Sertifikavimo įstaigų akreditavimo tvarkos aprašo
Priedas

SERTIFIKAVIMO ĮSTAIGŲ AKREDITAVIMO REIKALAVIMAI

Bendrieji akreditavimo reikalavimai yra nustatyti LST EN ISO/IEC 17065:2012 *Atitikties įvertinimas. Reikalavimai, keliami produktų, procesų ir paslaugų sertifikavimo įstaigoms* (toliau – ISO 17065 standartas). Šiuo priedu, vadovaujantis 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 (Bendrasis duomenų apsaugos reglamentas) (toliau – Reglamentas (ES) 2016/679) 43 straipsnio 3 dalimi ir 57 straipsnio 1 dalies p punktu, yra nustatomi papildomi sertifikavimo įstaigų akreditavimo reikalavimai. Sertifikavimo įstaigų akreditavimo reikalavimų (toliau – priedas) skyrių eilės numeriai ir pavadinimai, išskyrus 9 skyrių, atitinka ISO 17065 standarto skirsnių numerius ir pavadinimus. Inspekcija, akredituoja sertifikavimo įstaigas tiek pagal ISO 17065 standarte, tiek pagal priede nurodytus reikalavimus. Tuo atveju, jei sertifikavimo įstaiga pagal ISO 17065 standartą jau yra akredituota, Inspekcija vertinta tik atitiktį priede nurodytiems akreditavimo reikalavimams.

1 SKYRIUS
TAIKYMO APIMTIS

Šis priedas nustato sertifikavimo įstaigų kompetencijos, vieningos praktikos ir nepriklausomumo vertinimo reikalavimus, papildančius nustatytus ISO 17065 standarte.

ISO 17065 standartas taikomas atsižvelgiant į Reglamentą (ES) 2016/679. Daugiau informacijos pateikiama Europos duomenų apsaugos valdybos (toliau – Valdyba) „Bendrojo duomenų apsaugos reglamento (2016/679) 43 straipsnyje nurodytų sertifikavimo įstaigų akreditavimo gairėse Nr. 4/2018“ (toliau – Gairės Nr. 4/2018) ir „Sertifikavimo ir sertifikavimo kriterijų nustatymo pagal Reglamento 42 ir 43 straipsnius gairėse Nr.1/2018“ (toliau – Gairės Nr. 1/2018).

Pastebėtina, kad pagal Reglamento (ES) 2016/679 42 straipsnio 1 dalį sertifikavimas taikomas tik duomenų valdytojų ir duomenų tvarkytojų atliekamoms tvarkymo operacijoms.

2 SKYRIUS
NORMINĖS NUORODOS

ISO 17065 standarto taikymo sritis, apimanti produktus, procesus ir paslaugas, neturi sumažinti arba pakeisti Reglamento (ES) 2016/679 reikalavimų. Reglamentas (ES) 2016/679 turi pirmenybę prieš ISO 17065 standartą. Jei ISO 17065 standarte, šiame priede ar sertifikavimo įstaigų vertinimo tvarkos apraše būtų daromos nuorodos į kitus ISO standartus, jie turi būti aiškinami laikantis Reglamento (ES) 2016/679 nustatytų reikalavimų.

3 SKYRIUS
TERMINAI IR APIBRĖŽTYS

Šiame priede vartojami Gairėse Nr. 1/2018 ir Gairėse Nr. 4/2018 nustatyti terminai ir apibrėžtys, kurie turi pirmenybę prieš terminus ir apibrėžtis, nustatytas ISO 17065 standarte.

Priede taip pat naudojami šie terminai ir apibrėžtys:

1. **Akreditavimas** – sertifikavimo įstaigos atitikties akreditavimo reikalavimams vertinimo pagal Reglamento (ES) 2016/679 43 straipsnį procesas.

2. **Akreditavimo reikalavimai** – ISO17065 standarte ir šiame priede nustatyti reikalavimai, kuriuos turi atitikti sertifikavimo įstaiga, siekianti būti akredituota teikti sertifikavimo paslaugas arba atnaujinti akreditaciją.

3. **Asmens duomenų apsaugą reglamentuojantys teisės aktai** – Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (toliau – ADTAĮ), Lietuvos Respublikos elektroninių ryšių įstatymas, Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas ir kt. teisės aktai.

4. **Atitikties vertinimas** – sertifikuojamo subjekto asmens duomenų tvarkymo operacijų atitikties sertifikavimo kriterijams vertinimas.

5. **Prašymas** – sertifikavimo įstaigos prašymas dėl jos akreditavimo ar akreditavimo atnaujinimo.

6. **Priežiūros institucijos** – Valstybinės duomenų apsaugos inspekcija (toliau – Inspekcija) ir žurnalistų etikos inspektorius.

7. **Sertifikavimo įstaiga** – fizinis ar juridinis asmuo, akredituotas ar siekiantis būti akredituotu Inspekcijos teikti sertifikavimo paslaugas.

8. **Sertifikavimo kriterijai** – sertifikavimo įstaigos nustatyti ir Inspekcijos patvirtinti kriterijai, kuriuos turi atitikti duomenų valdytojas ar duomenų tvarkytojas, siekiantis sertifikuoti savo veiklą ar jos dalį (prekes, paslaugas ar procesus) pagal Reglamento (ES) 2016/679 42 straipsnį.

9. **Sertifikavimo mechanizmas** – Reglamento (ES) 2016/679 42 straipsnio pagrindu nustatyta sertifikavimo sistema, kuria vadovaujantis sertifikavimo įstaiga vertina sertifikuojamo subjekto prekių, paslaugų ar procesų atitiktį sertifikavimo kriterijams.

10. **Sertifikavimo paslaugos** – trečiosios šalies atliekamas atestavimas, susijęs su duomenų valdytojų ir (ar) duomenų tvarkytojų atliekamomis asmens duomenų tvarkymo operacijomis.

11. **Sertifikuojamas subjektas** – fizinis ar juridinis asmuo, kuris kreipiasi į sertifikavimo įstaigą dėl jo veiklos ar jos dalies atitikties sertifikavimo kriterijams įvertinimo ir sertifikato išdavimo.

12. **Susitarimas** – sertifikavimo įstaigos ir sertifikuojamo subjekto susitarimas dėl sertifikavimo paslaugų teikimo.

4 SKYRIUS
BENDRIEJI AKREDITAVIMO REIKALAVIMAI

Eil. Nr.	Reikalavimas	Reikalavimo paaiškinimas ir atitikties šiam reikalavimui patvirtinimo dokumentai ar informacija
4.1.	**Teisiniai ir sutartiniai klausimai**	
4.1.1.	**Teisinė atsakomybė**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 4.1.1 papunktyje, sertifikavimo įstaiga turi sugebėti bet kuriuo metu įrodyti Inspekcijai, kad: 1. laikosi akreditavimo reikalavimuose nustatytų teisinių įsipareigojimų ir papildomų reikalavimų, susijusių su Reglamento (ES) 2016/679, ir, jei taikoma, ADTAĮ ir kitų asmens duomenų apsaugą reglamentuojančių teisės aktų taikymu, o taip pat, kad sertifikavimui taikomos procedūros ir dokumentai yra laiku atnaujinamos; 2. tvarkydama asmens duomenis ji laikosi Reglamento (ES) 2016/679 ir, kai taikoma, kitų asmens duomenų apsaugą

		reglamentuojančių teisės aktų, t. y. yra priėmusi asmens duomenų tvarkymo taisykles ir kitus būtinus dokumentus (privatumo pranešimus, veiklos įrašus, asmens duomenų saugumo pažeidimų tyrimo instrukcijas ir kt.), laiku juos atnaujina, taip pat yra paskyrusi duomenų apsaugos pareigūną (jei taikoma) ir t. t.; 3. sertifikavimo įstaigai nėra pradėta bankroto procedūra, pavyzdžiui, pateikiant juridinių asmenų registro išrašą. 4. sertifikavimo įstaiga Lietuvoje ir kitose valstybėse narėse nebuvo bausta ar teista dėl pažeidimų, susijusių su jos vykdoma veikla, pavyzdžiui, Sertifikavimo įstaigos patvirtinimą ar pažymą. Sertifikavimo įstaiga turi pateikti visą informaciją apie reikšmingus faktinės ar teisinės padėties pasikeitimus, susijusius su teisine atsakomybe, nešališkumu, finansavimu, konfidencialumu, skaidrumu, ekspertinėmis žiniomis ir veiksmingu skundų nagrinėjimu, kurie gali turėti įtakos jos akreditavimui.
4.1.2.	**Susitarimas dėl sertifikavimo**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 4.1.2 papunktyje, susitarimuose (kurie turi būti sudaromi rašytine forma): 1. reikalaujama, kad sertifikuojamas subjektas visada atitiktų bendruosius sertifikavimo reikalavimus, kaip apibrėžta ISO 17065 standarto 4.1.2.2 papunkčio a dalyje, ir sertifikavimo įstaigos nustatytus ir Inspekcijos patvirtintus sertifikavimo kriterijus; 2. reikalaujama, kad sertifikuojamas subjektas užtikrintų skaidrumo principo laikymąsi ir, vadovaujantis Reglamento (ES) 2016/679 42 straipsnio 7 dalimi ir 58 straipsnio 1 dalies c punktu, suteiktų Inspekcijai visą reikalingą informaciją, įskaitant konfidencialią, apie sertifikavimo procedūrą, kiek tai susiję su asmens duomenų apsaugos reikalavimų laikymusi; 3. nėra mažinamos sertifikuojamo subjekto ar sertifikavimo įstaigos pareigos, nustatytos Reglamente (ES) 2016/679, nėra mažinama iš Reglamento (ES) 2016/679 kylanti atsakomybė, o taip pat nėra daromas poveikis Inspekcijos įgaliojimams ir (ar) užduotims pagal Reglamento (ES) 2016/679 42 straipsnio 5 dalį, 55 – 58 straipsnius; 4. reikalaujama, kad sertifikuojamas subjektas sertifikavimo įstaigai pateiktų visą sertifikavimo procedūrai pagal Reglamento (ES) 2016/679 42 straipsnio 6 dalį reikalingą informaciją, įskaitant prieigą prie sertifikuojamų asmens duomenų tvarkymo operacijų; 5. nustatyti taikomi sertifikavimo kriterijai ir metodai, sertifikavimo objekto vertinimo (įskaitant vertinimo, ar sertifikavimo įstaiga turi pakankamą kompetenciją sertifikavimo objekto vertinimo kontekste) kriterijai, terminai, procedūros ir sertifikuojamo subjekto pareiga laikytis su sertifikavimu ar jo atnaujinimu susijusių terminų ir

