



Skaidrojums par atsevišķu sertifikācijas institūcijas (struktūras) akreditācijas prasību piemērošanu

Priekšvārds

Šajā dokumentā Datu valsts inspekcija (turpmāk — Inspekcija) sniedz skaidrojumu par atsevišķu sertifikācijas institūcijas akreditācijas prasību, kuras tā izstrādājusi saskaņā ar Datu regulas¹ 43. panta 2. punktu, 43. panta 3. punktu, 58. panta 3. punkta e) un f) apakšpunktu, Fizisko personas datu apstrādes likumu un starptautiskā standarta LVS EN ISO/IEC 17065:2013 prasībām (Atbilstības novērtēšana — Prasības institūcijām, kas sertificē produktus, procesus un pakalpojumus (turpmāk — ISO/IEC 17065) (turpmāk – Prasības), piemērošanu.

Skaidrojums sagatavots nolūkā sniegt informāciju organizācijām, kuras sagatavo pieteikumu, par to, kā praktiski izpildīt Prasībās noteikto. Skaidrojumā iekļautas norādes, kādi dokumenti iekļaujami akreditācijas pieteikumā, kā tie izstrādājami un noformējami. Tāpat Prasību izpilde šajā dokumentā skaidrota, aprakstot atsevišķas pārbaudes procedūras, ko atbilstības pārbaudes nolūkā veic Inspekcija.

Šajā skaidrojumā ievērota ISO/IEC 17065 struktūra un numerācija. Skaidrojumā izmantotie termini atbilst Prasībās izmantotajiem un skaidrotajiem terminiem un saīsinājumiem.

¹Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (95/46. gada aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula)

4. VISPĀRĪGĀS AKREDITĀCIJAS PRASĪBAS

4.1 Juridiskie un līgumiskie jautājumi

4.1.1 Juridiskā atbildība

- a) Lai apliecinātu atbilstību 4.1.1.1. punktā noteiktajai prasībai, sertifikācijas institūcija sagatavo un iesniedz apliecinājumu, ka uz to neattiecas Inspekcijas uzsāktās pārbaudes un/vai izmeklēšanas, un sertifikācijas struktūra pēdējo četrus gadus laikā nav administratīvi sodīta par personas datu aizsardzības pārkāpumiem.

Akreditācijas procesu var ietekmēt Datu regulas pārkāpums un Inspekcijas pieņemts lēmums piemērot administratīvu sodu. Šajā gadījumā sertifikācijas struktūras akreditācija var tikt apturēta līdz brīdim, kad sertifikācijas struktūra pierāda, ka ir veikti vajadzīgie pasākumi, lai novērstu pārkāpumu.

- b) Lai apliecinātu atbilstību 4.1.1.2. punktā noteiktajai prasībai, sertifikācijas struktūra sagatavo un iesniedz Inspekcijai apliecinājumu, ka tiek ievērotas Inspekcijas izstrādātās papildu prasības un ka sertifikācijas saņemšanai pieteiktās procedūras un dokumenti tiek laikus atjaunināti

- c) Lai apliecinātu atbilstību 4.1.1.3. punkta prasībām, sertifikācijas institūcija Inspekcijai iesniedz apliecinājumu, ka tā, apstrādājot personas datus, ievēro Datu regulas un citu normatīvo aktu, kas regulē fizisku personu datu apstrādi, prasības, tostarp, piemēram, informējot par to, vai institūcija ir iecēlusi datu aizsardzības speciālistu; sertifikācijas institūcijas personas datu apstrādes noteikumus un/vai citus nepieciešamos dokumentus (paziņojumi par privātumu, apstrādes darbību pieraksti, norādījumi par personas datu aizsardzības pārkāpumu izmeklēšanu utt.) un apliecinājumu, ka tiek regulāri atjaunoti;

Inspekcija, izvērtējot sertifikācijas institūcijas sniegto informāciju un izmantojot Inspekcijas rīcībā esošo informāciju, LATAK sniegs atzinumu par:

- a) sertifikācijas struktūras reputāciju;*
- b) informāciju par Inspekcijas uzsāktajām pārbaudēm un/vai izmeklēšanu;*
- c) administratīvo sodu, ko piemēro sertifikācijas struktūrai, ja tāds ir;*
- d) pašas sertifikācijas institūcijas atbilstība personas datu aizsardzības prasībām.*

4.1.2 Sertifikācijas līgums

- a) Lai izpildītu 4.1.2.3. apakšpunktā noteikto prasību, sertifikācijas institūcija nedrīkst līgumos iekļaut nosacījumus, kas samazina Klienta vai sertifikācijas institūcijas atbildību, kas izriet no Datu regulas, kā arī līguma nosacījumi nedrīkst ietekmēt Inspekcijas pilnvaras un/vai uzdevumus saskaņā ar Datu regulas 42. panta 5. punktu un 55.–58. pantu. Attiecībā uz šo prasību sertifikācijas institūcijai papildu jāiesniedz tās apliecinājums, ka līgumi šādus nosacījumus neparedz.
- b) 4.1.2.13. noteiktā prasība nosaka, ka sertifikācijas līgumiem jāparedz Prasību 7.4. punktā noteikto metožu izmantošana Klienta sertifikācijas procesā.

