Suunised

Suunised 4/2018 isikuandmete kaitse üldmääruse (2016/679) artikli 43 kohase sertifitseerimisasutuste akrediteerimise kohta

Versioon 3.0

4. juuni 2019

Vastu võetud

Versioonid

Versioon 3.0	4. juuni 2019	1. lisa (1. lisa versioon 2.0, mis võeti vastu 4. juunil 2019 pärast avalikku konsultatsiooni) lisamine
Versioon 2.0	4. detsember 2018	Suuniste vastuvõtmine pärast avalikku konsultatsiooni – samal kuupäeval võeti avalikuks konsultatsiooniks vastu 1. lisa (versioon 1.0)
Versioon 1.0	6. veebruar 2018	Suuniste vastuvõtmine artikli 29 töörühma poolt (avalikuks konsultatsiooniks mõeldud versioon). Euroopa Andmekaitsenõukogu kiitis selle versiooni heaks 25. mail 2018.

Sisukord

Euroopa Andmekaitsenõukogu,

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta) artikli 70 lõike 1 punkti e,

võttes arvesse, et isikuandmete kaitse üldmääruse artikli 70 lõikega 4 on ette nähtud avalik konsultatsioon, ja arvestades veebruaris 2018 suuniste üle toimunud avaliku konsultatsiooni ning 14. detsembrist 2018 kuni 1. veebruarini 2019 lisa üle toimunud avaliku konsultatsiooni tulemusi,

ON VASTU VÕTNUD JÄRGMISED SUUNISED:

1 SISSEJUHATUS

1. 25. mail 2018 jõustunud isikuandmete kaitse üldmäärusega (määrus (EL) 2016/679) on ette nähtud ajakohastatud vastutus- ja põhiõiguste järgimise raamistik andmete kaitsmiseks Euroopas. Uue raamistiku keskmes on mitmesugused meetmed, mis hõlbustavad isikuandmete kaitse üldmääruse sätetest kinnipidamist. Need meetmed hõlmavad teatud asjaoludel kohaldatavaid kohustuslikke nõudeid (sh andmekaitseametnike määramine ja andmekaitsealaste mõjuhinnangute tegemine) ning vabatahtlikke meetmeid, näiteks toimimisjuhendid ja sertifitseerimismehhanismid.
2. Vastavalt isikuandmete kaitse üldmääruse artikli 43 lõikele 1 peavad liikmesriigid sertifitseerimismehhanismide ning andmekaitsepitserite ja -märgiste kasutuselevõtu osana kindlaks määrama, kas artikli 42 lõike 1 kohaselt sertifikaate väljastavad sertifitseerimisasutused akrediteerib pädev järelevalveasutus või riiklik akrediteerimisasutus või mõlemad. Kui akrediteerib riiklik akrediteerimisasutus standardi ISO/IEC 17065/2012 kohaselt, tuleb täita ka pädeva järelevalveasutuse kehtestatud täiendavaid nõudeid.
3. Asjakohased sertifitseerimismehhanismid võivad parandada isikuandmete kaitse üldmääruse järgimist ning suurendada läbipaistvust nii andmesubjektide jaoks kui ka ettevõtjate, näiteks vastutavate töötlejate ja volitatud töötlejate vahelistes suhetes. Vastutavate töötlejate ja volitatud töötlejate jaoks on sõltumatu kolmanda isiku tehtav atesteerimine kasulik, sest võimaldab neil tõendada oma andmetöötlustoimingute vastavust nõuetele[1].
4. Euroopa Andmekaitsenõukogu tunnistab sellega seoses vajadust kehtestada akrediteerimise suunised. Akrediteerimise eriline väärtus ja otstarve on, et sellega antakse sertifitseerimisasutuste pädevusele usaldusväärne hinnang, mis võimaldab luua usaldust sertifitseerimismehhanismi suhtes.

[1] Isikuandmete kaitse üldmääruse põhjenduses 100 on märgitud, et sertifitseerimismehhanismide kasutuselevõtt võib parandada läbipaistvust ja määruse järgimist ning anda andmesubjektidele võimaluse hinnata asjakohaste toodete ja teenuste andmekaitse taset.

