Pamatnostādnes

Pamatnostādnes 4/2018 par sertifikācijas struktūru akreditāciju saskaņā ar Vispārīgās datu aizsardzības regulas (2016/679) 43. pantu

Versija 3.0

2019. gada 4. jūnijs

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Pieņemtas

Versiju vēsture

Versija 3.0	2019. gada 4. jūnijs	1. pielikuma iekļaušana (1. pielikuma versija 2.0 pieņemta 2019. gada 4. jūnijā pēc sabiedriskās apspriešanas)
Versija 2.0	2018. gada 4. decembris	Pamatnostādņu pieņemšana pēc sabiedriskās apspriešanas — tajā pašā datumā, kad 1. pielikums (versija 1.0) tika pieņemts sabiedriskai apspriešanai
Versija 1.0	2018. gada 6. februāris	29. panta darba grupa pieņem pamatnostādnes (sabiedriskai apspriešanai paredzētā versija) Šo versiju 2018. gada 25. maijā apstiprināja EDAK

Saturs

Eiropas Datu aizsardzības kolēģija,

ņemot vērā 70. panta 1. punkta e) apakšpunktu Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulā (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK,

ņemot vērā sabiedrisko apspriešanu par pamatnostādnēm, kas notika 2018. gada februārī, un par pielikumu, kas notika laika posmā no 2018. gada 14. decembra līdz 2019. gada 1. februārim, saskaņā ar VDAR 70. panta 4. punktu rezultātus,

IR PIEŅĒMUSI ŠĪS PAMATNOSTĀDNES.

1 IEVADS

1. Vispārīgā datu aizsardzības regula (Regula (ES) 2016/679) ("VDAR"), kas stājas spēkā 2018. gada 25. maijā, nodrošina modernizētu, uz pārskatatbildību un pamattiesībām balstītu atbilstības regulējumu datu aizsardzības jomā Eiropā. Šajā jaunajā regulējumā būtiskākie ir dažādu veidu pasākumi, kas veicina atbilstību VDAR noteikumiem. Tie ietver obligātas prasības konkrētos apstākļos (tostarp datu aizsardzības speciālistu iecelšanu un datu aizsardzības ietekmes novērtējumu veikšanu) un brīvprātīgus pasākumus, piemēram, rīcības kodeksus un sertifikācijas mehānismus.

2. Saistībā ar sertifikācijas mehānismu un datu aizsardzības zīmogu un marķējumu izstrādi VDAR 43. panta 1. punktā ir noteikts, ka dalībvalstīm ir jānodrošina, ka sertifikācijas struktūras, kuras izsniedz sertifikātus saskaņā ar 42. panta 1. punktu, ir akreditējusi vai nu kompetentā uzraudzības iestāde, vai valsts akreditācijas struktūra, vai abas. Ja akreditāciju ir veikusi valsts akreditācijas struktūra saskaņā ar ISO/IEC 17065/2012, jāpiemēro arī kompetentās uzraudzības iestādes paredzētās papildu prasības.

3. Jēgpilni sertifikācijas mehānismi var veicināt atbilstību VDAR un pārredzamību datu subjektiem un attiecībās starp uzņēmumiem (*B2B*), piemēram, starp pārziņiem un apstrādātājiem. Datu pārziņi un apstrādātāji izmantos neatkarīgas trešās personas veiktu atestāciju, lai uzskatāmi parādītu savu apstrādes darbību atbilstību[1].

4. Šajā sakarā Eiropas Datu aizsardzības kolēģija (EDAK) atzīst, ka ir vajadzīgas pamatnostādnes saistībā ar akreditāciju. Akreditācijas īpašā nozīme un nolūks ir saistīts ar to, ka tā tiek sniegts autoritatīvs apliecinājums par sertifikācijas struktūru kompetenci, kas ļauj veidot uzticību sertifikācijas mehānismam.

5. Pamatnostādņu mērķis ir sniegt norādījumus par to, kā interpretēt un īstenot VDAR 43. panta noteikumus. Jo īpaši to mērķis ir palīdzēt dalībvalstīm, uzraudzības iestādēm un valsts

[1] VDAR 100. apsvērumā ir noteikts, ka sertifikācijas mehānismu izstrāde var uzlabot pārredzamību un atbilstību regulai un ļaut datu subjektiem novērtēt attiecīgo produktu un pakalpojumu datu aizsardzības līmeni.

akreditācijas struktūrām izstrādāt konsekventu, saskaņotu bāzi tādu sertifikācijas struktūru akreditācijai, kas izsniedz sertifikātus saskaņā ar VDAR.

2 PAMATNOSTĀDŅU DARBĪBAS JOMA

6. Šajās pamatnostādnēs ir:

- noteikts akreditācijas mērķis VDAR kontekstā;
- izklāstīts, kādas ir pieejamās sertifikācijas struktūru akreditācijas iespējas saskaņā ar 43. panta 1. punktu, un noteiktas galvenās problēmas, kas jāapsver;
- sniegts regulējums akreditācijas papildu prasību noteikšanai, kad akreditāciju veic valsts akreditācijas struktūra; un
- sniegts regulējums akreditācijas prasību noteikšanai, kad akreditāciju veic uzraudzības iestāde.

7. Šīs pamatnostādnes nav procedūras rokasgrāmata sertifikācijas struktūru akreditācijai saskaņā ar VDAR. Ar tām netiek izstrādāts jauns tehniskais standarts sertifikācijas struktūru akreditācijai VDAR nolūkos.

8. Šīs pamatnostādnes ir paredzētas:

- dalībvalstīm, kurām ir jānodrošina, ka sertifikācijas struktūras ir akreditējusi uzraudzības iestāde un/vai valsts akreditācijas struktūra;
- valsts akreditācijas struktūrām, kas veic sertifikācijas struktūru akreditāciju saskaņā ar 43. panta 1. punkta b) apakšpunktu;
- kompetentajai uzraudzības iestādei, kas nosaka "papildu prasības" tām prasībām, kas paredzētas ISO/IEC 17065/2012[2], ja akreditāciju veic valsts akreditācijas struktūra saskaņā ar 43. panta 1. punkta b) apakšpunktu;
- EDAK, kad tā sniedz atzinumu un apstiprina kompetentās uzraudzības iestādes akreditācijas prasības saskaņā ar 43. panta 3. punktu, 70. panta 1. punkta p) apakšpunktu un 64. panta 1. punkta c) apakšpunktu;
- kompetentajai uzraudzības iestādei, kas nosaka akreditācijas prasības, ja akreditāciju veic uzraudzības iestāde saskaņā ar 43. panta 1. punkta a) apakšpunktu;
- citām ieinteresētajām personām, piemēram, potenciālajām sertifikācijas struktūrām vai sertifikācijas shēmu īpašniekiem, kas nodrošina sertifikācijas kritērijus un procedūras[3].

9. Definīcijas

[2] Starptautiskā Standartizācijas organizācija "Atbilstības novērtējums. Prasības struktūrām, kuras sertificē produktus, procesus un pakalpojumus".

[3] Shēmas īpašnieks ir identificējama organizācija, kas ir noteikusi sertifikācijas kritērijus un prasības, saskaņā ar kurām tiek novērtēta atbilstība. Tiek akreditēta organizācija, kas veic novērtējumus (43. panta 4. punkts) atbilstīgi sertifikācijas shēmas prasībām un izsniedz sertifikātus (t. i., sertifikācijas struktūra, zināma arī kā atbilstības novērtēšanas struktūra). Organizācija, kas veic novērtējumus, var būt tā pati organizācija, kura izstrādā un kurai pieder shēma, taču var būt situācijas, kad vienai organizācijai pieder shēma, bet kāda cita (vai vairākas) veic novērtējumus.

