinė akreditavimo įstaiga pagal 43 straipsnio 1 dalies b punktą;
- Europos duomenų apsaugos valdybai, kuri teikia nuomonę ir tvirtina kompetentingos priežiūros institucijos akreditavimo reikalavimus pagal 43 straipsnio 3 dalį, 70 straipsnio 1 dalies p punktą ir 64 straipsnio 1 dalies c punktą;
- kompetentingai priežiūros institucijai, nustatančiai akreditavimo reikalavimus, kai akreditavimą atlieka priežiūros institucija pagal 43 straipsnio 1 dalies a punktą;

- kitiems suinteresuotiesiems subjektams, kaip antai būsimoms sertifikavimo įstaigoms arba sertifikavimo schemų savininkams, nustatantiems sertifikavimo kriterijus ir procedūras[3].

[2] Tarptautinė standartizacijos organizacija. Atitikties įvertinimas. Reikalavimai, keliami produktų, procesų ir paslaugų sertifikavimo įstaigoms.

[3] Schemos savininkas – tai atpažįstama organizacija, kuri nustatė sertifikavimo kriterijus ir reikalavimus, pagal kuriuos bus vertinama atitiktis. Akredituojanti organizacija atlieka vertinimus (43 straipsnio 4 dalis) pagal sertifikavimo schemos reikalavimus ir išduoda sertifikatus (t. y. sertifikavimo įstaiga, dar vadinama atitikties vertinimo įstaiga). Vertinimus gali atlikti ta pati organizacija, kuri sukūrė schemą ir kurios savininkė ji yra, tačiau gali būti ir tokia tvarka, pagal kurią schemos savininkė yra viena organizacija, o vertinimus atlieka kita organizacija (arba kelios organizacijos).

9. Apibrėžtys

10. Toliau pateiktomis terminų apibrėžtimis siekiama užtikrinti, kad pagrindiniai akreditavimo proceso elementai būtų suprantami vienodai. Jos turėtų būti suprantamos kaip gairės todėl nėra neginčijamos. Šios apibrėžtys yra paremtos esamais reguliavimo pagrindais ir standartais, visų pirma atitinkamomis BDAR ir ISO/IEC 17065/2012 nuostatomis.

11. Šiose gairėse vartojamų terminų apibrėžtys:

12. sertifikavimo įstaigų *akreditavimas* – akreditavimo pagal BDAR 43 straipsnį sąvoka išaiškinta 3 skirsnyje;

13. *papildomi reikalavimai* – kompetentingos priežiūros institucijos nustatyti reikalavimai, į kuriuos atsižvelgiant atliekamas akreditavimas[4];

14. *sertifikavimas* – tai vertinimas ir nešališkas trečiosios šalies patvirtinimas[5], kad atitiktis sertifikavimo kriterijams buvo įrodyta;

15. *sertifikavimo įstaiga* – trečiosios šalies atitikties vertinimo[6] įstaiga[7], valdanti sertifikavimo mechanizmus[8];

16. *sertifikavimo schema* – sertifikavimo sistema, susijusi su nurodytais produktais, procesais ir paslaugomis, kuriems taikomi vienodi nustatyti reikalavimai, konkrečios taisyklės ir procedūros[9];

17. kriterijai arba sertifikavimo kriterijai – kriterijai, į kuriuos atsižvelgiant atliekamas sertifikavimas (atitikties vertinimas)[10];

18. nacionalinė akreditavimo įstaiga – vienintelė valstybės narės įstaiga, paskelbta pagal Europos Parlamento ir Tarybos reglamentą (EB) Nr. 765/2008, atliekanti akreditavimą pagal tos valstybės suteiktus įgaliojimus[11].

# 3 AKREDITAVIMO SĄVOKOS AIŠKINIMAS BDAR 43 STRAIPSNIO TAIKYMO TIKSLAIS

19. BDAR akreditavimo sąvoka neapibrėžta. Reglamento (EB) Nr. 765/2008, kuriame nustatomi bendrieji akreditavimo reikalavimai, 2 straipsnio 10 punkte akreditavimas apibrėžiamas taip:

[4] 43 straipsnio 1, 3 ir 6 dalys.

[5] Atkreiptinas dėmesys, kad pagal ISO 17000 standartą trečiosios šalies atestavimas (sertifikavimas) būtinas visiems atitikties vertinimo objektams (5.5 skyrius), išskyrus pačias atitikties vertinimo įstaigas, kurioms būtinas akreditavimas (5.6 skyrius).

[6] Trečiosios šalies atitikties vertinimo veiklą vykdo organizacija, nepriklausoma nuo objektą teikiančio asmens ar organizacijos ir nuo naudotojo interesų, susijusių su minėtu objektu, plg. ISO 17000 2.4 skyrių.

[7] Žr. ISO 17000 2.5 skyrių: „įstaiga, teikianti atitikties vertinimo paslaugas“; ISO 17011: „įstaiga, kuri vykdo atitikties vertinimo paslaugas ir gali būti akreditavimo objektas“; ISO 17065 3.12 skyrius.

[8] BDAR 42 straipsnio 1 ir 5 dalys.

[9] Žr. 3.9 skyrių ir ISO 17065 B priedą.

[10] Žr. 42 straipsnio 5 dalį.

[11] Žr. 765/2008/EB 2 straipsnio 11 punktą.

20. „nacionalinės akreditacijos įstaigos patvirtinimas, kad atitikties vertinimo įstaiga atitinka reikalavimus, apibrėžtus vieninguose standartuose, ir, kai taikoma, kitus papildomus reikalavimus, įskaitant pagal atitinkamų sektorių schemas taikomus reikalavimus, atlikti konkrečią atitikties vertinimo veiklą“.

**21.** Pagal ISO/IEC 17011,

22. „akreditavimas – trečiosios šalies patvirtinimas, kuriuo oficialiai parodoma, kad atitikties vertinimo įstaiga yra kompetentinga atlikti konkrečias atitikties vertinimo užduotis“.

23. Reglamento 43 straipsnio 1 dalyje nustatyta:

24. „Nedarant poveikio kompetentingos priežiūros institucijos užduotims ir įgaliojimams pagal 57 ir 58 straipsnius, sertifikavimo įstaigos, turinčios tinkamo lygio ekspertinių žinių duomenų apsaugos srityje, informavusios priežiūros instituciją, kad ji prireikus galėtų pasinaudoti savo įgaliojimais pagal 58 straipsnio 2 dalies h punktą, išduoda ir atnaujina sertifikatus. Valstybės narės užtikrina, kad tos sertifikavimo įstaigos yra akredituotos vienos ar abiejų toliau nurodytų subjektų:

    (a) priežiūros institucijos, kompetentingos pagal 55 arba 56 straipsnį;
    (b) nacionalinės akreditavimo įstaigos, paskelbtos pagal Europos Parlamento ir Tarybos reglamentą (EB) Nr. 765/2008, laikantis ISO/IEC 17065/2012 ir papildomų reikalavimų, kuriuos nustatė priežiūros institucija, kompetentinga pagal 55 arba 56 straipsnį“.

25. BDAR taikymo tikslais akreditavimo reikalavimai bus nustatomi pagal:

- ISO/IEC 17065/2012 ir papildomus reikalavimus, kuriuos nustatė priežiūros institucija, kompetentinga pagal 43 straipsnio 1 dalies b punktą, kai akreditavimą vykdo nacionalinė akreditavimo įstaiga, ir priežiūros institucija, kai ji pati vykdo akreditavimą.