		procedūrų, numatytų Susitarime, sertifikavimo įstaigos nustatytoje tvarkoje ir, jei taikoma, kituose ISO standartuose; 6. sertifikuojamas subjektas suteikia teisę Sertifikavimo įstaigai, vadovaujantis Reglamento (ES) 2016/679 43 straipsnio 5 dalimi, atskleisti Inspekcijai sertifikato išdavimo ar panaikinimo priežastis. 7. sertifikuojamas subjektas suteikia teisę sertifikavimo įstaigai, vadovaujantis Reglamento (ES) 2016/679 42 straipsnio 8 dalimi, atskleisti Valdybai visą informaciją apie sertifikavimo mechanizmą, t. y. sertifikuojamo subjekto pavadinimą, sertifikatą išdavusį subjektą, sertifikato datą, sertifikuotos asmens duomenų tvarkymo operacijos aprašymą ir, kai taikoma, sertifikato panaikinimo datą ir priežastį arba sertifikato galiojimo sustabdymo datą, terminą ir priežastį. sertifikuojamas subjektas Susitarime turi patvirtinti, kad supranta, jog ši informacija bus įtraukta į Valdybos interneto svetainėje viešai prieinamą registrą; 8. sertifikuojamas subjektas įsipareigoja nustatyti išsamią skundų dėl sertifikavimo pažeidimų arba dėl to, kaip sertifikuotas duomenų valdytojas ar duomenų tvarkytojas įgyvendino ar įgyvendina įsipareigojimus pagal sertifikavimo kriterijus, nagrinėjimo procedūras ir struktūras bei užtikrinti, kad jos būtų skaidrios ir lengvai prieinamos, kaip tai nustatyta ISO 17065 standarto 4.1.2.2 papunkčio c dalies 2 įtraukoje, 4.1.2.2 papunkčio j dalyje ir Reglamento (ES) 2016/679 43 straipsnio 2 dalies d punkte; 9. Sertifikuojamas subjektas įsipareigoja informuoti Sertifikavimo įstaigą apie bet kokius priežiūros institucijų ar teismo nustatytus Reglamento (ES) 2016/679 ir kitų asmens duomenų apsaugą reglamentuojančių teisės aktų pažeidimus, galinčius turėti įtakos atitikties vertinimui. Ši informacija turi būti pateikta nedelsiant po to, kai informacija apie nustatytą pažeidimą tapo Sertifikuojamam subjektui žinoma; 10. atsižvelgiant į ISO 17065 standarto 4.1.2.2 papunkčio c dalies 1 įtrauką, nustatomos atitikties vertinimo galiojimo, atnaujinimo ir panaikinimo taisyklės, laikantis Reglamento (ES) 2016/679 42 straipsnio 7 dalies ir 43 straipsnio 4 dalies, įskaitant taisykles, susijusias su reguliariais pakartotinio atitikties vertinimo ar peržiūros intervalais pagal Reglamento (ES) 2016/679 42 straipsnio 7 dalį; 11. jei sertifikavimo įstaigos akreditavimo panaikinimas ar sustabdymas turėtų poveikį sertifikuojamam subjektui, papildomai prie ISO 17065 standarto 4.1.2.2 papunktyje nustatytų minimalių reikalavimų, Susitarime turi būti nurodomos sertifikavimo įstaigos akreditavimo panaikinimo ar sustabdymo pasekmės (pavyzdžiui, kad tokiu atveju sertifikavimo įstaigos išduotas sertifikatas netenka galios), o taip pat visos pasekmės duomenų subjektui ir kaip visos

		kilsiančios pasekmės bus sprendžiamos; 12. sertifikuojamas subjektas įsipareigoja informuoti sertifikavimo įstaigą apie sertifikavimo procesui ar atitikties sertifikavimo kriterijams reikšmingus jo faktinės ar teisinės padėties, sertifikavimo objekto pokyčius, reikšmingus atitikties vertinimui. *Pastaba Nr. 1. Reikšmingų faktinės ar teisinės padėties pokyčių pavyzdžiai pateikiami ISO 17065 standarto 4.1.2.2 papunkčio 3 pastaboje.* *Pastaba Nr. 2. Reikšmingais sertifikavimo objekto pokyčiais yra tokie pokyčiai, dėl kurių reikalingas naujas ar papildomas sertifikavimo objekto atitikties vertinimas, pavyzdžiui, asmens duomenų tvarkymo operacijos ar jai atlikti pasitelkiamų priemonių ar įrankių pasikeitimas, sertifikuojamo (sertifikuoto) proceso taikymo apimties išplėtimas, sąsajų tarp procesų ar paslaugų pasikeitimas, perdavimo kitoms sistemoms ar subjektams priemonių ar platformų pasikeitimas, techninių ir (ar) organizacinių saugumo priemonių pasikeitimas, duomenų gavėjų ar duomenų tvarkytojų pasikeitimas, su duomenų subjektų teisių įgyvendinimu susijusių technologinių sprendimų ir pasikeitimai kt.*
4.1.3.	**Duomenų apsaugos ženklų ir žymenų naudojimas**	Sertifikatai, ženklai ir žymenys naudojami tik laikantis Reglamento (ES) 2016/679 42 ir 43 straipsnių, taip pat Gairių Nr. 1/2018 ir Gairių Nr. 4/2018. Sertifikatai, ženklai ir žymenys turi būti naudojami skaidriai ir aiškiai, siekiant išvengti bet kokios klaidinančios informacijos apie sertifikuotų asmens duomenų tvarkymo operacijų apimtį. Nustačius neteisingos ar klaidinančios informacijos apie sertifikavimo mechanizmą skleidimo faktą arba netinkamą ar klaidinantį sertifikatų, ženklų ar žymenų naudojimą (dokumentuose ar viešai) turi būti imamasi šių veiksmų: 1. nutraukiamas sertifikatų, ženklų ir žymenų naudojimo pažeidimas; 2. viešai paskelbiama apie įvykdytus sertifikatų, ženklų ir žymenų naudojimo pažeidimus; 3. apie sertifikatų, ženklų ir žymenų naudojimo pažeidimus informuojama Inspekcija ir, kai taikoma, sertifikavimo įstaiga. 4. taip pat gali būti apribojamas sertifikatų, ženklų ir žymenų naudojimas. Inspekcija ar, kai taikoma, sertifikavimo įstaiga, įvertinusi pažeidimo aplinkybes ir kilusias (galėjusias kilti) pasekmes, gali teikti nurodymus dėl taisomųjų ar papildomų veiksmų, kurių turi imtis pažeidimą padaręs sertifikuotas subjektas.
4.2.	**Nešališkumo valdymas**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 4.2 papunktyje, sertifikavimo įstaiga turi:

		1. vadovaujantis Reglamento (ES) 2016/679 43 straipsnio 2 dalies a punktu, pateikti atskirus savo nepriklausomumo įrodymus. Visų pirma, tai taikoma sertifikavimo įstaigos finansavimo įrodymams, kiek jie susiję su nešališkumo patvirtinimu; 2. įrodyti, kad jos užduotys ir pareigos nesukels interesų konflikto pagal Reglamento (ES) 2016/679 43 straipsnio 2 dalies e punktą; 3. patvirtinti, kad nėra susijusi su Inspekcija ar jos darbuotojais; 4. identifikuoti galimas interesų konfliktų, kurie gali kilti teikiant sertifikavimo paslaugas, rizikas ir kokiomis priemonėmis šios rizikos bus valdomos. *Interesų konfliktų ar šališkumo pavyzdžiai*: 1. sertifikavimo įstaiga ar jos darbuotojas (įskaitant vadovybę) yra įsidarbinęs sertifikuojamame subjekte arba priklauso sertifikuojamo subjekto valdymo organams, turi sertifikuojamo subjekto nuosavybės teisių (yra jos narys, dalininkas, savininkas, akcininkas, kt.); 2. sertifikavimo įstaiga ar jos darbuotojas (įskaitant vadovybę) yra sertifikuojamo subjekto kreditorius arba turi kitų reikalavimo teisių į sertifikuojamo subjektą; 3. sertifikavimo įstaigos darbuotojas, įskaitant duomenų apsaugos pareigūną ir vadovybę, teikia duomenų apsaugos pareigūno paslaugas sertifikuojamam subjektui; 4. sertifikavimo įstaiga ar jos darbuotojai, įskaitant vadovybę, yra viena iš sutarties (išskyrus Susitarimą) su sertifikuojamu subjektu dėl komercinių paslaugų teikimo šalių; 5. sertifikavimo įstaigos esminę apyvartos dalį sudaro pajamos iš sertifikavimo paslaugų teikimo; 6. sertifikavimo įstaigos veiklą finansuoja sertifikuojamas subjektas; sertifikavimo įstaiga atitikties vertinimui nuomojasi darbuotojus iš kitų juridinių asmenų; 7. sertifikavimo įstaiga nuomos, panaudos ar kitais pagrindais naudojasi sertifikuojamo subjekto patalpomis; 8. sertifikavimo įstaigos darbuotojų mokymus ir kvalifikacijos kėlimą finansuoja sertifikuojamas subjektas, kt. Atitiktį šiam reikalavimui pagrindžiančių dokumentų pavyzdžiai: 1. sertifikavimo įstaigos įstatai; 2. sertifikavimo įstaigos dalyvių ir valdymo organų narių sąrašai ir informacija apie turimas kitų juridinių asmenų nuosavybės teises, dalyvavimą jų veikloje (pavyzdžiui, darbo santykiuose) ar priimant sprendimus valdymo veikloje; 3. Juridinių asmenų registro išplėstinis išrašas; 4. sertifikavimo įstaigos darbuotojų pareigybių aprašymai, jų atskaitomybės schema, atrankos proceso paaiškinimas (įskaitant, ar atrankos procesui turi įtakos kiti subjektai, ar kiti subjektai dalyvauja atrankos proceso metu, kokie yra