10. Turpmāk minētās definīcijas ir paredzētas, lai veicinātu kopēju izpratni par akreditācijas procesa pamatelementiem. Tās būtu jāuzskata par atsauces punktiem, un tās nenozīmē, ka kāds pieņēmums ir neapstrīdams. Šo definīciju pamatā ir pašreizējie tiesiskie regulējumi un standarti, jo īpaši attiecīgie VDAR un ISO/IEC 17065/2012 noteikumi.

11. Šajās pamatnostādnēs piemēro šādas definīcijas:

12. "akreditācija" — par sertifikācijas struktūru akreditāciju skatīt 3. sadaļu par akreditācijas interpretāciju VDAR 43. panta izpratnē;

13. "papildu prasības" ir prasības, kuras paredzējusi kompetentā uzraudzības iestāde un atbilstīgi kurām tiek veikta akreditācija[4];

14. "sertifikācija" ir novērtējums un objektīvs trešās personas apliecinājums[5] tam, ka ir pierādīta sertifikācijas kritēriju izpilde;

15. "sertifikācijas struktūra" ir trešās personas atbilstības novērtēšanas[6] struktūra[7], kas izmanto sertifikācijas mehānismus[8];

16. "sertifikācijas shēma" ir sertifikācijas sistēma, kas saistīta ar konkrētiem produktiem, procesiem un pakalpojumiem, uz kuriem attiecas tās pašas konkrētās prasības, īpašie noteikumi un procedūras[9];

17. "kritēriji" jeb sertifikācijas kritēriji ir kritēriji, atbilstīgi kuriem tiek veikta sertifikācija (atbilstības novērtēšana)[10];

18. "valsts akreditācijas struktūra" ir viena struktūra dalībvalstī, kas noteikta saskaņā ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 765/2008 un kas veic akreditāciju ar valsts piešķirtu atļauju[11].

3 TERMINA "AKREDITĀCIJA" INTERPRETĀCIJA VDAR 43. PANTA IZPRATNĒ

19. VDAR termins "akreditācija" nav definēts. Regulas (EK) Nr. 765/2008, ar ko nosaka akreditācijas vispārīgās prasības, 2. panta 10. punktā akreditācija ir definēta kā

20. "valsts akreditācijas struktūras atestācija, ka atbilstības novērtēšanas struktūra atbilst saskaņotajos standartos noteiktajām prasībām un attiecīgā gadījumā — jebkurām papildu

[4] 43. panta 1., 3. un 6. punkts.

[5] Jāņem vērā ka saskaņā ar ISO 17000 trešās personas apliecinājums (sertifikāts) ir "piemērojams visiem atbilstības novērtējuma subjektiem" (5.5. punkts), "izņemot pašas atbilstības novērtēšanas struktūras, uz kurām attiecas akreditācija" (5.6. punkts).

[6] Trešās personas atbilstības novērtēšanu veic organizācija, kas ir neatkarīga no personas vai organizācijas, kas nodrošina subjektu, un no šā subjekta lietotāju interesēm, sk. ISO 17000 2.4. punktu.

[7] Sk. ISO 17000 2.5. punktu: "struktūra, kas veic pakalpojumu atbilstības novērtēšanu"; ISO 17011: "struktūra, kas veic pakalpojumu atbilstības novērtēšanu un kas var būt akreditācijas subjekts"; ISO 17065 3.12. punkts.

[8] VDAR 42. panta 1. un 5. punkts.

[9] Sk. ISO 17065 3.9. punktu apvienojumā ar B pielikumu.

[10] Sk. 42. panta 5. punktu.

[11] Sk. Regulas Nr. 765/2008/EK 2. panta 11. punktu.

prasībām, tostarp atbilstīgajās nozaru sistēmās izklāstītajām, lai veiktu īpašas atbilstības novērtēšanas darbības".

21. Saskaņā ar ISO/IEC 17011

22. "akreditācija attiecas uz trešās personas apliecinājumu attiecībā uz atbilstības novērtēšanas struktūru, kas oficiāli apliecina tās kompetenci veikt konkrētus atbilstības novērtēšanas uzdevumus."

23. 43. panta 1. punktā ir noteikts:

24. "neskarot kompetentās uzraudzības iestādes uzdevumus un pilnvaras saskaņā ar 57. un 58. pantu, sertifikātu izdod un atjauno sertifikācijas struktūras, kam ir atbilstīgas specializētās zināšanas datu aizsardzības jomā, pēc tam, kad tās ir informējušas uzraudzības iestādi, lai tā vajadzības gadījumā varētu īstenot savas pilnvaras saskaņā ar 58. panta 2. punkta h) apakšpunktu. Dalībvalstis nodrošina, ka minētās sertifikācijas struktūras akreditē viena vai abas no turpmāk minētajām:

    (a) uzraudzības iestāde, kas ir kompetenta, ievērojot 55. vai 56. pantu;
    (b) valsts akreditācijas struktūra, kas norādīta saskaņā ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 765/2008 atbilstīgi ISO/IEC 17065/2012 un papildu prasībām, ko paredzējusi uzraudzības iestāde, kura ir kompetenta, ievērojot 55. vai 56. pantu".

25. Attiecībā uz VDAR akreditācijas prasības reglamentēs:

- ISO/IEC 17065/2012 un "papildu prasības", ko noteikusi uzraudzības iestāde, kas ir kompetenta saskaņā ar 43. panta 1. punkta b) apakšpunktu, kad akreditāciju veic valsts akreditācijas struktūra, un uzraudzības iestāde, kad tā pati veic akreditāciju.

26. Abos gadījumos konsolidētajās prasībās ir jāiekļauj 43. panta 2. punktā minētās prasības.

27. EDAK atzīst, ka akreditācijas mērķis ir dot autoritatīvu apliecinājumu par struktūras kompetenci veikt sertifikāciju (atbilstības novērtēšanas darbības)[12]. Saskaņā VDAR ar akreditāciju saprot:

28. valsts akreditācijas struktūras un/vai uzraudzības iestādes apliecinājumu[13], ka sertifikācijas struktūra[14] ir kvalificēta veikt sertifikāciju saskaņā ar VDAR 42. un 43. pantu, ņemot vērā ISO/IEC 17065/2012 un papildu prasības, ko paredzējusi uzraudzības iestāde un/vai kolēģija.

4 AKREDITĀCIJA SASKAŅĀ AR VDAR 43. PANTA 1. PUNKTU

29. 43. panta 1. punktā ir atzīts, ka pastāv vairākas sertifikācijas struktūru akreditācijas iespējas. VDAR ir noteikts, ka uzraudzības iestādēm un dalībvalstīm ir jādefinē sertifikācijas struktūru akreditācijas process. Šajā sadaļā ir izklāstīti 43. pantā noteiktie akreditācijas veidi.

4.1 Dalībvalstu uzdevums

[12] Sk. Regulas Nr. 765/2008/EK 15. apsvērumu.
[13] Sk. 2. panta 10. punktu Eiropas Parlamenta un Padomes Regulā (EK) Nr. 765/2008 (2008. gada 9. jūlijs), ar ko nosaka akreditācijas un tirgus uzraudzības prasības attiecībā uz produktu tirdzniecību.
[14] Sk. termina "akreditācija" definīciju ISO 17011.

30. 43. panta 1. punktā ir noteikts, ka dalībvalstīm *ir jānodrošina*, ka sertifikācijas iestādes ir akreditētas, taču katrai dalībvalstij ir atļauts noteikt, kuram būtu jāatbild par tāda novērtējuma veikšanu, kas ir akreditācijas pamatā. Pamatojoties uz 43. panta 1. punktu, ir pieejamas trīs iespējas; akreditāciju veic:

(1) tikai uzraudzības iestāde, pamatojoties uz savām prasībām;
(2) tikai valsts akreditācijas struktūra, kas noteikta saskaņā ar Regulu (EK) Nr. 765/2008, pamatojoties uz ISO/IEC 17065/2012, un atbilstīgi kompetentās uzraudzības iestādes noteiktajām papildu prasībām; vai
(3) gan uzraudzības iestāde, gan valsts akreditācijas struktūra (un saskaņā ar visām 2. punktā minētajām prasībām).