26. Abiem atvejais konsoliduoti reikalavimai turi apimti 43 straipsnio 2 dalyje nurodytus reikalavimus.

27. EDAV pripažįsta, kad akreditavimo tikslas – oficialiai patvirtinti įstaigos kompetenciją atlikti sertifikavimą (atitikties vertinimo veiklą)[12]. Atsižvelgiant į BDAR, akreditavimas suprantamas taip:

28. nacionalinės akreditavimo įstaigos ir (arba) priežiūros institucijos patvirtinimas[13], kad sertifikavimo įstaiga[14] yra kompetentinga atlikti sertifikavimą pagal BDAR 42 ir 43 straipsnius, atsižvelgiant į standartą ISO/IEC 17065/2012 ir papildomus reikalavimus, nustatytus priežiūros institucijos ir (arba) Valdybos.

[12] 765/2008/EB 15 konstatuojamoji dalis.
[13] Žr. 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 765/2008, nustatančio su gaminių prekyba susijusius akreditavimo ir rinkos priežiūros reikalavimus, 2 straipsnio 10 punktą.
[14] Plg. su termino „akreditavimas“ apibrėžtimi pagal standartą ISO 17011.

# 4 AKREDITAVIMAS PAGAL BDAR 43 STRAIPSNIO 1 DALĮ

29. 43 straipsnio 1 dalyje nurodoma, kad yra keletas sertifikavimo įstaigų akreditavimo būdų. BDAR reikalaujama, kad priežiūros institucijos ir valstybės narės nustatytų sertifikavimo įstaigų akreditavimo procesą. Šiame skirsnyje nustatomi 43 straipsnyje nurodyto akreditavimo būdai.

## 4.1 Valstybių narių vaidmuo

30. Pagal 43 straipsnio 1 dalį reikalaujama, kad valstybės narės *užtikrintų*, kad sertifikavimo įstaigos būtų akredituotos, tačiau kiekviena valstybė narė gali nustatyti, kas turėtų atlikti vertinimą, po kurio įstaigos galėtų būti akredituotos. Remiantis 43 straipsnio 1 dalimi yra trys galimybės; akreditavimą atlieka:

(1) tik priežiūros institucija, remdamasi savo pačios reikalavimais;
(2) tik nacionalinė akreditavimo įstaiga, paskelbta pagal Reglamentą (EB) Nr. 765/2008, remdamasi standarto ISO/IEC 17065/2012 ir papildomais reikalavimais, kuriuos nustatė kompetentinga priežiūros institucija, arba
(3) priežiūros institucija ir nacionalinė akreditavimo įstaiga kartu (laikydamosi visų 2 punkte išvardytų reikalavimų).

31. Pati valstybė narė turi nuspręsti, ar nacionalinė akreditavimo įstaiga, ar priežiūros institucija, ar jos abi kartu vykdys minėtą akreditavimo veiklą, tačiau bet kuriuo atveju ji turėtų užtikrinti, kad tam būtų skirta pakankamai išteklių[15].

## 4.2 Sąveika su Reglamentu (EB) Nr. 765/2008

32. EDAV pažymi, kad Reglamento (EB) Nr. 765/2008 2 straipsnio 11 punkte nacionalinė akreditavimo įstaiga apibrėžiama kaip „*vienintelė* valstybės narės įstaiga, vykdanti akreditavimą pagal tos valstybės suteiktus įgaliojimus“.

33. 2 straipsnio 11 dalis galėtų būti laikoma nesuderinama su BDAR 43 straipsnio 1 dalimi, pagal kurią akreditavimą leidžiama atlikti įstaigai, kuri nėra valstybės narės nacionalinė akreditavimo įstaiga. EDAV nuomone, ES teisės aktuose buvo siekiama nukrypti nuo bendro principo, pagal kurį akreditavimą turi atlikti tik nacionalinė akreditavimo institucija, priežiūros institucijoms suteikiant tokius pačius įgaliojimus akredituoti sertifikavimo įstaigas. Todėl 43 straipsnio 1 dalis yra *lex specialis* Reglamento 765/2008 2 straipsnio 11 punkto atžvilgiu.

## 4.3 Nacionalinės akreditavimo įstaigos vaidmuo

34. 43 straipsnio 1 dalies b punkte nustatyta, kad nacionalinė akreditavimo įstaiga akredituos sertifikavimo įstaigas laikantis standarto ISO/IEC 17065/2012 ir papildomų reikalavimų, kuriuos nustatė kompetentinga priežiūros institucija.

35. Siekdama aiškumo, EDAV pažymi, kad 43 straipsnio 3 dalyje pateikta konkreti nuoroda į to paties straipsnio 1 dalies b punktą reiškia, kad tie reikalavimai yra papildomi reikalavimai, kuriuos nustatė 43 straipsnio 1 dalies b punkte nurodyta kompetentinga priežiūros institucija, ir 43 straipsnio 2 dalyje nustatyti reikalavimai.

36. Vykdydamos akreditavimo veiklą nacionalinės akreditavimo įstaigos taiko papildomus reikalavimus, kuriuos turi nustatyti priežiūros institucijos.

[15] Žr. Reglamento (EB) Nr. 765/2008 4 straipsnio 9 dalį.

37. Sertifikavimo įstaiga, akredituota pagal ISO/IEC 17065/2012 vykdyti su BDAR nesusijusią sertifikavimo schemų veiklą, kuri pageidauja išplėsti akreditavimo paslaugų apimtį, į ją įtraukiant su BDAR susijusį sertifikavimą, turės atitikti papildomus reikalavimus, kuriuos nustato priežiūros institucija, jeigu akreditavimą vykdys nacionalinė akreditavimo įstaiga. Jei pagal BDAR vykdomos sertifikavimo veiklos akreditavimą atlieka tik kompetentinga priežiūros institucija, sertifikavimo įstaiga, prašanti akreditavimo, turės atitikti atitinkamos priežiūros institucijos nustatytus reikalavimus.

## 4.4 Priežiūros institucijos vaidmuo

38. EDAV pažymi, kad 57 straipsnio 1 dalies q punkte nustatyta, kad priežiūros institucijos užduotis pagal 57 straipsnį *yra* vykdyti sertifikavimo įstaigos akreditavimą pagal 43 straipsnį, o 58 straipsnio 3 dalies e punkte nustatyta, kad priežiūros institucija turi leidimo išdavimo ir patariamuosius įgaliojimus akredituoti sertifikavimo įstaigas pagal 43 straipsnį. 43 straipsnio 1 dalies formuluotė suteikia tam tikro lankstumo, todėl priežiūros institucijos akreditavimo funkcija turėtų būti laikoma užduotimi tik tinkamais atvejais. Šis punktas gali būti patikslintas valstybės narės teisėje. Vis dėlto, kai akreditavimą atlieka nacionalinė akreditavimo įstaiga, pagal 43 straipsnio 2 dalies a punktą reikalaujama, kad sertifikavimo įstaiga kompetentingai priežiūros institucijai įtikinamai įrodytų savo nepriklausomumą ir ekspertines žinias jos siūlomo sertifikavimo mechanizmo dalyko srityje[16].