5. Suuniste eesmärk on anda juhiseid, kuidas tõlgendada ja rakendada isikuandmete kaitse üldmääruse artikli 43 sätteid. Eelkõige on eesmärk aidata liikmesriikidel, järelevalveasutustel ja riiklikel akrediteerimisasutustel kehtestada järjekindlad ühtlustatud põhimõtted selliste sertifitseerimisasutuste akrediteerimiseks, kes väljastavad sertifikaate kooskõlas isikuandmete kaitse üldmäärusega.

2 SUUNISTE KOHALDAMISALA

6. Käesolevates suunistes

- sätestatakse akrediteerimise eesmärk isikuandmete kaitse üldmääruse kontekstis;
- selgitatakse sertifitseerimisasutuste akrediteerimise eri võimalusi vastavalt artikli 43 lõikele 1 ja selgitatakse välja peamised küsimused, mida tuleb arvesse võtta;
- esitatakse täiendavate akrediteerimisnõuete kehtestamise raamistik juhuks, kui akrediteerib riiklik akrediteerimisasutus, ja
- esitatakse akrediteerimisnõuete kehtestamise raamistik juhuks, kui akrediteerib järelevalveasutus.

7. Suunised ei ole menetlusjuhend sertifitseerimisasutuste akrediteerimiseks kooskõlas isikuandmete kaitse üldmäärusega. Nendega ei kehtestata sertifitseerimisasutuste akrediteerimise uut tehnilist standardit isikuandmete kaitse üldmääruse kohaldamisel.

8. Suunised on adresseeritud

- liikmesriikidele, kes peavad kindlaks määrama, kas sertifitseerimisasutused akrediteerib järelevalveasutus ja/või riiklik akrediteerimisasutus;
- riiklikele akrediteerimisasutustele, kes akrediteerivad sertifitseerimisasutusi vastavalt artikli 43 lõike 1 punktile b;
- pädevatele järelevalveasutustele, kes sätestavad standardile ISO/IEC 17065/2012[2] lisanduvad täiendavad nõuded, kui akrediteerib riiklik akrediteerimisasutus vastavalt artikli 43 lõike 1 punktile b;
- Euroopa Andmekaitsenõukogule, kui ta esitab pädeva järelevalveasutuse akrediteerimisnõuete kohta arvamuse ja kiidab need heaks vastavalt artikli 43 lõikele 3, artikli 70 lõike 1 punktile p ja artikli 64 lõike 1 punktile c;
- pädevatele järelevalveasutustele, kes sätestavad akrediteerimisnõuded, kui akrediteerib järelevalveasutus vastavalt artikli 43 lõike 1 punktile a;
- teistele sidusrühmadele, näiteks tulevastele sertifitseerimisasutustele või sertifitseerimiskriteeriume ja -menetlusi kehtestavatele sertifitseerimissüsteemi omanikele[3].

[2] Rahvusvaheline Standardiorganisatsioon, „Conformity assessment – Requirements for bodies certifying products, processes and services“.

[3] Süsteemi omanik on tuvastatav organisatsioon, kes on kehtestanud sertifitseerimiskriteeriumid ja -nõuded, mille alusel hinnatakse nõuetele vastavust. Akrediteeritakse organisatsioone (sertifitseerimisasutusi ehk vastavushindamisasutusi), kes teevad hindamisi (artikli 43 lõige 4) sertifitseerimissüsteemi nõuete põhjal ja väljastavaid sertifikaate. Hindav organisatsioon võib olla sama organisatsioon, kes on süsteemi välja töötanud ja on selle omanik, kuid on võimalikud ka olukorrad, kus süsteemi omanik on üks organisatsioon ja seda hindab teine (hindavad teised) organisatsioon(id).

9. Mõisted

10. Järgmiste mõistete eesmärk on edendada akrediteerimisprotsessi põhielementide ühist mõistmist. Mõisteid tuleb käsitada võrdlusalusena ja need võivad ajas muutuda. Mõisted põhinevad olemasolevatel õigusraamistikel ja standarditel, eelkõige isikuandmete kaitse üldmääruse ja standardi ISO/IEC 17065/2012 asjakohastel sätetel.