31. Katra dalībvalsts var pieņemt lēmumu par to, vai akreditācijas darbības veiks valsts akreditācijas struktūra vai uzraudzības iestāde, vai abas kopā, taču jebkurā gadījumā tai būtu jānodrošina, ka tiek piešķirti pietiekami līdzekļi[15].

4.2 Mijiedarbība ar Regulu (EK) Nr. 765/2008

32. EDAK norāda, ka Regulas (EK) Nr. 765/2008 2. panta 11. punktā valsts akreditācijas struktūra ir definēta kā "*vienīgā* struktūra dalībvalstī, kura veic akreditāciju, pamatojoties uz minētās valsts piešķirtajām pilnvarām".

33. 2. panta 11. punktu varētu uzskatīt par nesaderīgu ar VDAR 43. panta 1. punktu, kas ļauj veikt akreditāciju struktūrai, kura nav dalībvalsts valsts akreditācijas struktūra. EDAK uzskata, ka ES tiesību akta nolūks ir atkāpties no vispārīgā principa, ka akreditāciju veic vienīgi valsts akreditācijas iestāde, piešķirot uzraudzības iestādēm tādas pašas pilnvaras kā saistībā ar sertifikācijas struktūru akreditāciju. Tādējādi 43. panta 1. punkts ir *lex specialis* attiecībā pret Regulas Nr. 765/2008 2. panta 11. punktu.

4.3 Valsts akreditācijas struktūras uzdevums

34. 43. panta 1. punkta b) apakšpunktā ir noteikts, ka valsts akreditācijas struktūra akreditēs sertifikācijas struktūras saskaņā ar ISO/IEC 17065/2012 un kompetentās uzraudzības iestādes paredzētajām papildu prasībām.

35. Skaidrības labad EDAK norāda, ka īpašā norāde uz 43. panta 3. punkta 1. daļas b) apakšpunktu nozīmē to, ka "minētās prasības" norāda uz "papildu prasībām", kuras ir paredzējusi kompetentā uzraudzības iestāde 43. panta 1. punkta b) apakšpunktā, un 43. panta 2. punktā noteiktajām prasībām.

36. Akreditācijas procesā valsts akreditācijas struktūras piemēro papildu prasības, kuras nosaka uzraudzības iestādes.

37. Sertifikācijas struktūrai, kas akreditēta, pamatojoties uz ISO/IEC 17065/2012, attiecībā uz sertifikācijas shēmām, kuras nav saistītas ar VDAR, un kas vēlas paplašināt savas akreditācijas darbības jomu, iekļaujot sertifikātus, kas izsniegti saskaņā ar VDAR, būs jāizpilda uzraudzības iestādes paredzētās papildu prasības, ja akreditāciju veic valsts akreditācijas struktūra. Ja sertifikācijas akreditāciju saskaņā ar VDAR piedāvā tikai kompetentā uzraudzības iestāde, sertifikācijas struktūrai, kura piesakās akreditācijai, būs jāizpilda attiecīgās uzraudzības iestādes noteiktās prasības.

[15] Sk. Regulas (EK) Nr. 765/2008 4. panta 9. punktu.

4.4 Uzraudzības iestādes uzdevums

38. EDAK norāda, ka 57. panta 1. panta q) apakšpunktā ir noteikts, ka uzraudzības iestāde *veic* sertifikācijas struktūras akreditāciju saskaņā ar 43. pantu kā "uzraudzības iestādes uzdevumu" saskaņā ar 57. pantu, un 58. panta 3. punkta e) apakšpunktā ir noteikts, ka uzraudzības iestādei ir atļauju izsniegšanas un padomdevēja pilnvaras akreditēt sertifikācijas struktūras saskaņā ar 43. pantu. 43. panta 1. punkta formulējums nodrošina noteiktu elastību, un uzraudzības iestādes akreditācijas funkcija būtu uzskatāma par uzdevumu tikai attiecīgā gadījumā. Lai precizētu šo punktu, var izmantot dalībvalsts tiesību aktus. Tomēr, ja akreditāciju veic valsts akreditācijas struktūra, saskaņā ar 43. panta 2. punkta a) apakšpunktu kompetentajai uzraudzības iestādei ir uzskatāmi jāparāda, ka tā darbojas neatkarīgi un pārzina tās piedāvātā sertifikācijas mehānisma tematiku[16].

39. Ja dalībvalsts nosaka, ka sertifikācijas struktūras ir jāakreditē uzraudzības iestādei, uzraudzības iestādei būtu jāparedz akreditācijas prasības, tostarp, bet ne tikai, prasības, kas sīki izklāstītas 43. panta 2. punktā. Salīdzinājumā ar pienākumiem saistībā ar valsts akreditācijas struktūru veiktu sertifikācijas struktūru akreditāciju 43. pantā ir sniegts mazāk norādījumu par prasībām attiecībā uz tādu akreditāciju, ko veic pati uzraudzības iestāde. Nolūkā veicināt saskaņotu pieeju akreditācijai uzraudzības iestādes izmantoto akreditācijas kritēriju pamatā vajadzētu būt ISO/IEC 17065, un tiem vajadzētu būt papildinātiem ar papildu prasībām, ko paredzējusi uzraudzības iestāde saskaņā ar 43. panta 1. punkta b) apakšpunktu. EDAK norāda, ka 43. panta 2. punkta a)–e) apakšpunkts ataino un precizē ISO 17065 prasības, kas uzlabos saskaņotību.

40. Ja dalībvalsts nosaka, ka sertifikācijas struktūras ir jāakreditē valsts akreditācijas struktūrām, uzraudzības iestādei būtu jāparedz papildu prasības, kas papildinātu pašlaik Regulā (EK) Nr. 765/2008 (kur 3.–14. pants attiecas uz atbilstības novērtēšanas struktūru akreditācijas organizāciju un darbību) paredzētās akreditācijas konvencijas, un tehniskos noteikumus, kuros būtu izklāstītas sertifikācijas struktūru metodes un procedūras. Šajā saistībā Regulā (EK) Nr. 765/2008 ir sniegti papildu norādījumi: 2. panta 10. punktā ir definēta akreditācija un sniegta atsauce uz "saskaņotiem standartiem" un "jebkurām papildu prasībām, tostarp atbilstīgajās nozaru sistēmās izklāstītajām". Tāpēc uzraudzības iestādes paredzētajās papildu prasībās būtu jāiekļauj konkrētas prasības un lielākā uzmanība jāpievērš novērtēšanas veicināšanai, cita starpā sertifikācijas struktūru neatkarības un zināšanu par datu aizsardzību līmeni novērtēšanas veicināšanai, piemēram, to spējām novērtēt un sertificēt pārziņu un apstrādātāju veiktās personas datu apstrādes darbības saskaņā ar 42. panta 1. punktu. Tas ietver kompetenci, kas vajadzīga nozares shēmām un saistībā ar fizisku personu pamattiesību un brīvību aizsardzību, jo īpaši attiecībā uz to tiesībām uz personas datu apstrādi[17]. Šo pamatnostādņu pielikums var palīdzēt informēt kompetentās uzraudzības iestādes par to, kad paredzēt "papildu prasības" saskaņā ar 43. panta 1. punkta b) apakšpunktu un 43. panta 3. punktu.