39. Jeigu valstybė narė nustato, kad sertifikavimo įstaigas turi akredituoti priežiūros institucija, priežiūros institucija turėtų parengti akreditavimo reikalavimus, įskaitant 43 straipsnio 2 dalyje nurodytus reikalavimus, bet jais neapsiribojant. Palyginti su nacionalinių akreditavimo įstaigų įsipareigojimais, susijusiais su sertifikavimo įstaigų akreditavimu, 43 straipsnyje pateikiama mažiau nurodymų dėl akreditavimo reikalavimų, kai priežiūros institucija pati atlieka akreditavimą. Siekiant prisidėti prie vieningo požiūrio į akreditavimą, priežiūros institucijos taikomi akreditavimo kriterijai turėtų būti grindžiami ISO/IEC 17065 ir papildyti reikalavimais, kuriuos pagal 43 straipsnio 1 dalies b punktą nustato priežiūros institucija. EDAV pažymi, kad 43 straipsnio 2 dalies a–e punktai atitinka ir patikslina ISO 17065 reikalavimus, o tai padės užtikrinti nuoseklumą.

40. Jeigu valstybė narė nustato, kad sertifikavimo įstaigas turi akredituoti nacionalinės akreditavimo įstaigos, priežiūros institucija turėtų nustatyti papildomus reikalavimus, papildysiančius Reglamente (EB) Nr. 765/2008 (kurio 3–14 straipsniai susiję su atitikties vertinimo įstaigų akreditavimo organizavimu ir vykdymu) numatytas esamas akreditavimo konvencijas ir technines taisykles, kuriomis apibūdinami sertifikavimo įstaigų darbo metodai ir procedūros. Atsižvelgiant į tai, Reglamente (EB) Nr. 765/2008 pateikiamos papildomos rekomendacijos: 2 straipsnio 10 dalyje apibrėžiamas akreditavimas, paminint vieningus standartus ir bet kokius kitus papildomus reikalavimus, įskaitant pagal susijusių sektorių schemas taikomus reikalavimus. Tai reiškia, kad priežiūros institucijos nustatyti papildomi reikalavimai turėtų apimti konkrečius reikalavimus ir jais turėtų būti siekiama palengvinti, be kita ko, sertifikavimo įstaigų nepriklausomumo ir ekspertinių žinių duomenų apsaugos srityje vertinimą, pavyzdžiui, jų gebėjimą įvertinti ir sertifikuoti duomenų valdytojų ir duomenų tvarkytojų vykdomas asmens duomenų tvarkymo operacijas pagal 42 straipsnio 1 dalį. Jie apima sektorių schemoms reikalingą kompetenciją, taip pat su pagrindinių fizinių asmenų

[16] Papildomi reikalavimai, kuriuos pagal 43 straipsnio 1 dalies b punktą nustato priežiūros institucija, turėtų apimti nepriklausomumo ir ekspertinių žinių reikalavimus. Taip pat žr. gairių 1 priedą.

teisių ir laisvių, ypač jų teisės į asmens duomenų apsaugą[17], apsauga susijusią kompetenciją,. Šių gairių priedas gali padėti kompetentingoms priežiūros institucijoms nustatyti papildomus reikalavimus pagal 43 straipsnio 1 dalies b punktą ir 43 straipsnio 3 dalį.

41. 43 straipsnio 6 dalyje nustatyta, kad „priežiūros institucija šio straipsnio 3 dalyje nurodytus reikalavimus ir 42 straipsnio 5 dalyje nurodytus kriterijus padaro lengvai viešai prieinamus“. Todėl siekiant užtikrinti skaidrumą skelbiami visi priežiūros institucijos patvirtinti kriterijai ir reikalavimai. Siekiant sertifikavimo įstaigų veiklos kokybės ir patikimumo, būtų pageidautina, kad visi akreditavimo reikalavimai būtų lengvai prieinami visuomenei.

## 4.5 Priežiūros institucija, atliekanti sertifikavimo įstaigos funkcijas

42. 42 straipsnio 5 dalyje nustatyta, kad priežiūros institucija gali išduoti sertifikatus, tačiau pagal BDAR nereikalaujama, kad ji būtų akredituota siekiant atitikties Reglamento (EB) Nr. 765/2008 reikalavimams. EDAV pažymi, kad 43 straipsnio 1 dalies a punkte ir konkrečiai 58 straipsnio 2 dalies h punkte bei 3 dalies a ir e–f punktuose priežiūros institucijoms suteikiami įgaliojimai atlikti akreditavimą bei sertifikavimą ir tuo pačiu metu teikti konsultacijas, ir, kai taikytina, panaikinti sertifikatus arba sertifikavimo įstaigoms nurodyti neišduoti sertifikatų.

43. Gali būti atvejų, kai tinkama arba būtina atskirti akreditavimo ir sertifikavimo funkcijas ir pareigas, pavyzdžiui, jei valstybėje narėje veikia ir priežiūros institucija, ir kitos sertifikavimo įstaigos, kurios išduoda tos pačios taikymo srities sertifikatus. Tokiu atveju priežiūros institucijos turėtų imtis pakankamų organizacinių priemonių, kad atskirtų pagal BDAR vykdomas užduotis, siekdamos įtvirtinti ir palengvinti sertifikavimo mechanizmus, kartu imdamosi atsargumo priemonių, kad išvengtų interesų konfliktų, kurių gali kilti dėl minėtų užduočių. Be to, rengdamos nacionalinės teisės aktus ir procedūras, susijusias su akreditavimu ir sertifikavimu pagal BDAR, valstybės narės ir priežiūros institucijos turėtų atsižvelgti į vieningą Europos lygmenį.

## 4.6 Akreditavimo reikalavimai

44. Šių gairių priede pateikiamos rekomendacijos, kaip nustatyti papildomus akreditavimo reikalavimus. Jame nurodomos atitinkamos BDAR nuostatos ir siūlomi reikalavimai, kuriuos priežiūros institucijos ir nacionalinės akreditavimo įstaigos turėtų apsvarstyti, siekdamos užtikrinti BDAR laikymąsi.

45. Kaip nustatyta pirmiau, jei sertifikavimo įstaigas akredituoja nacionalinė akreditavimo įstaiga pagal Reglamentą (EB) Nr. 765/2008, bus taikomas akreditavimo standartas ISO/IEC 17065/2012, papildytas priežiūros institucijos nustatytais papildomais reikalavimais. 43 straipsnio 2 dalis atitinka bendrąsias ISO/IEC 17065/2012 nuostatas, atsižvelgiant į pagrindinių teisių apsaugą pagal BDAR. BDAR numatytų sertifikavimo įstaigų ekspertinių žinių duomenų apsaugos srityje ir jų gebėjimo nepažeisti fizinių asmenų teisių ir laisvių tvarkant asmens duomenis vertinimo reikalavimai ir papildomi kriterijai nustatomi pagal priede pateiktą sistemą, kurioje remiamasi 43 straipsnio 2 dalies ir ISO/IEC 17065/2012 nuostatomis. EDAV pažymi, kad visų pirma ja siekiama užtikrinti, kad sertifikavimo įstaigos turėtų tinkamo lygio ekspertinių žinių duomenų apsaugos srityje, kaip nurodyta 43 straipsnio 1 dalyje.