11. Suunistes kasutatakse järgmisi mõisteid:

12. „akrediteerimine“ – sertifitseerimisasutuste akrediteerimine, vt punkt 3 „Akrediteerimise tõlgendamine isikuandmete kaitse üldmääruse artikli 43 kohaldamisel“;

13. „täiendavad nõuded“ – pädeva järelevalveasutuse kehtestatud nõuded, mille alusel akrediteeritakse[4];

14. „sertifitseerimine“ – kolmanda isiku tehtav hindamine ja objektiivne atesteerimine,[5] mis kinnitab, et sertifitseerimiskriteeriumide täitmine on tõendatud;

15. „sertifitseerimisasutus“ – kolmanda isikuna vastavust hindav[6] asutus[7], mis haldab sertifitseerimismehhanisme[8];

16. „sertifitseerimissüsteem“ – selliste kindlaksmääratud toodete, protsesside ja teenustega seotud sertifitseerimissüsteem, mille suhtes kohaldatakse samu kindlaksmääratud nõudeid, erieeskirju ja menetlusi[9];

17. „kriteeriumid“ või „sertifitseerimiskriteeriumid“ – kriteeriumid, mille alusel sertifitseeritakse (vastavushinnatakse)[10];

18. „riiklik akrediteerimisasutus“ – Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 765/2008 kohaselt määratud ainus akrediteeriv asutus liikmesriigis, kelle on selleks volitanud riik[11].

[4] Artikli 43 lõiked 1, 3 ja 6.

[5] Standardi ISO 17000 kohaselt on kolmanda isiku tehtav atesteerimine (sertifitseerimine) „kohaldatav kõigile vastavushindamise objektidele“ (5.5), „välja arvatud vastavushindamisasutustele endile, mille suhtes kohaldatakse akrediteerimist“ (5.6).

[6] Kolmanda isikuna hindab vastavust organisatsioon, kes ei sõltu hindamisobjekti esitavast isikust või organisatsioonist ega objektiga seotud kasutaja huvidest, vt ISO 17000, 2.4.

[7] Vt ISO 17000, 2.5: „asutus, mis osutab vastavushindamise teenuseid“; ISO 17011: „asutus, mis osutab vastavushindamise teenuseid ja mis võib olla akrediteerimise objekt“; ISO 17065, 3.12.

[8] Isikuandmete kaitse üldmääruse artikli 42 lõiked 1 ja 5.

[9] Vt 3.9 koostoimes standardi ISO 17065 B lisaga.

[10] Vt artikli 42 lõige 5.

[11] Vt määruse (EÜ) nr 765/2008 artikli 2 punkt 11.

3 AKREDITEERIMISE TÕLGENDAMINE ISIKUANDMETE KAITSE ÜLDMÄÄRUSE ARTIKLI 43 KOHALDAMISEL

19. Isikuandmete kaitse üldmääruses ei ole akrediteerimist määratletud. Määruse (EÜ) nr 765/2008 (milles nähakse ette akrediteerimise üldnõuded) artikli 2 punktis 10 on akrediteerimine määratletud järgmiselt:

20. „riikliku akrediteerimisasutuse poolt läbiviidav vastavushindamisasutuse atesteerimine, mis tõendab tema vastavust kindlaksmääratud vastavushindamisülesande täitmiseks harmoneeritud standardi põhjal kehtestatud nõuetele ja vajaduse korral mis tahes lisanõuetele, sealhulgas asjaomaste valdkondlike normide alusel kehtestatud nõuetele“.

21. Standardis ISO/IEC 17011 on sätestatud:

22. „akrediteerimine tähendab kolmanda isiku poolt läbiviidavat vastavushindamisasutuse atesteerimist, mis tõendab ametlikult tema pädevust konkreetsete vastavushindamisülesannete täitmisel“.

23. Artikli 43 lõikes 1 on sätestatud:

24. „Ilma et see piiraks artiklite 57 ja 58 kohaseid pädeva järelevalveasutuse ülesandeid ja volitusi, väljastab sertifikaadi ja pikendab seda sertifitseerimisasutus, millel on andmekaitse vallas asjakohased eksperditeadmised, olles enne järelevalveasutust teavitanud, et see saaks vajaduse korral kasutada oma volitusi vastavalt artikli 58 lõike 2 punktile h. Liikmesriik tagab, et neid sertifitseerimisasutusi akrediteerib üks või mõlemad järgmistest:

    (a) artikli 55 või 56 kohaselt pädev järelevalveasutus;
    (b) Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 765/2008 kohaselt, kooskõlas standardiga ISO/IEC 17065/2012 ning artiklite 55 või 56 kohaselt pädeva järelevalveasutuse kehtestatud täiendavate nõuete kohaselt nimetatud riiklik akrediteerimisasutus.“

25. Isikuandmete kaitse üldmääruse kohaldamisel lähtutakse akrediteerimisnõuete puhul

- standardist ISO/IEC 17065/2012 ja „täiendavatest nõuetest“, mille pädev järelevalveasutus kehtestab kooskõlas artikli 43 lõike 1 punktiga b, kui akrediteerib riiklik akrediteerimisasutus, ja mille järelevalveasutus kehtestab siis, kui ta akrediteerib ise.

26. Mõlemal juhul peavad konsolideeritud nõuded hõlmama artikli 43 lõikes 2 nimetatud nõudeid.

27. Euroopa Andmekaitsenõukogu tunnistab, et akrediteerimise eesmärk on anda usaldusväärne hinnang asutuse pädevusele viia läbi sertifitseerimist (vastavushindamist)[12]. Isikuandmete kaitse üldmääruse kohaldamisel tähendab akrediteerimine järgmist:

28. riikliku akrediteerimisasutuse ja/või järelevalveasutuse tehtav atesteerimine[13], mis tõendab, et sertifitseerimisasutus[14] on kvalifitseeritud sertifitseerima vastavalt isikuandmete kaitse

[12] Vt määruse (EÜ) nr 765/2008 põhjendus 15.
[13] Vt Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta määruse (EÜ) nr 765/2008 (millega sätestatakse akrediteerimise ja turujärelevalve nõuded seoses toodete turustamisega) artikli 2 punkt 10.
[14] Vt seoses termini „akrediteerimine“ määratlusega standard ISO 17011.

üldmääruse artiklitele 42 ja 43, võttes arvesse standardit ISO/IEC 17065/2012 ning järelevalveasutuse ja andmekaitsenõukogu kehtestatud täiendavaid nõudeid.

4 AKREDITEERIMINE VASTAVALT ISIKUANDMETE KAITSE ÜLDMÄÄRUSE ARTIKLI 43 LÕIKELE 1

29. Artikli 43 lõikes 1 tunnistatakse, et sertifitseerimisasutuse akrediteerimiseks on mitu võimalust. Isikuandmete kaitse üldmääruses nõutakse, et järelevalveasutused ja liikmesriigid määratleksid sertifitseerimisasutuste akrediteerimise protsessi. Käesolevas jaos käsitletakse artiklis 43 sätestatud akrediteerimisvõimalusi.

4.1 Liikmesriikide roll

30. Artikli 43 lõikes 1 nõutakse liikmesriikidelt selle *tagamist*, et sertifitseerimisasutused akrediteeritakse, kuid antakse igale liikmesriigile võimalus otsustada, kes vastutab akrediteerimisega lõppeva hindamise tegemise eest. Artikli 43 lõike 1 kohaselt on olemas kolm võimalust olenevalt sellest, kas akrediteerib

(1) üksnes järelevalveasutus vastavalt enda kehtestatud nõuetele;
(2) üksnes määruse (EÜ) nr 765/2008 kohaselt määratud riiklik akrediteerimisasutus vastavalt standardile ISO/IEC 17065/2012 ja pädeva järelevalveasutuse kehtestatud täiendavatele nõuetele või
(3) järelevalveasutus ja riiklik akrediteerimisasutus mõlemad (vastavalt kõigile eespool punktis 2 loetletud nõuetele).

31. Liikmesriik peab otsustama, kas akrediteerib riiklik akrediteerimisasutus või järelevalveasutus või mõlemad, kuid igal juhul peab ta tagama selleks piisavad vahendid[15].

4.2 Koostoime määrusega (EÜ) nr 765/2008

32. Euroopa Andmekaitsenõukogu märgib, et määruse (EÜ) nr 765/2008 artikli 2 punktis 11 on riiklik akrediteerimisasutus määratletud kui „*ainus* akrediteerimist teostav asutus liikmesriigis, kes on selleks riigi poolt volitatud“.