4.2. Objektivitātes pārvaldība

- a) 4.2.1. punktā noteikto sertifikācijas institūcijas dibināšanas dokumentu kopijām jābūt personas, kas tiesīga pārstāvēt sertifikācijas institūciju (valdes), apliecinātām. Sertifikācijas institūcija var iesniegt apliecinātus dibināšanas dokumentu izrakstus, iesniedzot dokumentus tikai tādā apjomā, kādā tie apliecina Prasību 4.2. sadaļā noteikto kritēriju izpildi. Iesniedzot dokumentus, papildus pievienojams sertifikācijas institūcijas paskaidrojums, kuras dokumentu sadaļas/nosacījumi/punkti sertifikācijas institūcijas ieskatā apliecina atbilstību konkrētiem Prasību 4.2. sadaļas kritērijiem.

- b) 4.2.6. punktā paredzētie interešu konflikti var ietvert, bet ne tikai, piemēram:

sertifikācijas struktūra pieder pie vienas un tās pašas uzņēmumu grupas un to kādā veidā kontrolē Klients;

sertifikācijas iestādi vai tās personālu (ieskaitot vadību) nodarbina Klients vai tā pieder Klienta vadības struktūrām, tai ir Klienta īpašumtiesības (ir tā biedrs, kopuzņēmuma dalībnieks, īpašnieks, akcionārs u. c.);

sertifikācijas institūcija vai tās personāls (ieskaitot vadību) ir Klienta kreditors vai tam ir citas tiesības celt prasības pret Klientu;

sertifikācijas struktūras darbinieki, tostarp datu aizsardzības inspektors vai vadība, sniedz Klientam datu aizsardzības inspektora pakalpojumus;

sertifikācijas struktūra izmanto Klienta telpas nomas, aizdevuma vai citu iemeslu dēļ.

4.3. Saistības un finansējums

- a) Lai izpildītu 4.3.1. punkta prasības, sertifikācijas struktūrai jāiesniedz apliecinājums, ka tai ir finanšu resursi (piemēram, apdrošināšana, rezerves), kas atbilst tās darbības jomai un apjomam, lai segtu savas saistības.
- b) Sertifikācijas institūcijai jānodrošina civiltiesiskās apdrošināšanas spēkā esamība visā akreditācijas laikā. 4.3.2. punktā noteiktā civiltiesiskās apdrošināšanas līguma atbilstību Inspekcija izvērtē, vadoties no potenciālajiem zaudējumiem, kurus sertifikācijas institūcijas darbība var radīt trešajām personām, to iestāšanās varbūtības, un normatīvo aktu prasībām apdrošināt civiltiesisko atbildību citās darbības sfērās. Inspekcija tostarp ņem vērā Datu regulas 83. panta nosacījumus par administratīvo naudas sodu piemērošanu par Datu regulas pārkāpumiem.

4.6. Viegli publiski pieejama informācija

- a) 4.6.1. punktā un tā apakšpunktos noteikto prasību izpildei institūcija iesniedz procedūras, kurās aprakstīta kārtība, kā sertifikācijas struktūra nodrošina šajā sadaļā minētās **informācijas publicēšanu tās tīmekļvietnē**, savukārt 4.6.2. punktā un tā apakšpunktos noteikto prasību izpildei institūcija iesniedz procedūras, kurās aprakstīta kārtība, kā sertifikācijas struktūra nodrošina šajā sadaļā minētās **informācijas pieejamību (izsniegšanu) trešajām personām pēc pieprasījuma (t.i., šo informāciju sertifikācijas institūcijai nav pienākums publicēt tīmekļvietnē)**.
- b) 4.6.1.5. punktā noteiktajā klientu reģistrā norāda informāciju par klientu, kā arī attiecīgos sertificētos produktus, procesus un pakalpojumus, kā arī sertifikāta derīgumu, ietvaru un nosacījumus.
- c) Norādot 4.6.1.6.2. punktā noteikto informāciju, sniedz informāciju par izmantoto novērtēšanas kritēriju spēkā esību novērtējuma ziņojuma sagatavošanas brīdī.