46. Priežiūros institucijos nustatyti papildomi akreditavimo reikalavimai bus taikomi visoms akreditavimo prašančioms sertifikavimo įstaigoms. Akreditavimo įstaiga įvertins, ar sertifikavimo įstaiga yra kompetentinga vykdyti sertifikavimo veiklą pagal papildomus

[17] BDAR 1 straipsnio 2 dalis.

reikalavimus ir sertifikavimo sritį. Būtina nurodyti konkrečius sektorius arba sritis, kuriose sertifikavimo įstaiga yra akredituota vykdyti sertifikavimo veiklą.

47. EDAV taip pat pažymi, kad kai dalį sertifikavimo veiklos ar atskirus jos etapus akredituotos sertifikavimo įstaigos vardu vykdo išorės įstaigos, kaip antai laboratorijos ar auditoriai, be ISO/IEC 17065/2012 reikalavimų jiems taip pat taikomi specialių ekspertinių žinių duomenų apsaugos srityje reikalavimai. Tokiais atvejais tokių išorės įstaigų akreditavimas tik pagal BDAR nėra įmanomas. Vis dėlto, siekiant užtikrinti šių įstaigų tinkamumą veikti akredituotų sertifikavimo įstaigų vardu, akredituota sertifikavimo įstaiga privalo užtikrinti, kad atitinkamą veiklą vykdanti išorės įstaiga taip pat turėtų akredituotai įstaigai taikytiną ekspertinių žinių duomenų apsaugos srityje lygį ir galėtų tai įrodyti.

48. Šių gairių priede pristatyta papildomų akreditavimo reikalavimų nustatymo sistema nėra akreditavimo proceso, kurį vykdo nacionalinė akreditavimo įstaiga arba priežiūros institucija, procedūrinis vadovas. Joje pateikiamos struktūros ir metodikos rekomendacijos, taigi ir priemonių rinkinys, kuriuo priežiūros institucijos gali vadovautis nustatydamos papildomus akreditavimo reikalavimus.

# 1 PRIEDAS

1 priede pateikiamos „papildomų“ akreditavimo reikalavimų nustatymo, laikantis ISO/IEC 17065/2012 ir BDAR 43 straipsnio 1 dalies b punkto ir 43 straipsnio 3 dalies, gairės.

Šiame priede pateikiami siūlomi reikalavimai, kuriuos turi parengti duomenų apsaugos priežiūros institucija ir kurie taikomi nacionalinei akreditavimo įstaigai arba kompetentingai priežiūros institucijai akredituojant sertifikavimo įstaigą[19]. Laikantis 64 straipsnio 1 dalies c punkto, prieš patvirtinant šiuos papildomus reikalavimus apie juos pranešama Europos duomenų apsaugos valdybai.

Šis priedas turėtų būti taikomas kartu su standartu ISO/IEC 17065/2012. Priedo skirsnių numeracija atitinka standarto ISO/IEC 17065/2012 numeraciją. Jei priežiūros institucijos atlieka akreditavimą pagal 43 straipsnio 1 dalies a punktą, gera praktika, kai tinkama, būtų laikytis šio metodo. Taip bus prisidėta prie darnios akreditacijos ES.

Nepaisant to, ar dėl standarto ISO/IEC 17065/2012 punktų toliau pateikiamos gairės ar ne, kompetentinga priežiūros institucija gali suformuluoti ir kitus su tais punktais susijusius papildomus reikalavimus, jeigu jie atitinka nacionalinę teisę.

# 0 ĮŽANGA

[Šiame skirsnyje, jei taikytina, pristatomos suderintos nacionalinės akreditavimo įstaigos (NAĮ) ir duomenų apsaugos priežiūros institucijos bendradarbiavimo sąlygos, pvz., nurodant, kas turėtų būti atsakingas už prašymų priėmimą arba kaip pripažįstami patvirtinti kriterijai akreditavimo procedūros metu.]

# 1 TAIKYMO SRITIS[20]

Standartas ISO/IEC 17065/2012 taikomas atsižvelgiant į pagal Bendrąjį duomenų apsaugos reglamentą (BDAR). Daugiau informacijos pateikiama gairėse dėl akreditavimo ir sertifikavimo. NAĮ ir kompetentingai priežiūros institucijai (KPI) akreditavimo metu atliekant vertinimą turėtų būti atsižvelgiama į sertifikavimo mechanizmo taikymo sritį (pvz., debesijos paslaugų tvarkymo operacijų sertifikavimas), ypač į kriterijus, ekspertines žinias ir vertinimo metodiką. Plati ISO/IEC 17065/2012 taikymo sritis, apimanti produktus, procesus ir paslaugas, neturėtų sumažinti arba pakeisti BDAR reikalavimų, pvz., valdymo mechanizmas negali būti vienintelis sertifikavimo mechanizmo elementas, nes sertifikavimas turi apimti asmens duomenų tvarkymą, t. y. duomenų tvarkymo operacijas. Pagal BDAR 42 straipsnio 1 dalį sertifikavimas taikomas tik duomenų valdytojų ir duomenų tvarkytojų atliekamoms tvarkymo operacijoms.

# 2 NORMINĖS NUORODOS

Nesutapimų atveju BDAR yra viršesnis už ISO/IEC 17065/2012. Jei papildomuose reikalavimuose arba pagal sertifikavimo mechanizmą nuoroda daroma į kitus ISO standartus, jie turi būti aiškinami laikantis BDAR nustatytų reikalavimų.

[19] Informacija apie sertifikavimo kriterijų patvirtinimo procesą teikiama Gairių dėl sertifikavimo 4 skirsnyje.
[20] Numeracija pagal ISO/IEC 17065/2012.

# 3 TERMINAI IR APIBRĖŽTYS

Šiame priede vartojami gairių dėl akreditavimo (WP 261) ir sertifikavimo (EDAV 1/2018) terminai ir apibrėžtys; jie viršesni už ISO apibrėžtis.

# 4 BENDRIEJI AKREDITAVIMO REIKALAVIMAI

## 4.1 Teisiniai ir sutartiniai klausimai

### 4.1.1 Teisinė atsakomybė

Sertifikavimo įstaiga (bet kuriuo metu) turėtų galėti įrodyti NAĮ arba KPI, kad turi atnaujintas procedūras, kuriomis įrodoma, kad laikomasi akreditavimo sąlygose nustatytų teisinių įsipareigojimų ir papildomų reikalavimų, susijusių su Reglamento 2016/679/EB taikymu. Atkreipiame dėmesį į tai, kad sertifikavimo įstaiga pati yra duomenų valdytoja ir (arba) tvarkytoja, todėl ji turi galėti įrodyti, kad jos procedūros ir priemonės, visų pirma susijusios su klientų organizacijos asmens duomenų kontrole ir tvarkymu sertifikavimo proceso metu, atitinka Reglamento 2016/679/EB reikalavimus.

KPI gali nuspręsti įtraukti kitus reikalavimus ir procedūras, kad prieš akredituodama sertifikavimo įstaigas patikrintų jų atitiktį BDAR.

### 4.1.2 Sertifikavimo susitarimas (SS)

Minimalūs sertifikavimo susitarimo reikalavimai papildomi toliau nurodytais punktais.