33. Artikli 2 punkti 11 võib pidada vastuolus olevaks isikuandmete kaitse üldmääruse artikli 43 lõikega 1, mille kohaselt võib akrediteerida ka muu asutus kui liikmesriigi riiklik akrediteerimisasutus. Andmekaitsenõukogu leiab, et Euroopa Liidu õigusaktiga kavatseti teha erand üldpõhimõttest, mille kohaselt akrediteerib ainult riiklik akrediteerimisasutus, andes järelevalveasutustele sertifitseerimisasutuste akrediteerimiseks samad volitused. Artikli 43 lõige 1 on seega määruse (EÜ) nr 765/2008 artikli 2 punkti 11 suhtes erinorm.

4.3 Riikliku akrediteerimisasutuse roll

34. Artikli 43 lõike 1 punktis b on sätestatud, et riiklik akrediteerimisasutus akrediteerib sertifitseerimisasutused kooskõlas standardiga ISO/IEC 17065/2012 ja pädeva järelevalveasutuse kehtestatud täiendavate nõuetega.

35. Euroopa Andmekaitsenõukogu märgib selguse huvides, et konkreetne viide artikli 43 lõikes 3 lõike 1 punktile b tähendab, et väljend „need nõuded“ osutab täiendavatele nõuetele, mille

[15] Vt määruse (EÜ) nr 765/2008 artikli 4 lõige 9.

pädev järelevalveasutus kehtestab vastavalt artikli 43 lõike 1 punktile b, ja artikli 43 lõikes 2 sätestatud nõuetele.

36. Riiklikud akrediteerimisasutused peavad akrediteerimisel kohaldama täiendavaid nõudeid, mille kehtestavad järelevalveasutused.

37. Kui sertifitseerimisasutus, mis on standardi ISO/IEC 17065/2012 alusel akrediteeritud muude kui isikuandmete kaitse üldmäärusega seotud sertifitseerimissüsteemide osas, soovib laiendada oma akrediteeringut isikuandmete kaitse üldmääruse kohaselt väljastatavatele sertifikaatidele, peab ta vastama järelevalveasutuse kehtestatud täiendavatele nõuetele, kui akrediteerib riiklik akrediteerimisasutus. Kui isikuandmete kaitse üldmääruse kohast sertifitseerimist akrediteerib üksnes pädev järelevalveasutus, peab akrediteerimist taotlev sertifitseerimisasutus vastama asjaomase järelevalveasutuse kehtestatud nõuetele.

4.4 Järelevalveasutuse roll

38. Euroopa Andmekaitsenõukogu märgib, et artikli 57 lõike 1 punktis q on sätestatud, et järelevalveasutus *akrediteerib* artikli 43 kohaselt sertifitseerimisasutuse, täites sellega järelevalveasutuse ülesande vastavalt artiklile 57, ja artikli 58 lõike 3 punktis e on sätestatud, et järelevalveasutusel on lubavad ja nõuandvad volitused akrediteerida sertifitseerimisasutused vastavalt artiklile 43. Artikli 43 lõike 1 sõnastus võimaldab teatavat paindlikkust ja järelevalveasutuse akrediteerimisfunktsiooni tuleks käsitada ülesandena üksnes asjakohastel juhtudel. Seda punkti saab täpsustada liikmesriikide õigusega. Riikliku akrediteerimisasutuse tehtaval akrediteerimisel on sertifitseerimisasutus artikli 43 lõike 2 punkti a kohaselt siiski kohustatud tõendama pädeva järelevalveasutuse jaoks rahuldavalt, et on sõltumatu ja omab eksperditeadmisi järelevalveasutuse pakutava sertifitseerimise sisu osas[16].

39. Kui liikmesriik sätestab, et sertifitseerimisasutused akrediteerib järelevalveasutus, peaks järelevalveasutus kehtestama akrediteerimisnõuded, mis hõlmavad artikli 43 lõikes 2 sätestatud nõudeid, kuid ei ole nendega piiratud. Artiklis 43 on sätestatud vähem juhiseid akrediteerimisnõuete kohta juhuks, kui järelevalveasutus akrediteerib ise, võrreldes kohustustega, mis on seotud sertifitseerimisasutuste akrediteerimisega riiklike akrediteerimisasutuste poolt. Akrediteerimise ühtlasema käsitluse huvides peaksid järelevalveasutuse kasutatavad akrediteerimiskriteeriumid juhinduma standardist ISO/IEC 17065 ja neid tuleks täiendada täiendavate nõuetega, mille järelevalveasutus kehtestab vastavalt artikli 43 lõike 1 punktile b. Euroopa Andmekaitsenõukogu märgib, et artikli 43 lõike 2 punktides a–e kajastatakse ja täpsustatakse standardi ISO 17065 nõudeid, mis aitab suurendada järjepidevust.