6.1. Sertifikācijas struktūras personāls

- a) 6.1.1., 6.1.2. un 6.1.3. nodaļā noteikto prasību izpildi sertifikācijas institūcija pierāda ar, piemēram, sertifikātiem, atsauksmēm, apliecinājumiem, personāla amata aprakstiem, darba līgumiem, CV un citiem dokumentiem.
- b) 6.1. punkta sadaļā noteiktas vispārīgas prasības attiecībā uz personāla kvalifikāciju, kuru izpildei sertifikācijas institūcijai jāpierāda, ka tās rīcībā ir darbinieki, kuri var nodrošināt tajās noteiktās zināšanas un prasmes. 6.1.2. sadaļā izvirzītas prasības, kurām jāatbilst sertifikācijas institūcijas personālam ar tehniskajām zināšanām, un 6.1.3. sadaļā – prasības, kurām jāatbilst personālam ar juridiskajām

zināšanām. Sertifikācijas institūcijai jāievēro, ka nošķiramas prasības, kas izvirzītas personālam, kas faktiski veic klienta novērtējumu un personālam, kas pieņem lēmumu par klienta atbilstību.

- c) Par zināšanām saistībā ar sertifikācijas objektu atbilstoši 6.1.1.2. punktā noteiktajai prasībai var liecināt, piemēram, personāla darba pieredze ekspertu darbībās, kas saistītas ar produktu, pakalpojumu vai procesu, vadības sistēmu sertifikāciju, revīziju vai citiem līdzīgiem novērtējumiem.
- d) Lai procedūrās demonstrētu 6.1.1.3. punktā noteikto prasību izpildi, personāla neatkarības draudu un interešu konfliktu draudu novērtēšanu veic saskaņā ar standarta ISO 17065 4.2. punktu un Inspekcijas izstrādāto papildus prasību 4.2. punktu.
- e) 6.1.1.5. apakšpunktā aprakstīto zināšanu apliecināšanu var veikt, pamatojoties, piemēram, bet ne tikai, uz zināšanām par Eiropas Savienības Kiberdrošības aģentūras ieteikumiem, ISO standartiem ISO/IEC 27001:2022 *“Information security, cybersecurity and privacy protection — Information security management systems — Requirements”*, ISO/IEC 27002:2022 *“Information security, cybersecurity and privacy protection — Information security controls”* un ISO/IEC 27701:2019 *“Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines”*
- f) 6.1.2. punkta prasības attiecināmas uz sertifikācijas institūcijas darbiniekiem, kuru kvalifikācija un pieredze tehniskajā jomā tiks izmantota Klientu atbilstības novērtēšanā sertifikācijas procesā.
- g) Lai apliecinātu atbilstību 6.1.2.1. punktā ietvertajai prasībai par personāla profesionālo pieredzi tehnoloģiju jomā, sertifikācijas institūcija var iesniegt informāciju, piemēram, par pieredzi saistībā ar informācijas drošības sistēmām, drošības pārvaldības sistēmām, informācijas drošības riska pārvaldību utt.
- h) Ja sertifikācijas institūcija atbilstību Inspekcijas izstrādātajam papildus prasībām pierāda, iesaistot apakšuzņēmējus, jāņem vērā, ka sertifikācijas institūcija var paļauties uz citu personu prasmēm pierādīt profesionālo pieredzi vai šīm prasībām atbilstoša personāla pieejamību tikai tad, ja šīs personas sniegs pakalpojumus, kuru izpildei ir nepieciešamas attiecīgās spējas.

7.4. Novērtējums

- a) Atbilstoši 7.4.4.3. punktam, gadījumā, ja sertifikācijas institūcija piesaista apakšuzņēmējus, jānodrošina, ka arī apakšuzņēmēji, tāpat kā sertifikācijas institūcija, demonstrē labu reputāciju datu aizsardzībā, savā darbībā ievēro datu aizsardzību regulējošo normatīvo aktu prasības, un, pildot tiem sertifikācijas procesa ietvaros uzdotos uzdevumus, ievēro Inspekcijas izstrādātās papildu prasības sertifikācijas institūciju akreditācijai, ciktāl tās attiecināmas uz apakšuzņēmēju, tāpat apakšuzņēmēji nodrošina objektivitāti savā darbībā un efektīvu interešu konfliktu pārvaldību.
- b) Atbilstību 7.4.4.3. punktā norādītajai prasībai sertifikācijas institūcija apliecina, iesniedzot līgumu, kas noslēgts starp apakšuzņēmēju un sertifikācijas institūciju un kurš paredz minēto prasību ievērošanu tiktāl, ciktāl tas attiecināms uz apakšuzņēmējam nodoto uzdevumu izpildi sertifikācijas procesa veikšanai.
- c) 7.4.8. punktā noteiktajā procesa aprakstā tostarp norāda, ka novērtējuma ziņojumā sertifikācijas institūcija norādīs detalizētu informāciju par sertifikāciju, iekļaujot personas datu būtību, datu subjektu skaitu, datu apstrādes kontekstu, datu vākšanas tehnoloģiju un to plānotās apstrādes sarežģītību, kā arī klienta izmantotos apstrādātājus. Tāpat novērtējuma ziņojumā norāda pārbaudītos dokumentus un uzskaita novērtētos procesus, intervēto personu veiktās funkcijas, kā arī jebkādu neatbilstību sertifikācijas kritērijiem, skaidri norādot neatbilstību un neatbilstības nopietnību.