Be to, kad laikosi ISO/IEC 17065/2012 reikalavimų, sertifikavimo įstaiga turi įrodyti, kad jos sertifikavimo susitarimais:

1. reikalaujama, kad pareiškėjas visada atitiktų bendruosius sertifikavimo reikalavimus, kaip apibrėžta ISO/IEC 17065/2012 4.1.2.2 punkto a papunktyje, ir kriterijus, kuriuos patvirtino kompetentinga priežiūros institucija arba Europos duomenų apsaugos valdyba pagal 43 straipsnio 2 dalies b punktą ir 42 straipsnio 5 dalį;
2. reikalaujama, kad pareiškėjas kompetentingai priežiūros institucijai suteiktų visišką skaidrumą dėl sertifikavimo procedūros, įskaitant konfidencialius sutartinius klausimus, susijusius su duomenų apsaugos reikalavimų laikymusi pagal 42 straipsnio 7 dalį ir 58 straipsnio 1 dalies c punktą;
3. nemažinama pareiškėjo atsakomybė už Reglamento 2016/679/EB laikymąsi ir nedaromas poveikis priežiūros institucijų, kurios yra kompetentingos pagal 42 straipsnio 5 dalį, užduotims ir įgaliojimams;
4. reikalaujama, kad pareiškėjas sertifikavimo įstaigai pateiktų visą informaciją ir prieigą prie savo duomenų tvarkymo veiklos, kurios yra būtinos sertifikavimo procedūrai atlikti pagal 42 straipsnio 6 dalį;
5. reikalaujama, kad pareiškėjas laikytųsi nustatytų terminų ir procedūrų. Sertifikavimo susitarime turi būti nurodyta, kad privaloma sutikti su terminais ir procedūromis, pvz., numatytais sertifikavimo programoje ar kituose reglamentuose, ir jų laikytis;
6. nustatomos su standarto ISO/IEC 17065/2012 4.1.2.2 punkto c papunkčio 1 įtrauka susijusios galiojimo, atnaujinimo ir panaikinimo taisyklės, laikantis 42 straipsnio 7 dalies ir 43 straipsnio 4 dalies, įskaitant taisykles, kuriomis nustatomi atitinkami pakartotinio vertinimo arba (teisingumo) peržiūros intervalai pagal 42 straipsnio 7 dalį;
7. leidžiama sertifikavimo įstaigai atskleisti visą informaciją, reikalingą sertifikatui išduoti pagal 42 straipsnio 8 dalį ir 43 straipsnio 5 dalį;

8. įtraukiamos taisyklės dėl atsargumo priemonių, kurios būtinos nagrinėjant skundus, kaip apibrėžta 4.1.2.2 punkto c papunkčio 2 įtraukoje, kartu su j papunkčiu, taip pat turi būti įtraukiami aiškūs pareiškimai dėl skundų nagrinėjimo struktūros ir procedūros laikantis 43 straipsnio 2 dalies d punkto;
9. be standarto ISO/IEC 17065/2012 4.1.2.2 punkte nurodytų minimalių reikalavimų, jei sertifikavimo įstaigos akreditavimo panaikinimo arba sustabdymo pasekmės turi poveikį klientui, taip pat turėtų būti atsižvelgiama į visas pasekmes klientui;
10. reikalaujama, kad pareiškėjas informuotų sertifikavimo įstaigą apie reikšmingus jos faktinės ar teisinės padėties ir jo sertifikuojamų produktų, procesų ir paslaugų pokyčius.

### 4.1.3 Duomenų apsaugos ženklų ir žymenų naudojimas

Sertifikatai, ženklai ir žymenys naudojami tik laikantis 42 ir 43 straipsnių ir gairių dėl akreditavimo ir sertifikavimo.

## 4.2 Nešališkumo valdymas

Be ISO/IEC 17065:2012 4.2 punkte nustatyto reikalavimo, akreditavimo įstaiga užtikrina, kad:

1. sertifikavimo įstaiga atitiktų kompetentingos priežiūros institucijos papildomus reikalavimus (pagal 43 straipsnio 1 dalies b punktą):
    **a.** pagal 43 straipsnio 2 dalies a punktą pateiktų atskirus jos nepriklausomumo įrodymus. Visų pirma tai taikoma sertifikavimo įstaigos finansavimo įrodymams, kiek jie susiję su nešališkumo patikinimu;
    **b.** jos užduotys ir pareigos nesukeltų interesų konflikto pagal 43 straipsnio 2 dalies e punktą;
2. sertifikavimo įstaiga šioje srityje nebūtų susijusi su jos vertinamu klientu.

## 4.3 Atsakomybė ir finansavimas

Be ISO/IEC 17065/2012 4.3.1 punkte nustatyto reikalavimo, akreditavimo įstaiga reguliariai užtikrina, kad sertifikavimo įstaiga turėtų tinkamų priemonių (pvz., draudimą arba rezervą) savo įsipareigojimams įvykdyti tuose geografiniuose regionuose, kuriuose ji veikia.

## 4.4 Nediskriminacinės sąlygos

Priežiūros institucija gali nustatyti papildomus reikalavimus, jeigu jie atitinka nacionalinę teisę.

## 4.5 Konfidencialumas

Priežiūros institucija gali nustatyti papildomus reikalavimus, jeigu jie atitinka nacionalinę teisę.

## 4.6 Viešai skelbiama informacija

Be ISO/IEC 17065/2012 4.6 punkte nustatyto reikalavimo, akreditavimo įstaiga iš sertifikavimo įstaigos reikalauja bent, kad:

1. visos patvirtintų kriterijų, kurie taikomi kaip apibrėžta 42 straipsnio 5 dalyje, versijos (dabartinė ir ankstesnės) būtų viešai skelbiamos ir visiems lengvai prieinamos, taip pat ir visos sertifikavimo procedūros, bendrai nurodant atitinkamus galiojimo laikotarpius;
2. informacija apie skundų nagrinėjimo procedūras ir kreipimusis į teismą būtų skelbiama pagal 43 straipsnio 2 dalies d punktą.

# 5 STRUKTŪROS REIKALAVIMAI, 43 STRAIPSNIO 4 DALIS („TINKAMAS VERTINIMAS“)

## 5.1 Organizacinė struktūra ir aukščiausioji vadovybė

Priežiūros institucija gali nustatyti papildomų reikalavimų.

## 5.2 Nešališkumo apsaugos mechanizmai

Priežiūros institucija gali nustatyti papildomų reikalavimų.

# 6 REIKALINGI IŠTEKLIAI

## 6.1 Sertifikavimo įstaigos darbuotojai

Be ISO/IEC 17065/2012 6 punkte nustatyto reikalavimo, akreditavimo įstaiga užtikrina, kad visų sertifikavimo įstaigų darbuotojai:

1. turėtų tinkamų ir atnaujintų ekspertinių žinių (žinių ir patirties) duomenų apsaugos srityje pagal 43 straipsnio 1 dalį;
2. būtų nepriklausomi ir turėtų reikiamų ekspertinių žinių apie sertifikavimo objektą pagal 43 straipsnio 2 dalies a punktą ir neturėtų interesų konflikto pagal 43 straipsnio 2 dalies e punktą;
3. įsipareigotų laikytis 42 straipsnio 5 dalyje nurodytų kriterijų pagal 43 straipsnio 2 dalies b punktą;
4. turėtų reikiamų ir tinkamų žinių apie duomenų apsaugos teisės aktus ir jų taikymo patirties;
5. turėtų reikiamų ir tinkamų žinių apie duomenų apsaugos technines ir organizacines priemones ir prireikus jų taikymo patirties;
6. galėtų įrodyti savo patirtį srityse, visų pirma nurodytose papildomų reikalavimų 6.1.1, 6.1.4 ir 6.1.5 punktuose.