40. Kui liikmesriik sätestab, et sertifitseerimisasutused akrediteerib riiklik akrediteerimisasutus, peaks järelevalveasutus kehtestama määruses (EÜ) nr 765/2008 (mille artiklid 3–14 käsitlevad vastavushindamisasutuste korraldust ja akrediteerimistegevust) sätestatud olemasolevaid akrediteerimistavasid täiendavad nõuded ja tehnilised eeskirjad, milles kirjeldatakse sertifitseerimisasutuste meetodeid ja menetlusi. Seda arvesse võttes on määruses (EÜ) nr 765/2008 sätestatud täiendavad juhised: artikli 2 punktis 10 on akrediteerimise määratlus ning viidatakse „harmoneeritud standarditele“ ja „lisanõuetele, sealhulgas asjaomaste

[16] Sõltumatuse ja eksperditeadmiste nõuded tuleks sätestada täiendavates nõuetes, mille järelevalveasutus kehtestab vastavalt artikli 43 lõike 1 punktile b. Vt ka suuniste 1. lisa.

valdkondlike normide alusel kehtestatud nõuetele“. Sellest tuleneb, et järelevalveasutuse kehtestatavad täiendavad nõudeid peaksid sisaldama konkreetseid nõudeid ja olema suunatud sellele, et toetada muu hulgas sertifitseerimisasutuste sõltumatuse ja andmekaitse eksperditeadmiste taseme hindamist, näiteks seoses nende suutlikkusega hinnata ja sertifitseerida vastutavate töötlejate ja volitatud töötlejate isikuandmete töötlemise toiminguid vastavalt artikli 42 lõikele 1. See hõlmab pädevust, mis on nõutav valdkondlike normide kohaselt ning seoses füüsiliste isikute põhiõiguste ja -vabaduste kaitsega ning eelkõige nende õigusega isikuandmete kaitsele[17]. Käesolevate suuniste lisa annab pädevatele järelevalveasutustele kasulikku teavet, kui nad kehtestavad täiendavaid nõudeid vastavalt artikli 43 lõike 1 punktile b ja artikli 43 lõikele 3.

41. Artikli 43 lõikes 6 on sätestatud, et „[j]ärelevalveasutus avaldab kergesti kättesaadaval kujul käesoleva artikli lõikes 3 osutatud nõuded ja artikli 42 lõikes 5 osutatud kriteeriumid“. Läbipaistvuse tagamiseks tuleb seega avaldada kõik järelevalveasutuse heakskiidetud kriteeriumid ja nõuded. Sertifitseerimisasutuste kvaliteedi ja nende usaldusväärsuse nimel on soovitatav, et kõik akrediteerimisnõuded oleksid üldsusele lihtsalt kättesaadavad.

4.5 Sertifitseerimisasutusena tegutsev järelevalveasutus

42. Artikli 42 lõike 5 kohaselt võib järelevalveasutus väljastada sertifikaate, kuid isikuandmete kaitse üldmääruses ei nõuta, et järelevalveasutus peab olema määruse (EÜ) nr 765/2008 nõuetele vastamiseks akrediteeritud. Euroopa Andmekaitsenõukogu märgib, et artikli 43 lõike 1 punktis a ning eriti artikli 58 lõike 2 punktis h ja lõike 3 punktides a ja e–f volitatakse järelevalveasutusi tegema mõlemat, akrediteerima ja sertifitseerima, ning ühtlasi andma nõu ja vajaduse korral võtma sertifikaat tagasi või andma sertifitseerimisasutustele korraldus jätta sertifikaat väljastamata.