		darbuotojų darbo užmokesčio ar kitų susijusių išmokų ar mokymų finansavimo šaltiniai, kt.); 5. sertifikavimo įstaigos finansinės atskaitomybės dokumentai ir paaiškinimai apie jos finansavimo šaltinius, taip pat kokią įtaką sertifikavimo įstaigos apyvartai turės pajamos, gautos iš klientų sertifikavimo; 6. sertifikavimo įstaigos darbuotojų, įskaitant vadovų ir kitų valdymo organų narių, nepriklausomumo įsipareigojimų ir patvirtinimų apie galimus interesų konfliktus ir tai, kad jiems suprantama, kad kilus interesų konfliktų grėsmei, darbuotojai turi apie tai pranešti sertifikavimo įstaigos atsakingam asmeniui, formų pavyzdžiai. Turi būti nustatytas šių įsipareigojimų ir patvirtinimų valdymas ir priežiūra, pavyzdžiui, atnaujinimo intervalai (ne rečiau nei kartą per 1 metus), pasekmės už duomenų nepateikimą, neatnaujinimą ir pan.; 7. sertifikavimo įstaigos identifikuotų galimų nepriklausomumo ir šališkumo grėsmių, susijusių su jos veikla, jos santykiais, jos darbuotojų santykiais, aprašymas. 8. sertifikavimo įstaigos parengtos taisyklės, kurių turi laikytis jos darbuotojai, siekiant išvengti interesų konflikto ar grėsmių nepriklausomumui, pavyzdžiui, kaip, gavus dokumentus sertifikavimo paslaugai suteikti, bus vertinama, ar tarp sertifikavimo įstaigos (jos darbuotojų) ir sertifikuojamo subjekto gali kilti interesų konfliktas, kokie kriterijai identifikuos interesų konflikto grėsmę, kaip bus elgiamasi, jei bus pastebėtas interesų konfliktas (pavyzdžiui, darbuotojai įsipareigoja apie jį pranešti) ar mėginimai spausti sertifikavimo įstaigą ar jos darbuotojus priimti tam tikrą sprendimą ar imtis veiksmų, nesusijusių su sertifikavimo įstaigos užduotimis ar pareigomis ar jiems prieštaraujančių veiksmų. Sertifikavimo įstaiga parengtus dokumentus (tvarkas, taisykles, kt.) turi peržiūrėti ir, jei būtina, atnaujinti bent kartą per 1 metus; 9. sertifikavimo įstaigos parengta tvarka dėl pranešimų apie nepriklausomumo ar su interesų konfliktų valdymu susijusius pažeidimus terminus, jų tyrimą, dokumentavimą ir susijusių nurodymų vykdymo priežiūrą; 10. sertifikavimo įstaigos parengta skundų dėl sertifikavimo procedūros pateikimo ir nagrinėjimo tvarka. *Pastaba. Sertifikavimo įstaiga gali pateikti papildomus dokumentus, galinčius pagrįsti sertifikavimo įstaigos atitiktį nešališkumo valdymo reikalavimui.*
4.3.	**Atsakomybė ir finansavimas**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 4.3 papunktyje, sertifikavimo įstaiga turi pateikti dokumentus, pagrindžiančius, kad ji turi tinkamų priemonių įsipareigojimams, susijusiems su sertifikavimo paslaugų teikimu, vykdyti savo veiklos teritorijoje ir yra finansiškai stabili, pavyzdžiui:

		1. sertifikavimo įstaiga yra apdraudusi veiklą ar veiklos, susijusios su sertifikavimo paslaugų teikimu, dalį civilinės atsakomybės draudimu arba turi pakankamą rezervą tokiems įsipareigojimams (ieškiniams ir kt.) padengti; 2. sertifikavimo įstaigai nėra pradėta bankroto, nemokumo ar likvidavimo procedūra, pavyzdžiui, juridinių asmenų registro išrašas; 3. sertifikavimo įstaiga neturi įsiskolinimų, susijusių su įmokomis į valstybės biudžetą, pavyzdžiui, Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos pažyma; 4. sertifikavimo įstaigos ar jos darbuotojų atžvilgiu Lietuvos ir kitų valstybių narių akreditavimo įstaigos, kompetentingos priežiūros institucijos ar teismai nėra priėmę galutinių sprendimų dėl pažeidimų, susijusių su sertifikuojamos įstaigos veikla, apskaitos tvarkymu, pavyzdžiui, sertifikavimo įstaigos patvirtinimas (pažyma); 5. sertifikavimo įstaiga yra atlikusi sertifikavimo paslaugų teikimo rizikos ir jos poveikio sertifikuojamam subjektui vertinimą ir šio vertinimo pagrindu yra patvirtinusi nustatytos rizikos pašalinimo ar sumažinimo priemones. Sertifikavimo įstaiga turi kartą per metus pateikti Inspekcijai atnaujintą informaciją apie aukščiau nurodytas priemones, jų taikymą ir, kai taikoma, jų pasikeitimus.
4.4.	**Nediskriminacinės sąlygos**	Taikomi ISO 17065 standarto 4.4 papunkčio reikalavimai. Sertifikavimo įstaiga turi pateikti savo sertifikavimo mechanizmo aprašymą, nustatytus reikalavimus sertifikuojamiems subjektams ir kitus dokumentus ar informaciją, pagrindžiančią nediskriminacines sertifikavimo sąlygas.
4.5.	**Konfidencialumas**	Taikomi ISO 17065 standarto 4.5 papunkčio reikalavimai. Sertifikavimo įstaiga turi pateikti darbuotojų pasižadėjimus ar susitarimus saugoti asmens duomenų paslaptį, kitą konfidencialią informaciją, komercines paslaptis ar kitą neskelbtiną informaciją, kuri bus prieinama sertifikavimo paslaugų teikimo metu ar po jo (pavyzdžiui, ginant sertifikavimo įstaigos ar savo teises ikiteisminio tyrimo ar teisminėse institucijose). Konfidencialumo pareiga turi galioti tiek darbo ar kitų lygiaverčių santykių metu, tiek jiems pasibaigus. Tokiame pasižadėjime ar susitarime turi būti identifikuota jo taikymo apimtis, galiojimo terminas ir konfidencialumo pažeidimo pasekmės. Sertifikavimo įstaiga turi nustatyti jos naudojamų priemonių, įskaitant elektroninių, naudojimo tvarką, juose tvarkomų asmens duomenų naudojimo tvarką, prieigų suteikimo, keitimo ir panaikinimo tvarką, ir supažindinti su jomis darbuotojus.

4.6.	**Viešai skelbiama informacija**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 4.6 papunktyje, Sertifikavimo įstaiga turi savo interneto svetainėje viešai skelbti: 1. visas sertifikavimo kriterijų, kurie taikomi pagal Reglamento (ES) 2016/679 42 straipsnio 5 dalį, ir sertifikavimo procedūrų versijas (esamas ir ankstesnes), nurodant jų galiojimo datas; 2. vadovaujantis Reglamento (ES) 2016/679 43 straipsnio 2 dalies d punktu, informaciją apie skundų dėl sertifikavimo pažeidimų arba dėl to, kaip duomenų valdytojas ar duomenų tvarkytojas įgyvendino ar įgyvendina sertifikavimą nagrinėjimo procedūras ir pateiktas apeliacijas; 3. informaciją apie sertifikuotus subjektus, pateikiant šią informaciją: sertifikuoto objekto (asmens duomenų tvarkymo operacijos) aprašymą, nuorodą į sertifikavimo kriterijų versiją, atitikties vertinimo rezultatą ir galiojimo datą, taip pat, kai taikoma, sertifikato galiojimo sustabdymo ar panaikinimo datą. Aukščiau nurodyta informacija turi būti lengvai prieinama visiems.