Techninės patirties turintys darbuotojai:

- būtų įgiję atitinkamos techninių žinių srities kvalifikaciją, kuri atitinka bent šeštą Europos kvalifikacijų sandaros[21] lygmenį, arba atitinkamos reglamentuojamos profesijos pripažintą saugomą vardą (pvz., diplomuotas inžinierius), arba turėtų ilgą profesinę patirtį.
- *Už sprendimų dėl sertifikavimo priėmimą atsakingi darbuotojai* turi turėti didelę profesinę patirtį duomenų apsaugos priemonių nustatymo ir įgyvendinimo srityje.
- *Už vertinimus atsakingi darbuotojai* turi turėti profesinės patirties techninių duomenų apsaugos srityje ir žinių apie panašią procedūrą bei darbo su ja patirties (pvz., sertifikavimo ir (arba) audito), kuri būtų tinkamai užregistruota.

Darbuotojai įrodo, kad jie tobulina tam tikros srities kompetenciją, susijusią su techninėmis ir audito žiniomis, dalyvaudami tęstinio profesinio tobulėjimo programose.

Teisinės patirties turintys darbuotojai:

[21] Žr. kvalifikacijos sandaros palyginimo priemonę https://ec.europa.eu/ploteus/en/compare?

- turi būti baigę teisės studijas ES arba valstybės pripažintame universitete, kurių trukmė buvo bent aštuoni semestrai ir po kurių buvo suteiktas akademinis magistro laipsnis (LL.M.) arba lygiavertis laipsnis, arba turėti didelę profesinę patirtį.
- *Už sprendimų dėl sertifikavimo priėmimą atsakingi darbuotojai* turi įrodyti, kad yra sukaupę ilgametę profesinę patirtį duomenų apsaugos teisės srityje, ir turi būti registruoti, kaip reikalaujama valstybėje narėje.
- *Už vertinimus atsakingi darbuotojai* turi įrodyti, kad turi bent dvejų metų profesinę patirtį duomenų apsaugos teisės srityje ir žinių bei patirties, susijusios su panašiomis procedūromis (pvz., sertifikavimu ir (arba) auditu), ir, kai to reikalauja valstybė narė, jie turi būti registruoti.
    - Darbuotojai įrodo, kad jie tobulina tam tikros srities kompetenciją, susijusią su techninėmis ir audito žiniomis, dalyvaudami tęstinio profesinio tobulėjimo programose.

### 6.2 Vertinimo ištekliai

Priežiūros institucija gali nustatyti papildomus reikalavimus, jeigu jie atitinka nacionalinę teisę.

## 7 PROCEDŪRINIAI REIKALAVIMAI, 43 STRAIPSNIO 2 DALIES C IR D PUNKTAI

### 7.1 Bendrieji reikalavimai

Be ISO/IEC 17065/2012 7.1 punkte nustatyto reikalavimo, akreditavimo įstaiga turi užtikrinti, kad:

1. sertifikavimo įstaigos, pateikdamos paraišką, atitiktų kompetentingos priežiūros institucijos papildomus reikalavimus (pagal 43 straipsnio 1 dalies b punktą), siekiant, kad užduotys ir pareigos nesukeltų interesų konflikto pagal 43 straipsnio 2 dalies b punktą;
2. atitinkamai KPI prieš sertifikavimo įstaigos veiklos pradžią praneštų apie naujoje valstybėje narėje per pagalbinį skyrių patvirtintą išduosimą Europos duomenų apsaugos ženklą.

### 7.2 Paraiška

Be to, kas nurodyta ISO/IEC 17065/2012 7.2 punkte, turėtų būti reikalaujama, kad:

1. sertifikavimo objektas (vertinimo objektas) būtų išsamiai aprašytas paraiškoje. Joje taip pat nurodomos sąsajos ir perdavimai į kitas sistemas ir organizacijas, protokolai ir kitos garantijos;
2. paraiškoje būtų nurodyta, ar pasitelkiami tvarkytojai, ir jei tvarkytojas yra pareiškėjas, aprašoma jų atsakomybė ir užduotys; prie paraiškos būtų pridėta (-os) atitinkama (-os) duomenų valdytojo ir (arba) duomenų tvarkytojo sutartis (-ys).

### 7.3 Paraiškos peržiūra

Be to, kas nurodyta ISO/IEC 17065/2012 7.3 punkte, turėtų būti reikalaujama, kad:

1. privalomi vertinimo metodai, taikomi vertinimo objektui, būtų nurodyti sertifikavimo susitarime;
2. atliekant 7.3 punkto e papunktyje nurodytą vertinimą dėl to, ar ekspertinės žinios yra pakankamos, tam tikru mastu būtų atsižvelgta tiek į technines, tiek į teisines duomenų apsaugos srities žinias.

### 7.4 Vertinimas

Be to, kas nurodyta ISO/IEC 17065/2012 7.4 punkte, sertifikavimo mechanizmuose aprašomi vertinimo metodai, kurių turi pakakti tvarkymo operacijos (-ų) atitikties sertifikavimo kriterijams įvertinti, įskaitant, pavyzdžiui, kai tinkama:

1. metodą, kuriuo vertinamas duomenų tvarkymo operacijų būtinumas ir proporcingumas, atsižvelgiant į jų tikslą ir atitinkamus duomenų subjektus;
2. metodą, kuriuo nustatoma aprėptis, sudėtis ir vertinimas tų rizikos rūšių, į kurias duomenų valdytojas ir duomenų tvarkytojas atsižvelgė nagrinėdami teisines pasekmes pagal BDAR 30, 32, 35 ir 36 straipsnius ir techninių ir organizacinių priemonių nustatymą pagal BDAR 24, 25 ir 32 straipsnius tiek, kiek minėti straipsniai taikomi sertifikavimo objektui;
3. metodą, kuriuo vertinamos teisių gynimo priemonės, įskaitant garantijas, apsaugos priemones ir procedūras, kuriomis užtikrinama asmens duomenų apsauga tvarkant duomenis, susijusius su sertifikavimo objektu, ir įrodoma, kad tenkinami kriterijuose nustatyti teisiniai reikalavimai, ir
4. metodų ir išvadų dokumentavimą.

Sertifikavimo įstaiga turėtų būti įpareigota užtikrinti, kad šie vertinimo metodai būtų standartizuoti ir visuotinai taikomi. Tai reiškia, kad palyginami vertinimo metodai taikomi palyginamiems vertinimo objektams. Bet koks nukrypimas nuo šios procedūros turi būti pagrįstas sertifikavimo įstaigos.

Be to, kas nurodyta ISO/IEC 17065/2012 7.4.2 punkte, turėtų būti leidžiama vertinimą atlikti sertifikavimo įstaigos pripažintiems išorės ekspertams.