43. Võib olla olukordi, kus akrediteerimise ja sertifitseerimise ülesannete ja kohustuste eraldamine on asjakohane või nõutav, näiteks kui liikmesriigis tegutsevad korraga järelevalveasutus ja muud sertifitseerimisasutused ning mõlemad väljastavad samu sertifikaate. Järelevalveasutused peaksid seetõttu võtma piisavad korralduslikud meetmed isikuandmete kaitse üldmääruse kohaste ülesannete eraldamiseks, et toetada ja lihtsustada sertifitseerimismehhanismide rakendamist, vältides samas huvide konflikte, mis võivad tuleneda nendest ülesannetest. Lisaks sellele peaksid liikmesriigid ja järelevalveasutused pidama meeles Euroopa tasandil ühtlustamist, kui nad sõnastavad akrediteerimise ja sertifitseerimisega seotud riiklikke õigusakte ja menetlusi kooskõlas isikuandmete kaitse üldmäärusega.

4.6 Akrediteerimisnõuded

44. Suuniste lisas on juhised, kuidas kindlaks määrata täiendavad akrediteerimisnõuded. Lisaks isikuandmete kaitse üldmääruse asjakohaste sätete selgitamisele on selles esitatud nõuded, mida järelevalveasutused ja riiklikud akrediteerimisasutused peaksid kaaluma, et tagada vastavus isikuandmete kaitse üldmäärusele.

45. Nagu eespool märgitud, kui sertifitseerimisasutused akrediteerib riiklik akrediteerimisasutus vastavalt määrusele (EÜ) nr 765/2008, on asjakohane akrediteerimisstandard ISO/IEC 17065/2012, mida täiendavad järelevalveasutuse kehtestatud täiendavad nõuded. Isikuandmete kaitse üldmääruse kohast põhiõiguste kaitset silmas pidades põhineb artikli 43

[17] Isikuandmete kaitse üldmääruse artikli 1 lõige 2.

lõige 2 standardi ISO/IEC 17065/2012 üldsätetel. Lisas esitatud raamistikus on lähtutud artikli 43 lõikest 2 ja standardist ISO/IEC 17065/2012 nõuete ja täiendavate kriteeriumide puhul, millega hinnata sertifitseerimisasutuste andmekaitsealaseid eksperditeadmisi ning nende suutlikkust järgida füüsiliste isikute õigusi ja vabadusi isikuandmete töötlemisel vastavalt isikuandmete kaitse üldmäärusele. Euroopa Andmekaitsenõukogu märgib, et ta keskendub selle tagamisele, et sertifitseerimisasutustel oleksid asjakohased andmekaitsealased eksperditeadmised kooskõlas artikli 43 lõikega 1.

46. Järelevalveasutuse kehtestatud täiendavaid akrediteerimisnõudeid kohaldatakse kõigi akrediteerimist taotlevate sertifitseerimisasutuste suhtes. Akrediteerimisasutus hindab, kas sertifitseerimisasutus on pädev sertifitseerima kooskõlas täiendavate nõuetega ja sertifitseerimise esemega. Täpsustada tuleb konkreetsed sertifitseerimissektorid või -valdkonnad, mille suhtes sertifitseerimisasutus akrediteeritakse.

47. Ühtlasi märgib Euroopa Andmekaitsenõukogu, et andmekaitsealaseid eksperditeadmisi nõutakse lisaks standardi ISO/IEC 17065/2012 nõuetele ka siis, kui teised välisasutused, näiteks laborid või audiitorid, teevad akrediteeritud sertifitseerimisasutuse nimel toiminguid sertifitseerimisprotsessi teatavate osade või elementidega. Sellistel juhtudel ei ole nende välisasutuste akrediteerimine kooskõlas isikuandmete kaitse üldmäärusega võimalik. Et tagada nende asutuste sobivus toiminguteks, mida nad teevad akrediteeritud sertifitseerimisasutuse nimel, peab akrediteeritud sertifitseerimisasutus siiski tagama, et välisasutusel on alati akrediteeritud asutuselt nõutavad andmekaitsealased eksperditeadmised, ja tõendab nende olemasolu seoses asjaomase toiminguga.

48. Suuniste lisas esitatud täiendavate akrediteerimisnõuete kindlaksmääramise raamistik ei ole mõeldud juhendina, mida riiklikud akrediteerimisasutused või järelevalveasutused peaksid akrediteerimisprotsessis kasutama. Selles on struktuuri- ja metoodikajuhised ning seega on tegemist järelevalveasutuste abivahendiga täiendavate akrediteerimisnõuete kindlaksmääramiseks.