5 SKYRIUS
STRUKTŪROS REIKALAVIMAI

Eil. Nr.	Reikalavimas	Reikalavimo paaiškinimai ir atitikties šiam reikalavimui patvirtinimo dokumentai ar informacija
5.1.	**Organizacinė struktūra ir aukščiausia vadovybė**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 5.1 papunktyje, sertifikavimo įstaiga turi paskirti bent 2 metų stažą asmens duomenų apsaugos teisės srityje turintį asmenį, atsakingą už asmens duomenų apsaugos reikalavimų laikymąsi ir informacijos valdymą, saugumo priemonių taikymą. Atitiktį šiam reikalavimui pagrindžiančių dokumentų pavyzdžiai: 1. organizacinės struktūros schema arba aprašymas, nurodant asmenų, dalyvaujančių atitikties vertinime pareigas, atsakomybes, atskaitomybę. Šiuo arba atskiru dokumentu taip pat turi būti pateikiama informacija, nurodyta ISO 17065 standarto 5.1.3 papunktyje. 2. schema arba kitoks aprašymas, nustatantys, kokiems asmenims kokia informacija, pavyzdžiui, apie galimus pažeidimus, interesų konfliktų rizikas, gautus skundus ir kt. teikiama. Šis punktas taikomas tuomet, kai informacija teikiama keliems asmenims.
5.2.	**Nešališkumo apsaugos mechanizmai**	Taikomi ISO 17065 standarto 5.2 papunkčio reikalavimai. Atitiktį šiam reikalavimui pagrindžiančių dokumentų pavyzdžiai nurodyti šio priedo 4.2. skiltyje, t. y.: 1. sertifikavimo įstaigos darbuotojų, įskaitant vadovų ir valdymo organų narių, nepriklausomumo įsipareigojimų ir patvirtinimų apie galimus interesų konfliktus ir tai, kad jiems suprantama,

		kad kilus interesų konfliktų grėsmei, turi apie tai pranešti sertifikavimo įstaigos atsakingam asmeniui formų pavyzdžiai. Turi būti nustatytas šių įsipareigojimų ir patvirtinimų valdymas ir priežiūra, pavyzdžiui, jų atnaujinimo intervalai (ne rečiau nei kartą per 1 metus), pasekmės už informacijos nepateikimą ar neatnaujinimą, taip pat nepranešimą apie kilusį ar galintį kilti interesų konfliktą ir pan.; 2. sertifikavimo įstaigos identifikuotų galimų nepriklausomumo ir nešališkumo grėsmių, susijusių su jos veikla, jos santykiais ar jos darbuotojų santykiais, aprašymas; 3. sertifikavimo įstaigos taikomos taisyklės, kurių turi laikytis jos darbuotojai, siekiant išvengti interesų konflikto ar grėsmės nepriklausomumui, pavyzdžiui, kaip, gavus dokumentus sertifikavimo paslaugai suteikti, bus vertinama, ar tarp sertifikavimo įstaigos (jos darbuotojų) ir sertifikuojamo subjekto gali kilti interesų konfliktas, kokie kriterijai identifikuos interesų konflikto grėsmę, kaip bus elgiamasi, jei bus pastebėtas interesų konfliktas (pavyzdžiui, darbuotojai įsipareigoja apie tai pranešti sertifikavimo įstaigos atsakingam asmeniui, kad jis gautą užduotį paskirtų kitam asmeniui) ar mėginimą paveikti sertifikavimo įstaigą ar jos darbuotojus priimti tam tikrą sprendimą ar imtis veiksmų, nesusijusių su sertifikavimo įstaigos užduotimis ar pareigomis ar jiems prieštaraujančių. Sertifikavimo įstaigos parengtus dokumentus (tvarkas, taisykles, kt.) turi peržiūrėti ir, jei būtina, atnaujinti bent kartą per 1 metus; 4. sertifikavimo įstaigos tvarka dėl pranešimo apie nepriklausomumo ar su interesų konfliktų valdymu susijusius pažeidimus, pranešimų terminus, jų tyrimą, dokumentavimą; 5. sertifikavimo įstaigos skundų dėl sertifikavimo procedūros pateikimo ir nagrinėjimo tvarka. *Pastaba. Sertifikavimo įstaiga gali pateikti papildomus dokumentus, galinčius pagrįsti sertifikavimo įstaigos atitiktį nešališkumo valdymo reikalavimui.*

6 SKYRIUS
REIKALINGI IŠTEKLIAI

Eil. Nr.	Reikalavimas	Reikalavimo paaiškinimai ir atitikties šiam reikalavimui patvirtinimo dokumentai ar informacija
6.1.	**Sertifikavimo įstaigos darbuotojai**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 6.1 papunktyje, Sertifikavimo įstaiga turi užtikrinti, kad jos darbuotojai: 1. turi atitikties sertifikavimo kriterijams vertinimui reikalingų aktualių žinių, įskaitant susijusių su asmens duomenų apsaugos teisės aktais ir jų taikymo praktika, pavyzdžiui, reguliariai dalyvauja praktiniuose mokymuose asmens duomenų tvarkymo ir saugumo užtikrinimo klausimais, su asmens duomenų

		tvarkymo operacijų atitikties Reglamento (ES) 2016/679 reikalavimams vertinimo ir susijusių dokumentų rengimo klausimais, poveikio duomenų apsaugai vertinimo ir (ar) rizikos vertinimo atlikimo klausimais, techninių ir organizacinių saugumo priemonių atrankos klausimais ir kt.; 2. turi pakankamai patirties asmens duomenų apsaugos srityje, pavyzdžiui, vykdė duomenų apsaugos pareigūno funkcijas, rengė asmens duomenų tvarkymo operacijų atitikties Reglamento (ES) 2016/679 ir kitų asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimams dokumentus, teikė konsultacijas asmens duomenų saugumo užtikrinimo, techninių ir organizacinių priemonių vertinimo ir atrankos klausimais, teikė duomenų valdytojų (duomenų tvarkytojų) veiklos ar atskirų procesų atitikties Reglamento (ES) 2016/679 reikalavimams audito ar kitokio vertinimo paslaugas, kt.; 3. turi ekspertinių žinių apie sertifikavimo objektą, atsižvelgiant į Reglamento (ES) 2016/679 43 straipsnio 2 dalies a punktą, pavyzdžiui, darbo patirtį ekspertinėje veikloje, susijusioje su prekių, paslaugų ar procesų sertifikavimu, auditavimu ar kitais analogiškais vertinimais, valdymo sistemomis, turi 2 metų patirtį veikloje, susijusioje su sertifikuojamu objektu; 4. yra nepriklausomi ir jų funkcijos ir atskaitomybė sertifikavimo įstaigos veikloje nesukels interesų konflikto (darbuotojų nepriklausomumo ir interesų konfliktų grėsmių vertinimas atliekamas atsižvelgiant į ISO 17065 standarto 4.2 papunkčio ir šio Priedo 4.2 papunkčio reikalavimus), atsižvelgiant į Reglamento (ES) 2016/679 43 straipsnio 2 dalies a ir e punktus; 5. įsipareigoję laikytis Reglamento (ES) 2016/679 42 straipsnio 5 dalyje nurodytų reikalavimų pagal 43 straipsnio 2 dalies b punktą; 6. turi reikiamų ir tinkamų žinių apie asmens duomenų technines ir organizacines saugumo priemones, joms keliamus reikalavimus, įskaitant, bet neapsiribojant, Europos Sąjungos kibernetinio saugumo agentūros rekomendacijose, ISO standartuose LST ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ bei ISO/IEC 27701:2019 „Saugumo metodai–ISO/IEC 27001 ir ISO/IEC 27002 papildymas dėl privatumo valdymo–Reikalavimai ir gairės“ ir prireikus jų taikymo patirties“ ir jų taikymo patirties; Sertifikavimo įstaiga turi sugebėti įrodyti, kad jos techninės patirties

		turintys darbuotojai: 1. yra įgiję atitinkamos techninių žinių srities kvalifikaciją, kuri atitinka bent šeštą Europos kvalifikacijų sandaros lygmenį[1], arba atitinkamos reglamentuojamos profesijos pripažintą saugomą vardą (pvz., technologijos mokslų daktaras), arba turėti bent 5 metų profesinę patirtį informacinių technologijų srityje, pavyzdžiui, informacijos saugumo sistemų, saugumo valdymo sistemų, informacijos saugumo rizikos valdymo ir kt. 2. už sprendimų dėl sertifikavimo priėmimą atsakingi darbuotojai turi turėti bent 3 metų profesinę patirtį duomenų apsaugos priemonių nustatymo ir įgyvendinimo srityje. 3. už atitikties vertinimą atsakingi darbuotojai turi turėti bent 2 metų profesinę patirtį duomenų apsaugos srityje ir ekspertinių žinių apie sertifikavimo, audito ar panašią procedūrą bei darbo su ja patirties. 4. turi įrodyti, kad jie tobulina tam tikros srities kompetenciją, susijusią su techninėmis ir audito žiniomis, dalyvavimu tęstinio profesinio tobulėjimo programose. Sertifikavimo įstaiga turi sugebėti įrodyti, kad jos teisinės patirties turintys darbuotojai: 1. yra baigę teisės studijas Europos Sąjungos arba Lietuvos Respublikos pripažintame universitete, kurių trukmė buvo bent aštuoni semestrai ir po kurių buvo suteiktas akademinis magistro (LL.M.) arba lygiavertis laipsnis, arba turėti bent 5 metų teisinio darbo patirtį. 2. už sprendimų dėl sertifikavimo priėmimą atsakingi darbuotojai turi įrodyti, kad yra sukaupę bent 3 metų profesinę patirtį duomenų apsaugos teisės srityje. 3. už Atitikties vertinimo atlikimą atsakingi darbuotojai turi įrodyti, kad turi pakankamą profesinę patirtį duomenų apsaugos teisės srityje ir žinių bei patirties, susijusios su panašiomis procedūromis (pvz., sertifikavimu ir (arba) auditu) ir (ar) sertifikuojamu objektu; 4. turi įrodyti, kad jie tobulina tam tikros srities kompetenciją, susijusią su teisinėmis ir audito atlikimo žiniomis, dalyvavimu tęstinio profesinio tobulėjimo programose. Atitiktį šiam reikalavimui pagrindžiančių dokumentų pavyzdžiai, be nurodytų šio priedo 4.2. skiltyje ir ISO 17065 standarto 4.2 papunktyje: 1. dokumentai, atitinkantys ISO 17065 standarto 6.1.2.1, 6.1.2.2 ir 6.1.3 papunkčių, šio priedo 4.5 skilties reikalavimus; 2. sertifikavimo įstaigos dokumentas, pagrindžiantis, kokie reikalavimai vertintojų žinioms, įgūdžiams ir patirčiai yra būtini konkretaus sertifikuojamo objekto kontekste;

[1] https://ec.europa.eu/ploteus/en/compare?field_location_selection_tid%5B%5D=455&field_location_selection_tid%5B%5D=471