41. 43. panta 6. punktā ir paredzēts, ka "uzraudzības iestāde viegli pieejamā veidā publisko šā panta 3. punktā minētās prasības un 42. panta 5. punktā minētos kritērijus". Tāpēc, lai nodrošinātu pārredzamību, tiek publicēti visi uzraudzības iestādes apstiprinātie kritēriji un

[16] Papildu prasībās, ko uzraudzības iestāde nosaka saskaņā ar 43.panta 1. punkta b) apakšpunktu, būtu jāprecizē prasības attiecībā uz neatkarību un zināšanām. Sk. arī pamatnostādņu 1. pielikumu.
[17] VDAR 1. panta 2. punkts.

prasības. Sertifikācijas struktūru kvalitātes un uzticamības ziņā būtu vēlams, lai sabiedrībai būtu pieejamas visas akreditācijas prasības.

4.5 Uzraudzības iestāde, kas rīkojas kā sertifikācijas struktūra

42. 42. panta 5. punktā ir paredzēts, ka uzraudzības iestāde var izdot sertifikātus, taču VDAR nenosaka, ka tai ir jābūt akreditētai, lai izpildītu Regulas (EK) Nr. 765/2008 prasības. EDAK norāda, ka 43. panta 1. punktā un jo īpaši 58. panta 2. punkta h) apakšpunktā, 58. panta 3. punkta a), e) un f) apakšpunktā uzraudzības iestādēm ir paredzētas pilnvaras veikt akreditāciju un sertifikāciju un vienlaikus sniegt konsultācijas, kā arī attiecīgā gadījumā atsaukt sertifikātus un izdot rīkojumu sertifikācijas struktūrām neizsniegt sertifikātus.

43. Var būt situācijas, kad ir atbilstoši vai nepieciešams nodalīt akreditācijas un sertifikācijas uzdevumus un pienākumus, piemēram, ja dalībvalstī vienlaikus pastāv uzraudzības iestāde un citas sertifikācijas struktūras un tās izsniedz vienādus sertifikātus. Tāpēc uzraudzības iestādēm būtu jāveic pietiekami organizatoriski pasākumi, lai nodalītu VDAR paredzētos uzdevumus nolūkā nostiprināt un veicināt sertifikācijas mehānismus, vienlaikus veicot piesardzības pasākumus, lai izvairītos no interešu konfliktiem, kurus varētu izraisīt šie uzdevumi. Turklāt dalībvalstīm un uzraudzības iestādēm, formulējot valsts tiesību aktus un procedūras saskaņā ar VDAR, būtu jāpatur prātā saskaņotais Eiropas līmenis.

4.6 Akreditācijas prasības

44. Šo pamatnostādņu pielikumā ir sniegti norādījumi par to, kā noteikt akreditācijas papildu prasības. Tajā ir norādīti būtiskie VDAR noteikumi un ieteiktas prasības, kuras uzraudzības iestādēm un valsts akreditācijas struktūrām būtu jāapsver, lai nodrošinātu atbilstību VDAR.

45. Kā noteikts iepriekš, ja sertifikācijas struktūras akreditē valsts akreditācijas struktūra saskaņā ar Regulu (EK) Nr. 765/2008, ISO/IEC 17065/2012 būs atbilstošais akreditācijas standarts, ko papildinās uzraudzības iestādes paredzētas papildu prasības. 43. panta 2. punktā ir atainoti ISO/IEC 17065/2012 vispārēji noteikumi, ņemot vērā VDAR paredzētās pamattiesības. Pielikumā izklāstītajā regulējumā 43. panta 2. punkts un ISO/IEC 17065/2012 ir izmantoti kā pamats, lai noteiktu prasības un papildu kritērijus saistībā ar novērtējumu par sertifikācijas struktūru zināšanām par datu aizsardzību un to spēju ievērot fizisko personu tiesības un brīvības saistībā ar personas datu apstrādi, kā paredzēts VDAR. EDAK norāda, ka pielikumā īpaša uzmanība ir pievērstam tam, lai nodrošinātu, ka sertifikācijas struktūrām ir atbilstošas zināšanas par datu aizsardzību saskaņā ar 43. panta 1. punktu.

46. Uzraudzības iestādes paredzētās akreditācijas papildu prasības attieksies uz visām sertifikācijas struktūrām, kas pieprasa akreditāciju. Akreditācijas struktūra novērtēs, vai sertifikācijas struktūra ir kompetenta veikt sertifikāciju atbilstīgi papildu prasībām un sertifikācijas tematikai. Tiek norādītas atsauces uz konkrētām sertifikācijas nozarēm vai jomām, kurās sertifikācijas struktūra tiek akreditēta.

47. EDAK norāda arī to, ka papildus ISO/IEC 17065/2012 prasībām ir vajadzīgas arī īpašas zināšanas par datu aizsardzības jomu, ja daļu sertifikācijas darbību vai tās komponentus akreditētas sertifikācijas struktūras vārdā īsteno tādas ārējas struktūras kā laboratorijas vai revidenti. Šādos gadījumos nav iespējams akreditēt šīs ārējās struktūras saskaņā ar VDAR. Tomēr, lai nodrošinātu šo struktūru piemērotību darbībai akreditētu sertifikācijas struktūru vārdā, akreditētajai sertifikācijas struktūrai ir jānodrošina, ka akreditētajai struktūrai ir zināšanas par datu aizsardzību un tās ir uzskatāmi parādītas ārējai struktūrai saistībā ar attiecīgo veikto darbību.

48. Šo pamatnostādņu pielikumā izklāstīto akreditācijas papildu prasību noteikšanas regulējums nav valsts akreditācijas struktūras vai uzraudzības iestādes īstenota akreditācijas procesa procedūras rokasgrāmata. Tajā ir sniegti norādījumi un metodika, un tādējādi instrumentu kopums uzraudzības iestādēm akreditācijas papildu prasību noteikšanai.

1. PIELIKUMS

1. pielikumā sniegti norādījumi par "papildu" akreditācijas prasību specifikāciju attiecībā uz ISO/IEC 17065/2012 un saskaņā ar VDAR 43. panta 1. punkta b) apakšpunktu un 43. panta 3. punktu.

Šajā pielikumā izklāstītas ierosinātās prasības, kuras datu aizsardzības uzraudzības iestāde izstrādā un piemēro sertifikācijas struktūras akreditācijā, ko veic valsts akreditācijas struktūra vai kompetentā uzraudzības iestāde[18]. Par šīm papildu prasībām Eiropas Datu aizsardzības kolēģija ir jāinformē pirms apstiprināšanas saskaņā ar 64. panta 1. punkta c) apakšpunktu.

Šis pielikums lasāms kopā ar ISO/IEC 17065/2012. Šeit lietotie sadaļu numuri atbilst ISO/IEC 17065/2012. Ja uzraudzības iestādes veic akreditāciju atbilstīgi 43. panta 1. punkta a) apakšpunktam, visos gadījumos, kad tas ir lietderīgi, ir jāievēro šī pieeja. Tādējādi tiks veicināta ES mērogā saskaņota akreditācija.

Neskarot turpmāk minētos norādījumus vai norādījumu trūkumu attiecībā uz kādu no ISO/IEC 17065/2012 posteņiem, kompetentā uzraudzības iestāde var formulēt papildu prasības attiecībā uz šiem posteņiem, ja tas atbilst valsts tiesību aktiem.

0 PREFIKSS

[Šī sadaļa skar visus saskaņotos sadarbības noteikumus, ja tādi ir, starp valsts akreditācijas struktūru un datu aizsardzības uzraudzības iestādi, piemēram, kam būtu jāatbild par pieteikumu saņemšanu vai kā organizēt apstiprināto kritēriju atzīšanu akreditācijas procesā.]