Be to, kas nurodyta ISO/IEC 17065/2012 7.4.5 punkte, turėtų būti reikalaujama, kad duomenų apsaugos sertifikavimą pagal BDAR 42 ir 43 straipsnius, kuris jau yra sertifikavimo objekto dalis, būtų galima įtraukti į galiojantį sertifikavimą. Tačiau jis nepakankamas ir negali visiškai atstoti (dalinių) vertinimų. Sertifikavimo įstaiga privalo patikrinti atitiktį kriterijams. Siekiant patvirtinimo, bet kokiu atveju būtina pateikti išsamią vertinimo ataskaitą arba informaciją, leidžiančią įvertinti ankstesnę sertifikavimo veiklą ir jos rezultatus. Sertifikavimo pareiškimas arba panašūs sertifikavimo sertifikatai nėra tinkami ataskaitai atstoti.

Be to, kas nurodyta ISO/IEC 17065/2012 7.4.6 punkte, turėtų būti reikalaujama, kad sertifikavimo įstaiga savo sertifikavimo mechanizme išsamiai nurodytų, kaip 7.4.6 punkte reikalaujama informacija leis klientui (sertifikavimo pareiškėjui) sužinoti apie sertifikavimo mechanizmo neatitikties atvejus. Atsižvelgiant į tai, turėtų būti apibrėžtas tokios informacijos pobūdis ir pateikimo laikas.

Be to, kas nurodyta ISO/IEC 17065/2012 7.4.9 punkte, turėtų būti reikalaujama, kad esant duomenų apsaugos priežiūros institucijos prašymui, ji galėtų visapusiškai susipažinti su dokumentais.

## 7.5 Peržiūra

Kartu su tuo, kas nurodyta ISO/IEC 17065/2012 7.5 punkte, reikalaujama nustatyti atitinkamų sertifikatų išdavimo, reguliarios peržiūros ir atšaukimo procedūras pagal 43 straipsnio 2 ir 3 dalis.

## 7.6 Sprendimas dėl sertifikavimo

Be to, kas nurodyta ISO/IEC 17065/2012 7.6.1 punkte, reikalaujama, kad sertifikavimo įstaiga būtų įpareigota savo procedūrose išsamiai nurodyti, kaip užtikrinamas jos nepriklausomumas ir atsakomybė priimant individualius sprendimus dėl sertifikavimo.

## 7.7 Sertifikavimo dokumentai

Be to, kas nurodyta ISO/IEC 17065/2012 7.7.1 punkto e papunktyje, ir pagal BDAR 42 straipsnio 7 dalį turėtų būti reikalaujama, kad sertifikatų galiojimo laikotarpis neviršytų trejų metų.

Be to, kas nurodyta standarto ISO/IEC 17065/2012 7.7.1 punkto e papunktyje, turėtų būti reikalaujama, kad numatytos stebėsenos laikotarpis, kaip apibrėžta 7.9 skirsnyje, taip pat būtų patvirtintas dokumentais.

Be to, kas nurodyta ISO/IEC 17065/2012 7.7.1 punkto f papunktyje, turėtų būti reikalaujama, kad sertifikavimo įstaigos sertifikavimo dokumentuose įvardintų sertifikavimo objektą (nurodydamos versijos būseną arba panašias charakteristikas, jei taikoma).

## 7.8 Sertifikuotų produktų katalogas

Be to, kas nurodyta ISO/IEC 17065/2012 7.8 punkte, turėtų būti reikalaujama, kad sertifikavimo įstaiga saugotų informaciją apie sertifikuotus produktus, procesus ir paslaugas ir ji būtų prieinama tiek vidaus, tiek išorės subjektams. Sertifikavimo įstaiga pateiks visuomenei vertinimo ataskaitos santrauką. Šios santraukos tikslas – suteikti skaidrią informaciją apie tai, kas buvo sertifikuota ir kaip buvo atliekamas vertinimas. Joje bus paaiškinti šie dalykai:

(a) sertifikavimo taikymo apimtis ir pateiktas išsamus sertifikavimo objekto aprašymas,

(b) atitinkami sertifikavimo kriterijai (įskaitant jų versiją arba funkcinį statusą),

(c) vertinimo metodai ir atlikti testai, ir

(d) rezultatas (-ai).

Be to, kas nurodyta ISO/IEC 17065/2012 7.8 punkte, ir pagal BDAR 43 straipsnio 5 dalį sertifikavimo įstaiga informuoja kompetentingas priežiūros institucijas apie priežastis, dėl kurių išduodamas arba atšaukiamas sertifikatas.

## 7.9 Priežiūra

Be to, kas nurodyta ISO/IEC 17065/2012 7.9.1, 7.9.2 ir 7.9.3 punktuose, ir pagal BDAR 43 straipsnio 2 dalies c punktą turėtų būti reikalaujama, kad būtų privaloma reguliariai taikyti stebėsenos priemones, jei norima išsaugoti sertifikavimą stebėsenos laikotarpiu.

## 7.10 Pakeitimai, turintys įtakos sertifikavimui

Be to, kas nurodyta EN ISO/IEC 17065/2012 7.10.1 ir 7.10.2 punktuose, pakeitimai, turintys įtakos sertifikavimui, kuriuos sertifikavimo įstaiga turi išnagrinėti apima: duomenų apsaugos teisės aktų pakeitimus, Europos Komisijos deleguotųjų aktų priėmimą pagal 43 straipsnio 8 dalį ir 43 straipsnio 9 dalį, Europos duomenų apsaugos valdybos sprendimus ir su duomenų apsauga susijusius teismų sprendimus. Pakeitimų procedūros, dėl kurių tokiu atveju turi būti susitarta, galėtų apimti šiuos elementus: pereinamąjį laikotarpį, patvirtinimo procesą su kompetentinga priežiūros institucija, atitinkamo sertifikavimo objekto pakartotinį vertinimą ir atitinkamas priemones sertifikavimui atšaukti, jei sertifikuota tvarkymo operacija nebeatitinka atnaujintų kriterijų.

## 7.11 Sertifikato galiojimo nutraukimas, sutrumpinimas, sustabdymas arba panaikinimas

Be to, kas nurodyta ISO/IEC 17065/2012 7.11.1 skyriuje, turėtų būti reikalaujama, kad sertifikavimo įstaiga nedelsiant raštu informuotų kompetentingą priežiūros instituciją ir prireikus NAĮ apie priemones, kurių buvo imtasi, ir apie tęsiamą, apribojamą, sustabdomą arba panaikinimą sertifikavimą.

Pagal 58 straipsnio 2 dalies h punktą sertifikavimo įstaiga turi priimti kompetentingos priežiūros institucijos sprendimus ir nurodymus panaikinti sertifikatą arba jo neišduoti klientui (pareiškėjui), jei nesilaikoma arba nebesilaikoma sertifikavimo reikalavimų.

## 7.12 Registrai

Turėtų būti reikalaujama, kad sertifikavimo įstaiga saugotų visus dokumentus ir jie būtų išsamūs, suprantami, atnaujinti ir tinkami auditui.

### 7.13 Skundai ir kreipimaisi į teismą, 43 straipsnio 2 dalies d punktas

Be to, kas nurodyta ISO/IEC 17065/2012 7.13.1 punkte, turėtų būti reikalaujama, kad sertifikavimo įstaiga nustatytų:

(a) kas gali teikti skundus ar prieštaravimus,

(b) kas juos nagrinėja sertifikavimo įstaigoje,

(c) kokie tokiu atveju atliekami patikrinimai ir

(d) kaip galima konsultuotis su suinteresuotosiomis šalimis.