		3. Vertintojų sertifikatai ir (ar) pažymėjimai, patvirtinantys dalyvavimą mokymuose, seminaruose, kursų baigimą aukščiau nurodytose srityse, kurie yra ne senesni nei pastarųjų 2 metų; 4. Vertintojų išsilavinimą patvirtinantys dokumentai (kai susiję su atitiktimi aukščiau nurodytiems reikalavimams); 5. Vertintojų gyvenimo aprašymas, jame pateikiant darbo funkcijų aprašymą, pagrindžiantį aktualias (ekspertines) žinias, patirtį; 6. Vertintojų rašytinis įsipareigojimas laikytis Reglamento (ES) 2016/679 42 straipsnio 5 dalyje nurodytų reikalavimų pagal Reglamento (ES) 2016/679 43 straipsnio 2 dalies b punktą; 7. dokumentai, patvirtinantys Vertintojų stažuotes ar dalyvavimą darbuotojų mainų programose, įskaitant stažuočių ar Vertintojų mainų programos aprašymą, funkcijas, užduotis ir kt. (kai susiję su atitiktimi aukščiau nurodytiems reikalavimams); 8. Vertintojų ar kandidatų į Vertintojų, jų praktinių įgūdžių ir (ar) žinių asmens duomenų apsaugos srityje, įmonių atitikties vertinimo srityje ir (ar) jų ir (ar) žinių apie techninių ir organizacinių saugumo priemones ir jų taikymą ir (ar) jų taikymo patirtį, vertinimus (jų rezultatus); 9. Vertintojų patikrinimų dėl sertifikavimo įstaigos nustatytų taisyklių ir (ar) kitokių instrukcijų, susijusių su asmens duomenų tvarkymo ir saugumo užtikrinimo reikalavimais, laikymosi rezultatus.
6.2.	**Vertinimo ištekliai**	Taikomi ISO 17065 standarto 6.2 papunkčio reikalavimai.

7 SKYRIUS
REIKALAVIMAI SERTIFIKAVIMO PROCESUI

Eil. Nr.	Reikalavimas	Reikalavimo paaiškinimai ir atitikties šiems reikalavimams patvirtinimo dokumentai ar informacija
7.1.	**Bendrieji reikalavimai**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.1 papunktyje, sertifikavimo įstaiga turi užtikrinti, kad: 1. atitinka Inspekcijos nustatytus papildomus reikalavimus (pagal Reglamento (ES) 2016/679 43 straipsnio 1 dalies b punktą), siekiant, kad sertifikavimo įstaigos užduotys ir pareigos nesukeltų interesų konflikto (pagal Reglamento (ES) 2016/679 43 straipsnio 2 dalies e punktą); 2. prieš pradėdama naudoti patvirtintą Europos duomenų apsaugos ženklą padalinio veikloje naujoje valstybėje narėje, informuotų kompetentingas duomenų apsaugos priežiūros institucijas; 3. yra parengusi Inspekcijos informavimo tvarką apie siekiamus priimti sprendimus dėl sertifikatų. Šia tvarka turi būti užtikrinta, kad: 3.1. Inspekcija būtų nedelsiant informuojama apie sertifikatų išdavimą, atnaujinamą, panaikinimą ir tokių sprendimų

		priežastis; 3.2. informacija Inspekcijai būtų pateikta prieš sertifikatų išdavimą, atnaujinamą, panaikinimą; 3.3. teikiant Inspekcijai informaciją, sertifikavimo įstaiga turi pateikti sertifikuojamo subjekto vertinimo išvados santraukos kopiją (papildomai žr. šio priedo 7.8 skiltį). 4. Tuo atveju, jei Inspekcija ar sertifikuojamas subjektas informuoja sertifikavimo įstaigą apie bet kokį Inspekcijos atliekamą reikšmingą ir su sertifikuojamu objektu susijusį tyrimą sertifikuojamo subjekto atžvilgiu ar jam pritaikytus taisomuosius veiksmus, dėl kurių kyla ar gali kilti abejonių dėl sertifikuojamo subjekto atitikties asmens duomenų apsaugos reikalavimams, sertifikavimo įstaiga turi atlikti gautos informacijos tyrimą ir įvertinti jos poveikį sertifikavimo įstaigos atliktam vertinimui (ir jo išvadai). Atlikusi tyrimą, sertifikavimo įstaiga turi pateikti Inspekcijai pranešimą apie tai, ar sertifikuojamas subjektas vis dar atitinka sertifikavimo kriterijus. Šis sertifikavimo įstaigos tyrimas turi būti susijęs su sertifikavimo apimtimi ir vertinimo tikslu. 5. Jei Inspekcija, gavusi aukščiau nurodytą informaciją, pateikia sertifikavimo įstaigai nurodymą (ar sprendimą) atsisakyti išduoti sertifikatą ar panaikinti sertifikavimo įstaigos išduotą sertifikatą, sertifikavimo įstaiga turi įsipareigoti tokį nurodymą (ar sprendimą) vykdyti.
7.2.	**Paraiška**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.2 papunktyje, sertifikavimo įstaiga Prašyme turi reikalauti: 1. išsamiai aprašyti sertifikavimo objektą (vertinimo objektą), įskaitant sąsajas su kitomis sistemomis, teikimą į kitas sistemas ir kitiems gavėjams, protokolus ir kitas garantijas; 2. nurodyti, ar yra duomenų valdytojų, kurie sertifikavimo objekto kontekste, su sertifikuojamu subjektu veiks kaip bendri duomenų valdytojai. Jei taip, aprašyti jų atsakomybes ir įsipareigojimus. 3. nurodyti, ar pasitelkiami duomenų tvarkytojai. Jei sertifikuojamas subjektas yra duomenų tvarkytojas, paraiškoje turi būti aprašoma jo atsakomybė ir užduotys. 4. tuo atveju, jei sertifikavimo objektas apima ir asmens duomenų perdavimą į trečiąsias valstybes, paraiškoje turi būti reikalaujama nurodyti perduodamus asmens duomenis, jų gavėjus ir asmens duomenų saugumo priemones, kurios bus tokiu atveju taikomos; 5. nurodyti, ar priežiūros institucijos sertifikuojamo subjekto atžvilgiu atlieka tyrimą ar yra jį atlikusios. Jei taip, aprašyti baigtus tyrimus, kurių metu buvo nustatyti asmens duomenų tvarkymo pažeidimai (trumpas pažeidimo aprašymas, sprendimo data ir taikyti taisomieji veiksmai). Jei tyrimas atliekamas, trumpai aprašyti dėl ko.

		Atitiktį šiam reikalavimui pagrindžiantys dokumentai, be nurodytų ISO 17065 standarto 7.2 papunkčio 1 ir 2 pastabose: 1. bendrų duomenų valdytojų sutartis(-ys), kai taikomas šio priedo 7.2 skilties 2 reikalavimas; 2. asmens duomenų tvarkymo sutartis(-ys), kai taikomas šio priedo 7.2 skilties 3 reikalavimas; 3. dokumentai, nurodyti Reglamento (ES) 2016/679 46 ir (ar) 49 straipsnyje, pavyzdžiui, pasirašytos standartinės sutarčių sąlygos, patvirtintos įmonei privalomos taisyklės, duomenų subjekto sutikimas ir kt., kai taikomas šio priedo 7.2 skilties 4 reikalavimas.
7.3.	**Paraiškos peržiūra**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.3 papunktyje, sertifikavimo įstaiga turi pateikti kriterijus, kuriais remiantis sertifikavimo įstaiga vertins, ar asmens duomenų apsaugos srityje sertifikuojamas subjektas turi pakankamą kompetenciją (atsižvelgiant į technines ir teisines žinias) vertinti sertifikavimo objektą (ISO 17065 standarto 7.3.1 papunkčio e dalies reikalavimo kontekste). Sertifikavimo objekto vertinimo kriterijai turi būti nurodyti Susitarime. Atitiktį šiam reikalavimui pagrindžiančių dokumentų pavyzdžiai: 1. sertifikavimo įstaigos patvirtintos sertifikavimo objekto vertinimo taisyklės (ar kitas analogiškas dokumentas), kuriose aptarti sertifikavimo įstaigos kompetencijos sertifikavimo objekto kontekste vertinimo kriterijai ir vertinimo procesas *arba* 2. Susitarimas.
7.4.	**Vertinimas**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.4 papunktyje, sertifikavimo įstaiga turi: 1. sertifikavimo mechanizme aprašyti atitikties vertinimo metodus, pavyzdžiui (kai taikytina sertifikavimo objektui): 1.1. asmens duomenų tvarkymo operacijų būtinumo ir proporcingumo vertinimo metodus. Šio vertinimo metu turi būti atsižvelgiama į asmens duomenų tvarkymo tikslą ir duomenų subjektus, kurių asmens duomenys tvarkomi nurodytu tikslu; 1.2. metodus, kuriais sertifikavimo įstaiga vertins rizikų, kurias identifikavo ir įvertino sertifikuojamas subjektas (kaip duomenų valdytojas ar duomenų tvarkytojas), nagrinėdamas teisines pasekmes, kylančias asmens duomenų tvarkymo operacijų kontekste ir susijusias su Reglamento (ES) 2016/679 30, 32, 35 ir 36 straipsniu įgyvendinimu, taip pat pagal Reglamento (ES) 2016/679 24, 25 ir 32 straipsnius nustatytas technines ir organizacines priemones identifikuotų rizikų suvaldymui ar sumažinimui, apimtį, turinį ir sertifikuojamo subjekto atliktą vertinimą; 1.3. duomenų subjektų teisių gynimo priemonių, įskaitant asmens duomenų saugumo užtikrinimo priemones, garantijas ir