1 DARBĪBAS JOMA[19]

ISO/IEC 17065/2012 darbības jomu piemēro saskaņā ar VDAR. Akreditācijas un sertifikācijas pamatnostādnēs ir sniegta sīkāka informācija. Sertifikācijas mehānisma darbības joma (piemēram, mākoņpakalpojumu apstrādes darbību sertifikācija) būtu jāņem vērā, novērtējot VAS un kompetento uzraudzības iestādi akreditācijas procesā, jo īpaši attiecībā uz kritērijiem, kompetenci un izvērtēšanas metodiku. Plašajai ISO/IEC 17065/2012 darbības jomai, kas attiecas uz produktiem, procesiem un pakalpojumiem, nevajadzētu pazemināt vai ignorēt VDAR prasības, piemēram, pārvaldības mehānisms nevar būt vienīgais sertifikācijas mehānisma elements, jo sertifikācijai jāietver personas datu apstrāde, t. i., apstrādes darbības. Saskaņā ar 42. panta 1. punktu VDAR sertifikāciju piemēro tikai pārziņu un apstrādātāju veiktajām apstrādes darbībām.

2 NORMATĪVĀS ATSAUCES

VDAR ir priekšroka salīdzinājumā ar ISO/IEC 17065/2012. Ja papildu prasībās vai sertifikācijas mehānismā ir atsauce uz citiem ISO standartiem, tos interpretē saskaņā ar VDAR noteiktajām prasībām.

[18] Informāciju par sertifikācijas kritēriju apstiprināšanas procesu skatīt sertifikācijas pamatnostādņu 4. sadaļā.
[19] Numerācija atbilst ISO/IEC 17065/2012.

3 TERMINI UN DEFINĪCIJAS

Saistībā ar šo pielikumu piemēro akreditācijas (*WP 261*) un sertifikācijas (*EDPB 1/2018*) pamatnostādņu nosacījumus un definīcijas, un tiem ir priekšroka salīdzinājumā ar ISO sniegtajām definīcijām.

4 VISPĀRĪGAS PRASĪBAS AKREDITĀCIJAI

4.1 Juridiskie un līgumiskie jautājumi

4.1.1 Juridiskā atbildība

Sertifikācijas struktūrai būtu jāspēj (jebkurā laikā) pierādīt VAS vai KUI, ka tā piemēro aktualizētas procedūras, kas atbilst akreditācijas noteikumos, tostarp papildu prasībās attiecībā uz Regulas 2016/679/EK piemērošanu, noteiktajiem juridiskajiem pienākumiem. Jāatzīmē, ka, tā kā sertifikācijas struktūra pati ir datu pārzinis/apstrādātājs, tai jāspēj pierādīt, ka tās izmantotās procedūras un pasākumi atbilst Regulas 2016/679/EK prasībām, kas īpaši attiecas uz klienta organizācijas personas datu kontroli un apstrādi sertifikācijas procesā.

KUI var nolemt pievienot papildu prasības un procedūras sertifikācijas struktūru pārbaudei pirms akreditācijas.

4.1.2 Sertifikācijas līgums (*CA*)

Sertifikācijas līguma minimālās prasības papildina ar šādiem punktiem:

Sertifikācijas struktūra papildus ISO/IEC 17065/2012 prasībām pierāda, ka tās sertifikācijas līgumos:

1. pieprasīts, lai pieteikuma iesniedzējs vienmēr ievēro gan vispārējās sertifikācijas prasības ISO/IEC 17065/2012 4.1.2.2. punkta a) apakšpunkta izpratnē, gan kritērijus, ko apstiprinājusi kompetentā uzraudzības iestāde vai EDAK, saskaņā ar 43. panta 2. punkta b) apakšpunktu un 42. panta 5. punktu;
2. pieprasīts, lai pieteikuma iesniedzējs nodrošina pilnīgu pārredzamību kompetentajai uzraudzības iestādei attiecībā uz sertifikācijas procedūru, tostarp attiecībā uz līgumiski konfidenciāliem jautājumiem, kas saistīti ar datu aizsardzības atbilstību, saskaņā ar 42. panta 7. punktu un 58. panta 1. punkta c) apakšpunktu;
3. nav samazināts pieteikuma iesniedzēja atbildības apmērs par atbilstības Regulai 2016/679/EK nodrošināšanu un nav skarti to uzraudzības iestāžu uzdevumi un pilnvaras, kuras ir kompetentas saskaņā ar 42. panta 5. punktu;
4. pieprasīts, lai pieteikuma iesniedzējs sniedz sertifikācijas struktūrai visu informāciju un piekļuvi tā apstrādes darbībām, kas nepieciešamas sertifikācijas procedūras veikšanai saskaņā ar 42. panta 6. punktu;
5. pieprasīts pieteikuma iesniedzējam ievērot piemērojamos termiņus un procedūras. Sertifikācijas līgumā jāparedz, ka jāievēro un jāizpilda termiņi un procedūras, kas izriet, piemēram, no sertifikācijas programmas vai citiem noteikumiem;
6. attiecībā pret ISO/IEC 17065/2012 4.1.2.2. punkta c) apakšpunkta 1. noteikumu izklāstīti spēkā esības, atjaunošanas un atsaukšanas noteikumi atbilstīgi 42. panta 7. punktam un 43. panta 4. punktam, tostarp noteikumi, kas nosaka atbilstošus intervālus atkārtotai izvērtēšanai vai pārskatīšanai (regularitāte) saskaņā ar 42. panta 7. punktu;
7. atļauts sertifikācijas struktūrai atklāt jebkādu informāciju, kas nepieciešama sertifikācijas piešķiršanai saskaņā ar 42. panta 8. punktu un 43. panta 5. punktu;

8. iekļauti noteikumi par nepieciešamajiem piesardzības pasākumiem sūdzību izmeklēšanai 4.1.2.2. punkta c) apakšpunkta 2. noteikuma, papildus j) apakšpunkta, izpratnē ietver arī skaidru paziņojumu par sūdzību pārvaldības struktūru un procedūru saskaņā ar 43. panta 2. punkta d) apakšpunktu;
9. papildus minimālajām prasībām, kas norādītas ISO/IEC 17065/2012 4.1.2.2. punktā, ja sertifikācijas struktūras akreditācijas atsaukšanas vai apturēšanas sekas ietekmē klientu, šādā gadījumā ir jāaplūko arī sekas klientam
10. pieprasīts, lai pieteikuma iesniedzējs informē sertifikācijas struktūru, ja ir notikušas būtiskas izmaiņas tā faktiskajā vai juridiskajā stāvoklī, kā arī tā produktos, procesos un pakalpojumos, uz kuriem attiecas sertifikācija.

4.1.3 Datu aizsardzības zīmogu un marķējumu izmantošana

Sertifikātus, zīmogus un marķējumus izmanto tikai saskaņā ar 42. un 43. pantu un akreditācijas un sertifikācijas pamatnostādnēm.

4.2 Objektivitātes pārvaldība

Akreditācijas struktūra nodrošina, ka papildus ISO/IEC 17065:2012 4.2. punktā ietvertajām prasībām

1. sertifikācijas struktūra nodrošina atbilstību kompetentās uzraudzības iestādes papildu prasībām (atbilstīgi 43. panta 1. punkta b) apakšpunktam)
    - **a.** saskaņā ar 43. panta 2. punkta a) apakšpunktu sniedz atsevišķus savas neatkarības pierādījumus. Tas jo īpaši attiecas uz pierādījumiem, kas skar sertifikācijas struktūras finansējumu, ciktāl tas skar tās objektivitātes apliecinājumu;
    - **b.** tās uzdevumi un pienākumi nerada interešu konfliktu atbilstīgi 43. panta 2. punkta e) apakšpunktam;
2. sertifikācijas struktūrai nav būtiskas saistības ar klientu, kuru tā novērtē.

4.3 Saistības un finansējums

Akreditācijas struktūra papildus ISO/IEC 17065/2012 4.3.1. punktā noteiktajai prasībai regulāri nodrošina, ka sertifikācijas struktūrai ir piemēroti pasākumi (piemēram, apdrošināšana vai rezerves), lai segtu savas saistības ģeogrāfiskajos reģionos, kuros tas darbojas.