Be to, kas nurodyta ISO/IEC 17065/2012 7.13.2 punkte, turėtų būti reikalaujama, kad sertifikavimo įstaiga nustatytų:

(a) kam ir kaip toks patvirtinimas turi būti suteiktas,

(b) kokie yra su tuo susiję terminai ir

(c) kokie procesai turi būti pradėti vėliau.

Be to, kas nurodyta ISO/IEC 17065/2012 7.13.1 punkte, sertifikavimo įstaiga turi nustatyti, kaip atskiriama sertifikavimo ir skundų bei kreipimųsi į teismą nagrinėjimo veikla.

## 8 VALDYMO SISTEMOS REIKALAVIMAI

Pagal ISO/IEC 17065/2012 8 skyrių bendrasis valdymo sistemos reikalavimas yra tas, kad visų ankstesnių skyrių reikalavimų įgyvendinimas akredituotos sertifikavimo įstaigos sertifikavimo mechanizmo taikymo srityje būtų dokumentuojamas, vertinamas, kontroliuojamas ir stebimas nepriklausomai.

Pagrindinis valdymo principas – nustatyti sistemą, pagal kurią būtų veiksmingai ir efektyviai nustatyti jos tikslai – sertifikavimo paslaugų įgyvendinimas pagal tinkamas specifikacijas. Tam būtini: skaidrumas dėl to, ar sertifikavimo įstaiga tenkina akreditavimo reikalavimus, galimybė tai patikrinti ir nuolatinė atitiktis reikalavimams.

Šiuo tikslu valdymo sistemoje turi būti nurodyta metodika, kaip šiuos reikalavimus įgyvendinti ir kontroliuoti laikantis duomenų apsaugos taisyklių ir kaip kartu su pačia akredituota įstaiga nuolat juos tikrinti.

Šie valdymo principai ir jų dokumentuotas įgyvendinimas turi būti skaidrūs ir atskleisti akredituotos sertifikavimo įstaigos, laikantis akreditavimo procedūros pagal 58 straipsnį, ir vėliau duomenų apsaugos priežiūros institucijos prašymu bet kuriuo metu atliekant tyrimą duomenų apsaugos peržiūrų forma pagal 58 straipsnio 1 dalies b punktą arba pagal 42 straipsnio 7 dalį išduotų sertifikatų peržiūros forma pagal 58 straipsnio 1 dalies c punktą.

Visų pirma akredituota sertifikavimo įstaiga turi nuolat ir visam laikui paviešinti, kokios buvo atliekamos sertifikavimo procedūros ir kokiu pagrindu (arba kokių sertifikavimo mechanizmų ar schemų), koks sertifikatų galiojimo laikotarpis ir sąlygos (100 konstatuojamoji dalis).

### 8.1 Bendrieji valdymo sistemos reikalavimai

Kompetentinga priežiūros institucija gali nustatyti papildomus reikalavimus ir toliau juos pildyti, jeigu jie atitinka nacionalinę teisę.

## 8.2 Valdymo sistemos dokumentavimas

Kompetentinga priežiūros institucija gali nustatyti papildomus reikalavimus ir toliau juos pildyti, jeigu jie atitinka nacionalinę teisę.

## 8.3 Dokumentų kontrolė

Kompetentinga priežiūros institucija gali nustatyti papildomus reikalavimus ir toliau juos pildyti, jeigu jie atitinka nacionalinę teisę.

## 8.4 Registrų kontrolė

Kompetentinga priežiūros institucija gali nustatyti papildomus reikalavimus ir toliau juos pildyti, jeigu jie atitinka nacionalinę teisę.

## 8.5 Valdymo peržiūra

Kompetentinga priežiūros institucija gali nustatyti papildomus reikalavimus ir toliau juos pildyti, jeigu jie atitinka nacionalinę teisę.

## 8.6 Vidaus auditai

Kompetentinga priežiūros institucija gali nustatyti papildomus reikalavimus ir toliau juos pildyti, jeigu jie atitinka nacionalinę teisę.

## 8.7 Taisomieji veiksmai

Kompetentinga priežiūros institucija gali nustatyti papildomus reikalavimus ir toliau juos pildyti, jeigu jie atitinka nacionalinę teisę.

## 8.8 Prevenciniai veiksmai

Kompetentinga priežiūros institucija gali nustatyti papildomus reikalavimus ir toliau juos pildyti, jeigu jie atitinka nacionalinę teisę.

# 9 KITI PAPILDOMI REIKALAVIMAI22

## 9.1 Vertinimo metodų atnaujinimas

Sertifikavimo įstaiga nustato vertinimo metodų atnaujinimo procedūras, taikytinas atliekant vertinimą pagal 7.4 punktą. Atnaujinimas turi būti atliekamas atsižvelgiant į teisinės sistemos pakeitimus, atitinkamą riziką , techninių ir organizacinių priemonių plėtotę ir įgyvendinimo sąnaudas.

## 9.2 Ekspertinių žinių išsaugojimas

Sertifikavimo įstaigos nustato procedūras, kad užtikrintų savo darbuotojų mokymą, siekdamos atnaujinti jų įgūdžius ir atsižvelgti į 9.1 punkte išvardytus pakeitimus.

## 9.3 Pareigos ir kompetencija

### 9.3.1 Sertifikavimo įstaigos ir jos klientų ryšiai

Nustatomos procedūros, kurių laikantis taikomos procedūros ir sukuriamos struktūros sertifikavimo įstaigos ir jos klientų ryšiams palaikyti. Jos apima:

1. akredituotos sertifikavimo įstaigos užduočių ir atsakomybės dokumentavimą, siekiant:
    a. patenkinti informacijos prašymus arba

[22] Kompetentinga priežiūros institucija gali nustatyti papildomus reikalavimus ir toliau juos pildyti, jeigu jie atitinka nacionalinę teisę.

b. užmegzti ryšį, jei pateikiamas skundas dėl sertifikavimo;

2. paraiškų teikimo procesą, siekiant:
    a. informuoti apie paraiškos statusą;
    b. kompetentingai priežiūros institucijai leisti įvertinti:
        i. atsiliepimus;
        ii. kompetentingos priežiūros institucijos sprendimus.

### 9.3.2 Vertinimo veiklos dokumentavimas

Priežiūros institucija gali nustatyti papildomų reikalavimų.

### 9.3.3 Skundų nagrinėjimo administravimas

Skundų nagrinėjimas turi būti neatsiejamas nuo valdymo sistemos, kuria visų pirma įgyvendinami ISO/IEC 17065/2012 4.1.2.2 punkto c papunktyje, 4.1.2.2 punkto j papunktyje, 4.6 punkto d papunktyje ir 7.13 punkte nustatyti reikalavimai.

Informacija apie pagrįstus skundus ir prieštaravimus pateikiama kompetentingai priežiūros institucijai.

### 9.3.4 Panaikinimo valdymas

Su akreditavimo sustabdymu arba panaikinimu susijusios procedūros įtraukiamos į sertifikavimo įstaigos valdymo sistemą, įskaitant pranešimus klientams.