		asmens duomenų apsaugos užtikrinimo tvarką, vertinimo metodus. Vertinant teisių gynimo priemones atsižvelgiama į sertifikavimo objektą ir įrodymus, kuriais sertifikuojamas subjektas grindžia teisinių reikalavimų, taikomų Atitikties vertinimo metu, laikymąsi; 1.4. dokumentuoti taikytus vertinimo metodus ir vertinimo rezultatus. 2. užtikrinti, kad atitikties vertinimo metodai būtų standartizuoti ir visuotinai taikomi. Tai reiškia, kad palyginami vertinimo metodai taikomi palyginamiems sertifikavimo objektams. Sertifikavimo įstaiga turi pagrįsti bet kokį nukrypimą nuo šios procedūros. 3. teisę, papildomai prie ISO 17065 standarto 7.4.2 papunktyje nustatytų reikalavimų, atitikties vertinimui pasitelkti išorinius ekspertus, jei, sertifikavimo įstaigos vertinimu, šie ekspertai atitinka šio priedo 6.1 skilties reikalavimus. *Sertifikavimo įstaiga tokiu atveju turi pateikti* dokumentus, patvirtinančius tokio vertinimo atlikimą ir jo rezultatus, o jei esant Inspekcijos prašymui, su išorės ekspertais pasirašytas sutartis dėl atitikties vertinimo atlikimo. 4. atlikdama atitikties vertinimą atsižvelgti, papildomai prie ISO 17065 standarto 7.4.5 papunktyje nustatytų reikalavimų, į sertifikuojamo subjekto turimus galiojančius sertifikatus, jei jie apima visą ar dalį sertifikavimo, dėl kurio kreipėsi sertifikuojamas subjektas, objekto. Sertifikavimo įstaiga tokiu atveju turi įvertinti sertifikuojamo objekto atitiktį sertifikavimo kriterijams, kiek tai susiję su asmens duomenų apsaugos sertifikavimu pagal Reglamento (ES) 2016/679 42 ir 43 straipsnius. Kitaip tariant, turimi galiojantys sertifikatai negali savaime reikšti, kad sertifikuojamas objektas atitinka sertifikavimo kriterijus. Sertifikavimo įstaiga turi nustatyti, kad sertifikuojamas subjektas nurodytu atveju turi pateikti pilną vertinimo išvadą, kurios pagrindu buvo išduotas sertifikatas, ar kitą informaciją, sudarančią sąlygas įvertinti sertifikuojamo subjekto turimą galiojantį sertifikatą ir jo taikymo apimtį, pavyzdžiui, vertinimo kriterijus, vertinimo metodus, vertinimo apimtį ir kt. Sertifikavimo įstaigos atliktas galiojančių sertifikatų vertinimas turi būti išsamiai aprašytas sertifikavimo įstaigos išvadoje dėl naujos paraiškos atitikties sertifikavimo kriterijams. 5. sertifikavimo mechanizme aprašyti, kaip bus įgyvendinama ISO 17065 standarto 7.4.6 papunktyje nustatyta sertifikuojamo subjekto informavimo pareiga, nustatant bent informavimo pobūdį ir terminus. 6. papildomai prie ISO 17065 standarto 7.4.9 papunktyje nustatytų reikalavimų, sudaryti sąlygas, esant Inspekcijos prašymui, bet kuriuo metu susipažinti su visais atitikties vertinimo dokumentais.

7.5.	**Peržiūra**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.5 papunktyje, sertifikavimo įstaiga turi: 1. nustatyti sertifikatų išdavimo, reguliarios peržiūros ir panaikinimo tvarką, laikantis Reglamento (ES) 2016/679 43 straipsnio 2 ir 3 dalių; 2. papildomai prie ISO 17065 standarto 7.5.1 papunktyje nustatytų reikalavimų, pagrįsti, kad peržiūrai paskirtas asmuo nedalyvavo (tiesiogiai ar netiesiogiai) atitikties vertinimo metu. Atitiktį šio reikalavimo antram reikalavimui pagrindžiančių dokumentų pavyzdžiai: 1. dokumentas, kuriame pateiktas asmenų, dalyvavusių atliekant atitikties vertinimą, sąrašas, jame aprašant kiekvieno dalyvavusio asmens vaidmenį ir atskaitomybę; 2. dokumentas (tvarka, taisyklės, kt.), kuriame aprašyta, kaip atrenkami ir skiriami asmenys atlikties vertinimui ir atlikto vertinimo peržiūrai; 3. dokumentas, pagrindžiantis, kad asmenys, kurie paskiriami peržiūrėti vertinimo rezultatus ir susijusią informaciją, yra supažindinti su jų pareiga informuoti juos skyrusį asmenį apie savo dalyvavimą atliekant atitikties vertinimą.
7.6.	**Sprendimas dėl sertifikavimo**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.6 papunktyje, sertifikavimo įstaiga turi: 1. išsamiai aprašyti, kaip bus užtikrinamas jos nepriklausomumas ir atsakomybė, priimant individualius sprendimus dėl sertifikavimo; 2. prieš priimdama sprendimą dėl sertifikavimo (išdavimo, atnaujinimo), įsitikinti, ar priežiūros institucijose nėra sertifikuojamo subjekto atžvilgiu pradėtų tyrimų, rodančių, kad klientas neatitinka sertifikavimo kriterijų. Įgyvendinant šį reikalavimą, priežiūros institucijai turi būti pateiktas sprendimo projektas ir atitikties vertinimo išvada ar jos santrauka, nurodant atitiktį sertifikavimo kriterijams pagrindžiančius argumentus ir sertifikato išdavimo ar atnaujinimo priežastis; 3. Sprendime dėl sertifikavimo turi būti nurodyta sertifikuojamo subjekto teisė priimtą sprendimą apskųsti ir skundo pateikimo terminas. Atitiktį šiam reikalavimui pagrindžiančių dokumentų pavyzdžiai: 1. sprendimų dėl sertifikavimo priėmimo tvarka, kurioje, be sprendimų priėmimo procedūros, aprašyta, kaip bus užtikrinamas sertifikavimo įstaigos nepriklausomumas ir atsakomybė; 2. sertifikuojamo subjekto patvirtinimas, kad prieš jį priežiūros institucijose nėra ir, kai taikoma, nebuvo pradėtų tyrimų dėl galimų pažeidimų, susijusių su sertifikavimo objektu ar galinčių turėti įtakos sertifikuojamo subjekto atitikties

		vertinimui; 3. sertifikavimo įstaigos įsipareigojimas kreiptis į priežiūros instituciją, siekiant patikrinti, ar sertifikuojamo subjekto pateikta informacija dėl sertifikuojamo subjekto atžvilgiu atliekamų tyrimų yra teisinga (tai gali būti nustatyta sprendimų dėl sertifikavimo priėmimo tvarkoje); 4. dokumentas, kuriame pateiktas asmenų, dalyvavusių atliekant atitikties vertinimą, sąrašas, jame aprašant kiekvieno dalyvavusio asmens vaidmenį ir atskaitomybę; 5. dokumentas (tvarka, taisyklės, kt.), kuriame aprašyta, kaip atrenkami ir skiriami asmenys Atlikties vertinimui ir sprendimo dėl sertifikavimo priėmimui, išskyrus atvejus, kai sprendimą dėl sertifikavimo priims sertifikavimo įstaigos vadovas; 6. dokumentas, pagrindžiantis, kad asmenys, kurie paskiriami priimti sprendimą dėl sertifikavimo, yra supažindinti su jų pareiga informuoti juos skyrusį asmenį apie savo dalyvavimą atliekant atitikties vertinimą, išskyrus atvejus, kai sprendimą dėl sertifikavimo priims sertifikavimo įstaigos vadovas; 7. sutartį, nurodytą ISO 17065 standarto 7.6.3 papunktyje; 8. sertifikavimo įstaigos atitiktį organizacinės struktūros reikalavimui, nustatytam ISO 17065 standarto 7.6.4 papunktyje, patvirtinantį dokumentą, pavyzdžiui, Juridinių asmenų registro išrašą ar Juridinių asmenų dalyvių informacinės sistemos suformuotą sąrašą.
7.7.	**Sertifikavimo dokumentai**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.7.1 papunkčio e dalyje, sertifikavimo įstaiga turi užtikrinti, kad: 1. atsižvelgiant į Reglamento (ES) 2016/679 42 straipsnio 7 dalį, sertifikato galiojimo laikotarpis neviršytų 3 metų; 2. reguliari (bent kartą per metus) priežiūra, laikantis šio priedo 7.9 skilties reikalavimų, būtų patvirtinta dokumentais. Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.7.1 papunkčio f dalyje, sertifikavimo įstaiga turi: 1. sertifikate aiškiai identifikuoti sertifikavimo objektą ir jį aprašyti (jei taikoma, nurodant versiją ar panašias charakteristikas); 2. jei dėl objektyvių priežasčių dalis sertifikavimo kriterijų nebuvo vertinti (pavyzdžiui, jie konkrečiu atveju netaikomi), tuomet sertifikavimo įstaiga turi pateikti Inspekcijai tokių kriterijų sąrašą ir priežastis, dėl kurių jie nebuvo vertinti. Sertifikavimo įstaiga, išdavusi sertifikatą, jo kopiją turi pateikti Inspekcijai. Atitiktį šiam reikalavimui pagrindžiančių dokumentų pavyzdžiai: 1. sertifikato, kuris bus išduodamas sertifikuojamiems subjektams, atitinkančio ISO 17065 standarto 7.7.1 – 7.7.2 papunkčiuose nustatytus turinio reikalavimus, pavyzdys;