4.4 Nediskriminējoši nosacījumi

Uzraudzības iestāde var noformulēt papildu prasības, ja tās ir saskaņā ar valsts tiesību aktiem.

4.5 Konfidencialitāte

Uzraudzības iestāde var noformulēt papildu prasības, ja tās ir saskaņā ar valsts tiesību aktiem.

4.6 Publiski pieejama informācija

Akreditācijas struktūra papildus ISO/IEC 17065/2012 4.6. punktā ietvertajai prasībai pieprasa sertifikācijas struktūrai, lai vismaz

1. visas apstiprināto kritēriju versijas (spēkā esošās un iepriekšējās), kas izmantotas 42. panta 5. punkta izpratnē, būtu publicētas un viegli publiski pieejamas, tāpat arī visas sertifikācijas procedūras, parasti norādot attiecīgo derīguma termiņu;
2. informācija par sūdzību izskatīšanas procedūrām un pārsūdzībām būtu publiskota saskaņā ar 43. panta 2. punkta d) apakšpunktu.

5 STRUKTURĀLĀS PRASĪBAS, 43. PANTA 4. PUNKTS [“PIENĀCĪGI VEIKTS” NOVĒRTĒJUMS]

5.1 Organizatoriskā struktūra un augstākā līmeņa vadība

Uzraudzības iestāde var noformulēt papildu prasības.

5.2 Objektivitātes aizsargāšanas mehānismi

Uzraudzības iestāde var noformulēt papildu prasības.

6 PRASĪBAS ATTIECĪBĀ UZ RESURSIEM

6.1 Sertifikācijas struktūras darbinieki

Akreditācijas struktūra papildus ISO/IEC 17065/2012 6. sadaļā ietvertajai prasībai pārliecinās katrā sertifikācijas struktūrā, ka tās darbiniekiem:

1. ir pierādāma atbilstoša un pastāvīga kompetence (zināšanas un pieredze) attiecībā uz datu aizsardzību saskaņā ar 43. panta 1. punktu;
2. ir neatkarīga un pastāvīga pieredze attiecībā uz sertifikācijas objektu saskaņā ar 43. panta 2. punkta a) apakšpunktu un tiem nav interešu konflikta atbilstīgi 43. panta 2. punkta e) apakšpunktam;
3. tie apņemas ievērot 42. panta 5. punktā minētos kritērijus saskaņā ar 43. panta 2. punkta b) apakšpunktu;
4. ir atbilstošas un piemērotas zināšanas un pieredze datu aizsardzības tiesību aktu piemērošanā;
5. ir atbilstošas un piemērotas zināšanas un pieredze tehniskajos un organizatoriskajos datu aizsardzības pasākumos atkarībā no gadījuma.
6. Tie var apliecināt pieredzi jomās, kas minētas papildu prasībās 6.1.1., 6.1.4. un 6.1.5. punktā, konkrēti

Darbinieki ar tehniskajām zināšanām:

- ir ieguvuši kvalifikāciju attiecīgajā tehnisko zināšanu jomā vismaz EKI[20] 6. līmenī vai atzītu aizsargātu nosaukumu (piemēram, *Dipl. Ing*.) attiecīgajā reglamentētajā profesijā, vai tiem ir būtiska profesionālā pieredze.
- *Darbiniekiem, kuri ir atbildīgi par sertifikācijas lēmumiem*, ir nepieciešama būtiska profesionālā pieredze datu aizsardzības pasākumu noteikšanā un īstenošanā.
- *Darbiniekiem, kuri ir atbildīgi par izvērtēšanu*, nepieciešama profesionāla pieredze tehnisko datu aizsardzībā, kā arī zināšanas un pieredze salīdzināmajā procedūrā (piemēram, sertifikācija/revīzija), kā arī attiecīgā gadījumā jābūt reģistrētiem.

Darbiniekiem jāapliecina jomai specifisko zināšanu par tehniskajām un revīzijas prasmēm uzturēšana, nepārtraukti profesionāli pilnveidojoties.

Darbinieki ar juridiskajām zināšanām:

[20] Skatīt kvalifikācijas satvara salīdzinājuma rīku vietnē https://ec.europa.eu/ploteus/en/compare?

- studijas tiesību zinātnēs ES vai attiecīgās valsts atzītā universitātē vismaz astoņu semestru garumā, ieskaitot akadēmiskā maģistra grādu (LL.M.) vai līdzvērtīgu, vai būtiska profesionālā pieredze.
- *Darbiniekiem, kuri ir atbildīgi par sertifikācijas lēmumiem*, ir jāpierāda būtiska profesionālā pieredze datu aizsardzības tiesību jomā un jābūt attiecīgi reģistrētiem, kā to pieprasa dalībvalsts.
- *Darbiniekiem, kuri ir atbildīgi par izvērtēšanu*, jāapliecina vismaz divu gadu profesionālā pieredze datu aizsardzības tiesību jomā, kā arī zināšanas un pieredze salīdzināmajās procedūrās (piemēram, sertifikācijas/revīzijas), un, ja to pieprasa dalībvalsts, jābūt reģistrētiem.
    - Darbiniekiem jāapliecina jomai specifisko zināšanu par tehniskajām un revīzijas prasmēm uzturēšana, nepārtraukti profesionāli pilnveidojoties.

6.2 Izvērtēšanai nepieciešamie resursi

Uzraudzības iestāde var noformulēt papildu prasības, ja tās ir saskaņā ar valsts tiesību aktiem.

7 PROCESA PRASĪBAS, 43. PANTA 2. PUNKTA C) UN D) APAKŠPUNKTS

7.1 Vispārīgi

Akreditācijas struktūrai papildus ISO/IEC 17065/2012 7.1. sadaļā ietvertajai prasībai ir jānodrošina, ka:

1. sertifikācijas struktūras, iesniedzot pieteikumu, ievēro kompetentās uzraudzības iestādes papildu prasības (saskaņā ar 43. panta 1. punkta b) apakšpunktu), lai uzdevumi un pienākumi neradītu interešu konfliktu 43. panta 2. punkta b) apakšpunkta izpratnē;
2. informē attiecīgās KUI, pirms sertifikācijas struktūra sāk izmantot apstiprinātu Eiropas datu aizsardzības zīmogu jaunā dalībvalstī no satelītu biroja.

7.2 Pieteikumu iesniegšana

Papildus ISO/IEC 17065/2012 7.2. punktam būtu jāpieprasa, lai

1. sertifikācijas objekts (izvērtēšanas mērķis, *ToE*) pieteikumā būtu detalizēti aprakstīts. Tas ietver arī saskarnes un pārsūtīšanu uz citām sistēmām un organizācijām, protokolus, kā arī citas garantijas;
2. pieteikumā jānorāda, vai tiek izmantoti apstrādātāji, un ja apstrādātāji ir pieteikuma iesniedzēji, jāapraksta to pienākumi un uzdevumi, un pieteikumā jāiekļauj attiecīgo(-os) pārziņa/apstrādātāja līgumu(-us).

7.3 Pieteikuma izskatīšana

Papildus ISO/IEC 17065/2012 7.3. punktam būtu jāpieprasa, lai

1. sertifikācijas līgumā būtu noteiktas saistošas novērtēšanas metodes attiecībā uz izvērtēšanas mērķi (*ToE*);
2. 7.3. punkta e) apakšpunktā minētajā novērtējumā, vai ir pietiekama kompetence, pienācīgi ņem vērā gan tehnisko, gan juridisko kompetenci datu aizsardzības jomā.