7.5. Sertifikātu pārskatīšana

Sertifikācijas procedūrās, tostarp procedūrās, kas saistītas ar sertifikāta periodisku pārskatīšanu un atsaukšanu, lēmuma iemeslus skaidri norāda un dokumentē ar pamatotiem faktiem un pierādījumiem.

7.6. Sertifikācijas lēmums

7.6.2. pantā aprakstītajā paziņojumā Inspekcijai iekļauj kopsavilkumu par pasākumiem, kas veikti, lai pieņemtu lēmumu, tostarp revīzijas ziņojuma kopiju, pārskatīšanas procesu un lēmuma pamatojumu.

7.9. Uzraudzība

- a) 7.9.3. punktā noteiktās neatbilstības procedūru aprakstos var klasificēt pēc to smaguma, piemēram — nelielas neatbilstības gadījumā termiņš var sasniegt vienu mēnesi, bet, ja neatbilstības netiek savlaicīgi novērstas, ir jāuzsāk sertifikācijas apturēšanas procedūra.
- b) 7.9.4. punktā noteiktā neatbilstības analīze veicama, lai īstenotu efektīvas korigējošas darbības un novērstu neatbilstības atkārtošanos un noteiktu, vai ir citas saistītas vai līdzīgas kļūdas, kas arī jālabo. Sertifikācijas institūcija paredz kārtību, kādā klientam tiek pieprasīts veikt pārbaudi, kā arī, kā sertifikācija veic šādas analīzes pārbaudi.

7.11. Sertifikācijas izbeigšana, samazināšana, apturēšana vai atsaukšana

Izstrādājot 7.11.3. punktā noteikto kārtību, sertifikācijas institūcija ņem vērā, ka saskaņā ar Datu regulas 58. panta 2. punkta h) apakšpunktu sertifikācijas struktūrai ir pienākums ņemt vērā Inspekcijas lēmumus un rīkojumus atsaukt vai neizsniegt sertifikātu pieteikuma iesniedzējam, gadījumā, ja sertifikācijas prasības nav izpildītas vai vairs netiek izpildītas.

7.13. Sūdzības un apelācijas

Attiecībā uz 7.13.1.2. punktā noteikto prasību, procedūrai būtu jādemonstrē, kā tiek nodrošināta sertifikācijas institūcijas (struktūras) personāla sadale starp sertifikācijas procesu izskatīšanu, iebildumu, sūdzību izskatīšanu. Sertifikācijas struktūra nodrošina, ka lēmumu attiecībā uz saņemtu sūdzību vai iebildumu izvērtē, pieņem un apstiprina personas, kuras nav iesaistītas sertifikācijas novērtēšanas procesā.

8. VADĪBAS SISTĒMAS PRASĪBAS

Procedūras un metodes, kas pieņemtas Datu regulā noteikto pienākumu ievērošanai, sertifikācijas institūcija dokumentē pārvaldības sistēmā, lai efektīvi sasniegtu tās mērķus, kā arī nodrošinātu pārredzamu revīziju, piemērošanu un atbilstību papildu prasībām.

9. PIENĀKUMI UN KOMPETENCE

9.1. Novērtēšanas metožu atjaunināšana

Novērtēšanas metodes jāatjaunina, ņemot vērā izmaiņas tiesiskajā regulējumā, riskos, tehnisko un organizatorisko drošības pasākumu jaunākajos sasniegumos.

Saistībā ar novērtēšanas metodēm, sertifikācijas izstrādātajām procedūrām ir jāļauj noteikt, vai atsauces uz tiesību aktiem, līgumu saturu, identificētie risku avoti (tostarp tehnisko līdzekļu ievainojamība), tehniskie vai organizatoriskie pasākumi, kas piemērojami personas datu apstrādei (piemēram, sarežģītākai apstrādei) utml., ir jāmaina, lai nodrošinātu personas datu aizsardzības principus un prasības attiecībā uz personas datu drošību.

9.4. Novērtēšanas darbību dokumentēšana

Pēc 9.4.2.1. punktā minētās informācijas saņemšanas Inspekcija pārbauda, vai tā pret klientu nav uzsākusi izmeklēšanu, Datu regulas pārkāpumu vēsturi un personas datu aizsardzības pārkāpumus, ko veicis sertificējamais klients.