		2. sertifikavimo įstaigos įsipareigojimas vykdyti reguliarią išduotų sertifikatų priežiūrą, nustatant priežiūros periodiškumą, taip pat dokumentas, pagrindžiantis šios priežiūros vykdymo tvarką ir terminus; 3. sertifikavimo įstaigos įsipareigojimas išduoti sertifikatą tik esant visoms ISO 17065 standarto 7.7.3 papunktyje nustatytoms sąlygoms arba dokumentas, nustatantis sertifikato išdavimo tvarką, jei jame yra aptartas ISO 17065 standarto 7.7.3 papunkčio reikalavimas.
7.8.	**Sertifikuotų produktų katalogas**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.8 papunktyje, sertifikavimo įstaiga turi: 1. skelbti informaciją apie sertifikuotą objektą (prekes, procesus ir paslaugas), sertifikato išdavimo (atnaujinimo) datą ir galiojimo terminą. 2. viešai paskelbti atitikties sertifikavimo kriterijams vertinimo ataskaitos santrauką, kurios tikslas – informuoti apie tai, kas buvo sertifikuota ir kaip buvo atliekamas atitikties vertinimas. Šioje santraukoje turi būti pateikta ši informacija: 2.1. sertifikavimo apimtis ir išsamus sertifikavimo objekto aprašymas; 2.2. sertifikavimo kriterijai, įskaitant jų versiją ir statusą; 2.3. atlikti vertinimai ir jų metodai; 2.4. vertinimo rezultatas; 3. atsižvelgiant į Reglamento (ES) 2016/679 43 straipsnio 5 dalį, sertifikavimo įstaiga pateikia Inspekcijai sprendimo dėl sertifikavimo ar jo panaikinimo priežastis. Tuo atveju, jei sertifikatas buvo išduotas, Inspekcijai pateikiama išduoto sertifikato kopija. Jei Inspekcija, gavusi aukščiau nurodytą informaciją, pateikia sertifikavimo įstaigai nurodymą (ar sprendimą) atsisakyti išduoti sertifikatą ar panaikinti sertifikavimo įstaigos išduotą sertifikatą, sertifikavimo įstaiga turi įsipareigoti tokį nurodymą (ar sprendimą) vykdyti.
7.9.	**Priežiūra**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.9.1 – 7.9.3 papunkčiuose, atsižvelgiant į Reglamento (ES) 2016/679 43 straipsnio 2 dalies c punktą, sertifikavimo įstaiga turi: 1. reguliariai (bent kartą per metus) vykdyti išduotų sertifikatų peržiūrą. Peržiūros priemonės turi būti pasirenkamos, atsižvelgiant į galinčias kilti rizikas, jei nebūtų laikomasi įsipareigojimų, susijusių su išduotu sertifikatu. 2. dokumentuoti priežiūros procedūrą, nustatant: 2.1. rizikos asmens duomenų apsaugai vertinimo kriterijus; 2.2. priežiūros vykdymo terminus ir intervalus; 2.3. galimas taikyti priežiūros priemones; 2.4. priežiūros vykdymo tvarką (įskaitant tikrinimą vietoje be išankstinio įspėjimo);

		2.5. sprendimus, kurie priimami atlikus priežiūrą (t. y. priežiūros pasekmes).
7.10.	**Pakeitimai, turintys įtakos sertifikavimui**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.10.1–7.10.3 papunkčiuose, pakeitimai, turintys įtakos sertifikavimui, kuriuos sertifikavimo įstaiga turi įvertinti, yra: 1. Inspekcijos ar teismo nustatyti Reglamento (ES) 2016/679 ir (ar) kitų asmens duomenų apsaugą reglamentuojančių teisės aktų pažeidimai ar asmens duomenų saugumo pažeidimai, susiję su sertifikuojamu objektu ar turintys įtakos atitikties vertinimui; 2. esminiai asmens duomenų apsaugos operacijų, kurios yra (buvo) sertifikuotos, pasikeitimai; 3. asmens duomenų apsaugą reglamentuojančių teisės aktų pakeitimai; 4. Europos Komisijos priimti deleguotieji ar įgyvendinimo aktai, vadovaujantis Reglamento (ES) 2016/679 43 straipsnio 8 dalimi ir 43 straipsnio 9 dalimi; 5. Valdybos priimti sprendimai, nuomonės, gairės, rekomendacijos ar gerosios praktikos; 6. teismų sprendimai, susiję su asmens duomenų apsauga; 7. techninių ir organizacinių priemonių pažanga. Sertifikavimo įstaiga turi nustatyti pakeitimų vertinimo, ar sertifikuojamo subjekto informavimo ir pakeitimų įgyvendinimo tvarką, nustatant: 1. sertifikuojamų asmens duomenų apsaugos operacijų, aprašytų paraiškoje, pasikeitimų ar informacijos apie sertifikuojamo subjekto pažeidimus įtakos sertifikavimo procesui ar išduotam sertifikatui vertinimo kriterijus (kai apie pakeitimus praneša sertifikuojamas subjektas); 2. pakeitimų, apie kuriuos kyla pareiga pranešti sertifikuotam subjektui ir, kai tikslinga, atitinkamų pakeitimų (dokumentų tikslinimų, asmens duomenų tvarkymo operacijų taikymo apimties susiaurinimui, kt.) inicijavimo poreikį, vertinimo kriterijus; 3. sertifikuoto subjekto informavimo apie pakeitimus, galinčius turėti įtakos, atitikties vertinimui ar išduoto sertifikato galiojimui, tvarką ir terminus; 4. pereinamojo laikotarpio trukmę; 5. pakeitimų patvirtinimo Inspekcijoje inicijavimo procesą; 6. atitinkamo sertifikavimo objekto pakartotinį vertinimą ir jo tvarką; 7. priemones sertifikatui panaikinti, jei sertifikuota tvarkymo operacija nebeatitinka atnaujintų kriterijų.
7.11.	**Sertifikato galiojimo nutraukimas, sutrumpinimas, sustabdymas arba**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.11.1 papunktyje, sertifikavimo įstaiga turi nedelsiant raštu informuoti Inspekciją apie: 1. jos taikytas (ar planuojamas taikyti) priemones (pavyzdžiui,

	panaikinimas	pakartotinį atitikties vertinimą, vertinimo peržiūrą, priimto sprendimo peržiūrą, kt.) ir jų taikymo priežastis; 2. sertifikato atnaujinimą, apribojimą, sustabdymą ar panaikinimą. Atsižvelgiant į Reglamento (ES) 2016/679 58 straipsnio 2 dalies h punktą, sertifikavimo įstaiga turi įsipareigoti vykdyti Inspekcijos sprendimus ir nurodymus panaikinti sertifikavimo įstaigos išduotą sertifikatą arba jo neišduoti, jei nesilaikoma arba nebesilaikoma sertifikavimo kriterijų. Sertifikavimo įstaiga tokiu atveju turi Inspekcijai pateikti įrodymus, pagrindžiančius nurodymo ar sprendimo įvykdymą. *Pastaba Nr.1. Inspekcijai ar teismui nustačius, kad sertifikuojamas (sertifikuotas) subjektas padarė sunkų Reglamento (ES) 2016/679 ir (ar) kitų asmens duomenų apsaugą reglamentuojančių teisės aktų pažeidimą ar reikšmingą asmens duomenų saugumo pažeidimą, laikoma, kad sertifikuojamas subjektas nesilaiko arba nebesilaiko sertifikavimo kriterijų. Vertinant, ar pažeidimas gali būti laikomas sunkiu ar reikšmingu, atsižvelgiama į pažeidimo pobūdį, sunkumą, trukmę, nukentėjusių duomenų subjektų skaičių ir jų patirtos žalos dydį, asmens duomenų, kuriems pažeidimas turi poveikį, kategorijas, veiksmus, kurių sertifikuojamas subjektas ėmėsi, kad sumažintų duomenų subjektų patirtą ar kitą pažeidimu sukeltą žalą, kt.* *Pastaba Nr. 2. sertifikato apribojimu laikytinas sertifikavimo taikymo apimties sumažinimas. Tokiu atveju sertifikavimo įstaiga turi imtis priemonių susijusių dokumentų keitimu, pavyzdžiui, sprendimo per sertifikavimo, sertifikato, o taip pat kitų būtinų veiksmų (pavyzdžiui, pakeisti viešai skelbiamą informaciją) atlikimą.*
7.12.	**Registrai**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.12 papunktyje, sertifikavimo įstaiga turi: 1. 3 metus nuo sertifikato galiojimo pabaigos ar nuo sprendimo neišduoti sertifikato priėmimo dienos saugoti visus susertifikavimu susijusius dokumentus ir įrašus, taip pat užtikrinti, kad dokumentai ir įrašai būtų išsamūs, suprantami, aktualūs ir tinkami auditui; 2. 3 metus nuo sertifikato galiojimo pabaigos saugoti visus įrašus, susijusius su pakeitimais, turinčiais įtakos sertifikavimui, ir veiksmais, kurių buvo imtasi, siekiant įgyvendinti šiuos pakeitimus.
7.13.	**Skundai ir kreipimaisi į teismą**	Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.13.1 papunktyje, sertifikavimo įstaiga turi nustatyti: 1. kas turi teisę teikti skundą sertifikavimo įstaigai; 2. kas sertifikavimo įstaigoje nagrinės skundus (turi būti užtikrinama, kad juo nebus atitikties vertinime ar šio vertinimo

		peržiūroje dalyvavęs asmuo); 3. kokie veiksmai bus atliekami nagrinėjant skundus; 4. konsultavimosi su suinteresuotomis šalimis galimybes; 5. kokiu būdu sertifikavimo veikla bus atskirta nuo veiklos, susijusios su skundų nagrinėjimu. Skundų nagrinėjimo tvarka turi būti paskelbta viešai. *Pastaba Nr. 1. Sertifikavimo įstaiga turi fiksuoti informaciją apie gautus skundus ir veiksmus, kurių buvo imtasi juos nagrinėjant. Inspekcijai paprašius, jai turi būti sudaryta galimybė bet kuriuo metu susipažinti su šiais įrašais.* Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.13.2 papunktyje, sertifikavimo įstaiga turi nustatyti: 1. kaip ir kam turi būti pateiktas patvirtinimas apie gautą skundą; 2. per kiek laiko patvirtinimas turi būti pateiktas; 3. kokie tolimesni veiksmai turi būti atliekami. Papildomai prie reikalavimų, nustatytų ISO 17065 standarto 7.13.7 ir 7.13.8 papunkčiuose, sertifikavimo įstaiga turi nustatyti pagrįstą laikotarpį (pavyzdžiui, 3 mėnesius) skundą pateikusio asmens informavimui apie skundo nagrinėjimo eigą ir rezultatus. *Pastaba Nr. 2. Skundą pateikusio asmens informavimo laikotarpis galėtų būti pratęstas, atsižvelgiant į tikrinamo subjekto dydį, tyrimo sudėtingumą ir kitas objektyvias aplinkybes.* Atitiktį šiam reikalavimui pagrindžiančių dokumentų pavyzdžiai: 1. skundų nagrinėjimo tvarka; 2. skundą nagrinėsiančio asmens nustatymo kriterijai ir tvarka (jei ši informacija nėra nustatyta skundų nagrinėjimo tvarkoje); 3. pranešimo apie skundo nagrinėjimo eigą ir (ar) rezultatus pavyzdys; 4. sertifikavimo įstaigos darbuotojų patvirtinimas dėl atitikties šio priedo 4.2 ir 5.2 papunkčiuose aprašytam nešališkumo reikalavimui.