7.4 Izvērtēšana

Papildus ISO/IEC 17065/2012 7.4. punktam sertifikācijas mehānismos jāapraksta pietiekamas novērtēšanas metodes apstrādes operācijas(-u) atbilstības sertifikācijas kritērijiem novērtēšanai, tostarp, piemēram, attiecīgā gadījumā:

1. metode apstrādes darbību nepieciešamības un samērīguma attiecībā uz to mērķi un attiecīgajiem datu subjektiem novērtēšanai;
2. metode visu pārziņa un apstrādātāja apsvērto risku seguma, sastāva un izvērtējuma novērtēšanai, ņemot vērā juridiskās sekas saskaņā ar VDAR 30., 32. un 35., un 36. pantu, kā arī attiecībā uz tehnisko un organizatorisko pasākumu noteikšanu saskaņā ar VDAR 24., 25. un 32. pantu, ciktāl minētie panti attiecas uz sertifikācijas objektu, un
3. metode tiesiskās aizsardzības līdzekļu novērtēšanai, tostarp garantiju, aizsardzības pasākumu un procedūru, lai nodrošinātu personas datu aizsardzību saistībā ar apstrādi, ko attiecina uz sertifikācijas objektu, un, lai pierādītu, ka ir izpildītas kritērijos noteiktās juridiskās prasības; kā arī
4. metožu un secinājumu dokumentācija.

Sertifikācijas struktūrai būtu jānodrošina, lai šīs novērtēšanas metodes ir standartizētas un vispārēji piemērojamas. Tas nozīmē, ka salīdzināmiem *ToE* izmanto salīdzināmas novērtēšanas metodes. Jebkuras atkāpes no šīs procedūras pamato sertifikācijas struktūra.

Papildus ISO/IEC 17065/2012 7.4.2. punktam izvērtēšanu būtu jāļauj veikt ārējiem ekspertiem, kurus atzinusi sertificēšanas struktūra.

Papildus ISO/IEC 17065/2012 7.4.5. punktam būtu jāprasa, lai pašreizējā sertifikācijā varētu iekļaut datu aizsardzības sertifikāciju saskaņā ar VDAR 42. un 43. pantu, kas jau aptver daļu sertifikācijas objekta. Tomēr tas nebūs pietiekami, lai pilnībā aizstātu (daļējus) izvērtējumus. Sertifikācijas struktūrai ir pienākums pārbaudīt atbilstību kritērijiem. Atzīšana jebkurā gadījumā prasa pilnīgu izvērtējuma ziņojumu vai informāciju, kas ļauj novērtēt iepriekšējo sertifikācijas darbību un tās rezultātus. Sertifikācijas apliecinājumu vai līdzīgus sertifikācijas sertifikātus nevajadzētu uzskatīt par pietiekamiem ziņojuma aizstāšanai.

Papildus ISO/IEC 17065/2012 7.4.6. punktam būtu jāpieprasa, lai sertifikācijas struktūra savā sertifikācijas mehānismā sīki izklāstītu, kā 7.4.6. punktā prasītā informācija informē klientu (sertifikācijas pieteikuma iesniedzēju) par neatbilstībām attiecībā pret sertifikācijas mehānismu. Šajā kontekstā jānosaka vismaz šādas informācijas raksturs un sniegšanas laiks.

Papildus ISO/IEC 17065/2012 7.4.9. punktam būtu jāpieprasa, lai dokumentācija pēc pieprasījuma būtu pilnībā pieejama datu aizsardzības uzraudzības iestādei.

7.5 Pārskatīšana

Papildus ISO/IEC 17065/2012 7.5. punktam ir jābūt attiecīgo sertifikātu piešķiršanas, regulārās pārskatīšanas un atsaukšanas procedūrām saskaņā ar 43. panta 2. un 3. punktu.

7.6 Sertifikācijas lēmums

Papildus ISO/IEC 17065/2012 7.6.1. punktam sertifikācijas struktūrai būtu jāprasa savās procedūrās sīki izklāstīt, kā tiek nodrošināta tās neatkarība un atbildība par atsevišķiem sertifikācijas lēmumiem.

7.7 Sertifikācijas dokumenti

Papildus ISO/IEC 17065/2012 7.7.1. punkta e) apakšpunktam un saskaņā ar VDAR 42. panta 7. punktu būtu jāpieprasa, lai sertifikātu derīguma termiņš nepārsniegtu trīs gadus.

Papildus ISO/IEC 17065/2012 7.7.1. punkta e) apakšpunktam būtu jāpieprasa arī plānotā pārraudzības perioda 7.9. sadaļas izpratnē dokumentēšana.

Papildus ISO/IEC 17065/2012 7.7.1. punkta f) apakšpunktam sertifikācijas struktūrai jāpieprasa sertifikācijas dokumentācijā norādīt sertifikācijas objektu (norādot versijas statusu vai tamlīdzīgus raksturlielumus, ja tādi ir).

7.8 Sertificēto produktu direktorijs

Papildus ISO/IEC 17065/2012 7.8. punktam sertifikācijas struktūrai būtu jāpieprasa, lai informācija par sertificētiem produktiem, procesiem un pakalpojumiem būtu pieejama gan iekšēji, gan publiski. Sertifikācijas struktūra sniegs sabiedrībai izvērtējuma ziņojuma kopsavilkumu. Šā kopsavilkuma mērķis ir palīdzēt nodrošināt pārredzamību attiecībā uz to, kas ir sertificēts un kā tas ticis novērtēts. Tajā tiks izskaidroti šādi jautājumi:

(a) sertifikācijas darbības joma un jēgpilns sertifikācijas objekta (*ToE*) apraksts,

(b) attiecīgie sertifikācijas kritēriji (ieskaitot versiju vai funkcionālo statusu),

(c) veiktās novērtēšanas metodes un testi, un

(d) rezultāts(-i).

Papildus ISO/IEC 17065/2012 7.8. punktam un saskaņā ar VDAR 43. panta 5. punktu sertifikācijas struktūra informē kompetentās uzraudzības iestādes par pieprasītā sertifikāta piešķiršanas vai atsaukšanas iemesliem.

7.9 Pārraudzība

Papildus ISO/IEC 17065/2012 7.9.1., 7.9.2. un 7.9.3. punktam un saskaņā ar VDAR 43. panta 2. punkta c) apakšpunktu būtu jāpieprasa, lai regulārie uzraudzības pasākumi būtu obligāti sertifikācijas uzturēšanai pārraudzības periodā.

7.10 Izmaiņas, kas skar sertifikāciju

Papildus EN ISO/IEC 17065/2012 7.10.1. un 7.10.2. punktam sertifikāciju ietekmējošām izmaiņām, kuras sertifikācijas struktūras jāņem vērā, jāietver: grozījumi datu aizsardzības tiesību aktos, Eiropas Komisijas deleģēto aktu pieņemšana saskaņā ar 43. panta 8. un 9. punktu, Eiropas Datu aizsardzības kolēģijas lēmumi un ar datu aizsardzību saistīti tiesas lēmumi. Šeit paredzētās izmaiņu procedūras varētu ietvert tādus jautājumus kā: pārejas periodi, apstiprināšanas process kompetentajā uzraudzības iestādē, attiecīgā sertifikācijas objekta atkārtota novērtēšana un atbilstoši pasākumi sertifikāta atcelšanai, ja sertificētā apstrādes darbība vairs neatbilst atjauninātajiem kritērijiem.

7.11 Sertifikācijas izbeigšana, samazināšana, apturēšana vai atsaukšana

Papildus ISO/IEC 17065/2012 7.11.1. iedaļai sertifikācijas struktūrai nekavējoties jāinformē kompetentā uzraudzības iestāde un VAS rakstiski par veiktajiem pasākumiem un par sertifikācijas turpināšanu, ierobežojumiem, apturēšanu vai atsaukšanu.

Saskaņā ar 58. panta 2. punkta h) apakšpunktu sertifikācijas struktūrai ir jāpieņem kompetentās uzraudzības iestādes lēmumi un rīkojumi par sertifikāta atsaukšanu vai neizsniegšanu klientam (pieteikuma iesniedzējam), ja sertifikāciju prasības nav vai vairs nav izpildītas.

7.12 Ieraksti

Sertifikācijas struktūrai būtu jāpieprasa, lai visa dokumentācija būtu pilnīga, saprotama, atjaunināta un piemērota revīzijai.

7.13 Sūdzības un pārsūdzības, 43. panta 2. punkta d) apakšpunkts

Papildus ISO/IEC 17065/2012 7.13.1. punktam sertifikācijas struktūrai būtu jāpieprasa definēt,

(a) kas ir tiesīgs iesniegt sūdzības vai iebildumus,

(b) kas tās apstrādā sertifikācijas struktūras vārdā,

(c) kādas pārbaudes šajā saistībā tiek veiktas; kā arī

(d) apspriešanās ar ieinteresētajām personām iespējas.

Papildus ISO/IEC 17065/2012 7.13.2. punktam sertifikācijas struktūrai būtu jāpieprasa definēt,

(a) kādā veidā un kam šāds apstiprinājums izsniedzams,

(b) tam piemērojamie termiņi; kā arī

(c) kādi procesi pēc tam uzsākami.

Papildus ISO/IEC 17065/2012 7.13.1. punktam sertifikācijas struktūrai jānosaka, kā tiek nodrošināta sertifikācijas darbību nodalīšana un pārsūdzību un sūdzību izskatīšana.

8 PĀRVALDĪBAS SISTĒMAS PRASĪBAS

Pārvaldības sistēmas vispārēja prasība saskaņā ar ISO/IEC 17065/2012 8. iedaļu ir tāda, ka visu iepriekšējo iedaļu prasību īstenošana akreditētās sertifikācijas struktūras sertifikācijas mehānisma darbības jomā ir dokumentēta, izvērtēta, kontrolēta un neatkarīgi pārraudzīta.

Pārvaldības pamatprincips ir tādas sistēmas definēšana, saskaņā ar kuru tās mērķi tiek izvirzīti efektīvi un lietderīgi, konkrēti: sertifikācijas pakalpojumu ieviešana, izmantojot atbilstošas specifikācijas. Tas prasa pārredzamību un pārbaudāmību attiecībā uz akreditācijas prasību īstenošanu sertificēšanas struktūrā un to pastāvīgu ievērošanu.

Šim nolūkam pārvaldības sistēmā ir jānosaka metodika šo prasību izpildes panākšanai un kontrolei saskaņā ar datu aizsardzības noteikumiem un pastāvīgi tās jāpārbauda kopā ar pašu akreditēto struktūru.

Šiem pārvaldības principiem un to dokumentētajai īstenošanai jābūt pārredzamai, un akreditētajai sertifikācijas struktūrai tie jāatklāj atbilstīgi 58. pantā paredzētajai akreditācijas procedūrai un turpmāk pēc datu aizsardzības uzraudzības iestādes pieprasījuma jebkurā laikā, veicot izmeklēšanu datu aizsardzības pārskatīšanas veidā saskaņā ar 58. panta 1. punkta b) apakšpunktu vai saskaņā ar 42. panta 7. punktu izsniegto sertifikātu pārskatīšanu atbilstīgi 58. panta 1. punkta c) apakšpunktam.

Jo īpaši akreditētajai sertifikācijas struktūrai pastāvīgi un nepārtraukti jāpublisko, kādas sertifikācijas tikušas veiktas uz kāda pamata (vai atbilstīgi kādiem sertifikācijas mehānismiem vai shēmām), cik ilgi sertifikāti ir derīgi, saskaņā ar kādiem noteikumiem un nosacījumiem (100. apsvērums).

8.1 Vispārīgās pārvaldības sistēmas prasības

Kompetentā uzraudzības iestāde var precizēt un pievienot papildu prasības, ja tas ir saskaņā ar valsts tiesību aktiem.

8.2 Pārvaldības sistēmas dokumentācija

Kompetentā uzraudzības iestāde var precizēt un pievienot papildu prasības, ja tas ir saskaņā ar valsts tiesību aktiem.

8.3 Dokumentu vadība

Kompetentā uzraudzības iestāde var precizēt un pievienot papildu prasības, ja tas ir saskaņā ar valsts tiesību aktiem.

8.4 Dokumentvedība

Kompetentā uzraudzības iestāde var precizēt un pievienot papildu prasības, ja tas ir saskaņā ar valsts tiesību aktiem.

8.5 Pārvaldības apskats

Kompetentā uzraudzības iestāde var precizēt un pievienot papildu prasības, ja tas ir saskaņā ar valsts tiesību aktiem.

8.6 Iekšējā revīzija

Kompetentā uzraudzības iestāde var precizēt un pievienot papildu prasības, ja tas ir saskaņā ar valsts tiesību aktiem.

8.7 Koriģējošas darbības

Kompetentā uzraudzības iestāde var precizēt un pievienot papildu prasības, ja tas ir saskaņā ar valsts tiesību aktiem.

8.8 Preventīvie pasākumi

Kompetentā uzraudzības iestāde var precizēt un pievienot papildu prasības, ja tas ir saskaņā ar valsts tiesību aktiem.

9 SĪKĀKAS PAPILDU PRASĪBAS21

9.1 Novērtēšanas metožu atjaunināšana

Sertifikācijas struktūra izstrādā procedūras, lai vadītu novērtēšanas metožu atjaunināšanu piemērošanai saistībā ar izvērtējumu atbilstīgi 7.4. punktam. Atjauninājumi jāveic, mainoties tiesiskajam regulējumam, attiecīgajam(-ajiem) riskam(-iem), jaunākajiem tehnoloģijas sasniegumiem un tehnisko un organizatorisko pasākumu īstenošanas izmaksām.

9.2 Zināšanu līmeņa uzturēšana

Sertifikācijas struktūras izstrādā procedūras, ar ko nodrošina savu darbinieku apmācību, lai atjauninātu viņu prasmes, ņemot vērā 9.1. punktā uzskaitītās attīstības tendences.

9.3 Pienākumi un kompetences

9.3.1 Saziņa starp sertifikācijas struktūru un tās klientiem

Ir jāievieš procedūras atbilstīgo procedūru un komunikācijas struktūru ieviešanai starp sertifikācijas struktūru un tās klientu. Tas ietver

1. uzdevumu un pienākumu dokumentācijas uzturēšanu, ko veic akreditēta sertifikācijas struktūra šādiem nolūkiem
    a. informācijas pieprasījumi, vai
    b. lai nodrošinātu kontaktu sūdzības par sertifikāciju gadījumā.
2. Pieteikuma procesa uzturēšanu šādiem nolūkiem
    a. informācijai par pieteikuma statusu;
    b. kompetentās uzraudzības iestādes izvērtējumiem attiecībā uz
        i. atsauksmēm;

[21] Kompetentā uzraudzības iestāde var precizēt un pievienot papildu prasības, ja tas ir saskaņā ar valsts tiesību aktiem.

ii. kompetento uzraudzības iestāžu lēmumiem.

9.3.2 Izvērtēšanas darbību dokumentēšana

Uzraudzības iestāde var noformulēt papildu prasības.

9.3.3 Sūdzību izskatīšanas pārvaldīšana

Sūdzību izskatīšana jāizveido kā pārvaldības sistēmas neatņemama sastāvdaļa, kas jo īpaši īsteno ISO/IEC 17065/2012 4.1.2.2. punkta c) un j) apakšpunktā, 4.6. punkta d) apakšpunktā un 7.13. punktā noteiktās prasības.

Attiecīgās sūdzības un iebildumi būtu jāiesniedz kompetentajai uzraudzības iestādei.

9.3.4 Atsaukšanas pārvaldība

Akreditācijas apturēšanas vai atsaukšanas gadījumā procedūras integrē sertifikācijas struktūras pārvaldības sistēmā, tostarp klientu paziņojumus.