8 SKYRIUS
REIKALAVIMAI VALDYMO SISTEMAI

Vadovaujantis ISO 17065 standarto 8 skyriumi, pagrindinis reikalavimas valdymo sistemai – užtikrinti, kad visų ankstesnių skyrių reikalavimų įgyvendinimas akredituotos sertifikavimo įstaigos sertifikavimo mechanizmo taikymo srityje būtų dokumentuojamas, vertinamas, kontroliuojamas ir jo stebėsena būtų vykdoma nepriklausomai.

Reikalavimai valdymo sistemai:

1. Valdymo sistema turi apimti skaidraus akreditavimo reikalavimų įgyvendinimo ir nuolatinio atitikties jiems vertinimo, atliekamo pačios sertifikavimo įstaigos, metodologiją;

2. Valdymo sistema turi apimti šio priedo 9.3.3 ir 9.3.4 papunkčiuose nustatytus reikalavimus;

3. Valdymo principai ir jų dokumentais pagrįstas įgyvendinimas turi būti skaidrūs. Akredituota sertifikavimo įstaiga turi, Inspekcijai vykdant asmens duomenų apsaugos auditą, vadovaujantis Reglamento (ES) 2016/679 58 straipsnio 1 dalies b punktu, ar atliekant išduotų sertifikatų peržiūrą, vadovaujantis Reglamento (ES) 2016/679 58 straipsnio 1 dalies c punktu ir laikantis Reglamento (ES) 2016/679 42 straipsnio 7 dalimi, Inspekcijos prašymu bet kuriuo metu suteikti bet kokią su valdymo principais ir jų įgyvendinimu susijusią informaciją;

4. Akredituota sertifikavimo įstaiga turi viešai skelbti informaciją apie jos išduotus sertifikatus (Reglamento (ES) 2016/679 konstatuojamosios dalies 100 punktas), laikantis šio priedo 4.6 ir 7.8 papunkčių reikalavimų.

Eil. Nr.	Reikalavimas	Reikalavimo paaiškiniamai ir atitikties šiam reikalavimui patvirtinimo dokumentai ar informacija
8.1.	**Bendrieji valdymo sistemos reikalavimai**	Taikomi ISO 17065 standarto 8.1 papunkčio reikalavimai.
8.2.	**Valdymo sistemos dokumentavimas**	Taikomi ISO 17065 standarto 8.2 papunkčio reikalavimai.
8.3.	**Dokumentų kontrolė**	Taikomi ISO 17065 standarto 8.3 papunkčio reikalavimai.
8.4.	**Registrų kontrolė**	Taikomi ISO 17065 standarto 8.4 papunkčio reikalavimai.
8.5.	**Valdymo peržiūra**	Taikomi ISO 17065 standarto 8.5 papunkčio reikalavimai.
8.6.	**Vidaus auditai**	Taikomi ISO 17065 standarto 8.6 papunkčio reikalavimai.
8.7.	**Taisomieji veiksmai**	Taikomi ISO 17065 standarto 8.7 papunkčio reikalavimai.
8.8.	**Prevenciniai veiksmai**	Taikomi ISO 17065 standarto 8.8 papunkčio reikalavimai.

9 SKYRIUS
KITI REIKALAVIMAI

Eil. Nr.	Reikalavimas	Reikalavimo paaišinimai ir atitikties šiam reikalavimui patvirtinimo dokumentai ar informacija
9.1.	**Vertinimo metodų atnaujinimas**	Sertifikavimo įstaiga turi nustatyti paraiškos vertinimo metodų (pagal šio priedo 7.4 papunktį ir ISO 17065 standarto 7.4 papunktį) atnaujinimo tvarką. Vertinimo metodai turi būti atnaujinami, atsižvelgiant į teisinės sistemos pokyčius, susijusią(-ias) riziką(-as), techninių ir organizacinių saugumo priemonių pažangą ir jų įgyvendinimo kaštus. Vertinimo metodų kontekste aukščiau nurodytos procedūros turi sudaryti sąlygas nustatyti, ar, siekiant užtikrinti asmens duomenų apsaugos principus ir asmens duomenų saugumui keliamus reikalavimus, reikalinga keisti nuorodas į teisės aktus, Susitarimo turinį, identifikuotus rizikos šaltinius (įskaitant techninių priemonių pažeidžiamumą), asmens duomenų tvarkymo operacijoms taikomas technines ar organizacines priemones (pavyzdžiui, į pažangesnes) ir kt. Reikalingi pakeitimai turi būti dokumentuoti, išsaugant ankstesnes dokumentų versijas.
9.2.	**Ekspertinių žinių išsaugojimas**	Sertifikavimo įstaiga turi nustatyti darbuotojų mokymo ir kvalifikacijos kėlimo tvarką, užtikrinant jų ekspertinių žinių

		atnaujinimą, atsižvelgiant į šio priedo 7.10 skiltyje ir ISO 17065 standarto 7.10 papunktyje nurodytus pokyčius ir šio priedo 6.1 skiltyje ir ISO 17065 standarto 6.1papunktyje nurodytus reikalavimus.
9.3.	**Pareigos ir kompetencija**	
9.3.1.	**Sertifikavimo įstaigos ir jos klientų ryšiai**	Sertifikavimo įstaiga turi nustatyti komunikacijos su sertifikuojamu ar sertifikuotu subjektu tvarką, kuri apimtų: 1. akredituotos sertifikavimo įstaigos užduočių ir atsakomybės dokumentus, siekiant: 1.1. nagrinėti gautus prašymus dėl informacijos pateikimo; 1.2. užtikrinti tarpusavio komunikaciją dėl skundų, susijusių su sertifikavimu. 2. Paraiškos dėl sertifikavimo teikimo ir jos nagrinėjimo tvarką, siekiant: 2.1. informuoti apie paraiškos vertinimo eigą ir rezultatus; 2.2. sudaryti sąlygas Inspekcijos vertinimui ir (ar) patikrinimui, siekiant gauti Inspekcijos nuomonę ar sprendimą.
9.3.2.	**Vertinimo veiklos dokumentavimas**	Sertifikavimo įstaiga turi dokumentuoti savo atliekamą sertifikavimo veiklą. Atnaujinus dokumentus, turi būti pažymima dokumento versija ir atnaujinimo data. Ankstesnės dokumentų versijos saugomos 3 metus nuo pakeitimų atlikimo. Sertifikavimo įstaiga turi nustatyti informacijos teikimo Inspekcijai tvarką, kuri apimtų: 1. šio priedo 7.6 skiltyje nustatytų reikalavimų laikymąsi, t. y. informavimą apie gautas paraiškas dėl sertifikavimo ir (ar) siekiamą priimti sprendimą sertifikuoti sertifikuojamą subjektą. Inspekcija, gavusi šią informaciją, patikrina sertifikuojamo subjekto Reglamento (ES) 2016/679 pažeidimų ir asmens duomenų saugumo pažeidimų istoriją; 2. informavimą apie sertifikato išdavimo ar panaikinimo priežastis (vadovaujantis Reglamento (ES) 2016/679 43 straipsnio 5 dalimi), laikantis šio priedo 7.1 skilties reikalavimų; 3. informavimą apie su sertifikavimo paslaugų teikimu susijusių dokumentų, kurie buvo pateikti atitikties akreditavimo reikalavimams vertinimo metu, pakeitimus ir šių pakeitimų priežastis. Sertifikavimo įstaiga turi bendradarbiauti su Inspekcija, teikti Inspekcijai jos prašomą informaciją, sudaryti sąlygas vykdyti patikrinimus ir (ar) auditus. Šis įsipareigojimas turi būti pagrįstas dokumentais.
9.3.3.	**Skundų nagrinėjimo administravimas**	Sertifikavimo įstaigos skundų ir apeliacijų nagrinėjimo tvarka turi būti parengta kaip neatsiejama valdymo sistemos dalis, įgyvendinanti ISO 17065 standarto 4.1.2.2 papunkčio c dalies, 4.1.2.2 papunkčio j dalies, 4.6 papunkčio d dalies ir 7.13 papunkčio

		reikalavimus. Inspekcijai turi būti pateikta informacija apie sertifikavimo įstaigos gautus pagrįstus skundus.
9.3.4.	**Panaikinimo valdymas**	Sertifikavimo įstaiga valdymo sistemoje turi nustatyti kokių veiksmų bus imtasi, jei Inspekcija sustabdys ar panaikins sertifikavimo įstaigos akreditaciją, pavyzdžiui, kaip bus informuojami sertifikavimo įstaigos klientai (sertifikuojami subjektai).

_____