1. LISA

1. lisas antakse suuniseid isikuandmete kaitse üldmääruse artikli 43 lõike 1 punkti b ja artikli 43 lõike 3 kohaste standardiga ISO/IEC 17065/2012 seotud „täiendavate“ akrediteerimisnõuete täpsustamiseks.

Selles sätestatakse andmekaitse järelevalveasutuse koostatavad soovituslikud nõuded, mida riiklik akrediteerimisasutus või pädev järelevalveasutus kohaldab sertifitseerimisasutuse akrediteerimisel[18]. Need täiendavad nõuded tuleb edastada enne artikli 64 lõike 1 punkti c kohast heakskiitmist Euroopa Andmekaitsenõukogule.

Käesolevat lisa tuleks tõlgendada koostoimes standardiga ISO/IEC 17065/2012. Lisas osutatakse kõnealuse standardi jaotiste numbritele. Kui järelevalveasutus teostab artikli 43 lõike 1 punkti a kohast akrediteerimist, oleks hea tava võimaluse korral järgida seda lähenemisviisi. See toetab ELi ühtlustatud akrediteerimist.

Olenemata järgmistest suunistest või suuniste puudumisest standardi ISO/IEC 17065/2012 mis tahes elemendi kohta, võib pädev järelevalveasutus sõnastada kooskõlas siseriikliku õigusega teisigi nende elementidega seotud täiendavaid nõudeid.

0 EESSÕNA

[See jaotis on riikliku akrediteerimisasutuse ja andmekaitse järelevalveasutuse vahel kokku lepitud võimalike koostöötingimuste jaoks (nt kes vastutab taotluste vastuvõtmise eest või kuidas korraldada heakskiidetud kriteeriumide tunnustamine kui akrediteerimisprotsessi osa.]

1 KOHALDAMISALA[19]

Standardit ISO/IEC 17065/2012 kohaldatakse kooskõlas isikuandmete kaitse üldmäärusega. Lisateavet leiab akrediteerimist ja sertifitseerimist käsitlevatest suunistest. Riiklik akrediteerimisasutus ja pädev järelevalveasutus peaksid võtma akrediteerimise raames toimuval hindamisel arvesse sertifitseerimismehhanismi kohaldamisala (nt pilveteenuse töötlemistoimingute sertifitseerimine), eriti kriteeriumeid, eksperditeadmisi ja hindamismetoodikat. Tooteid, protsesse ja teenuseid hõlmava standardi ISO/IEC 17065/2012 lai kohaldamisala ei tohiks põhjustada isikuandmete kaitse üldmääruse nõuete leevendamist ega tühistamist, nt sertifitseerimismehhanismi ainus element ei saa olla juhtimismehhanism, kuna sertifitseerimine peab hõlmama isikuandmete töötlemist, st töötlemistoiminguid. Vastavalt isikuandmete kaitse üldmääruse artikli 42 lõikele 1 kohaldatakse määruse kohast sertifitseerimist vaid vastutavate töötlejate ja volitatud töötlejate sooritatavate isikuandmete töötlemise toimingute suhtes.

2 NORMIVIITED

Isikuandmete kaitse üldmäärus on standardi ISO/IEC 17065/2012 suhtes ülimuslik. Kui täiendavates nõuetes või sertifitseerimismehhanismi kohaldamisel viidatakse muudele ISO standarditele, tõlgendatakse neid kooskõlas isikuandmete kaitse üldmääruses sätestatud nõuetega.

[18] Teavet sertifitseerimiskriteeriumide heakskiitmise protsessi kohta leiab sertifitseerimissuuniste punktist 4.
[19] Kasutatakse standardi ISO/IEC 17065/2012 numeratsiooni.

3 MÕISTED JA MÄÄRATLUSED

Käesolevas lisas kohaldatakse akrediteerimissuunistes (WP 261) ja sertifitseerimissuunistes (Euroopa Andmekaitsenõukogu suunised 1/2018) kasutatud mõisteid ja määratlusi, mis on ISO standardi määratluste suhtes ülimuslikud.

4 ÜLDISED AKREDITEERIMISNÕUDED

4.1 Õiguslikud ja lepingulised küsimused

4.1.1 Õiguslikud kohustused

Sertifitseerimisasutus peaks olema võimeline riiklikule akrediteerimisasutusele või pädevale järelevalveasutusele (alati) tõendama, et ta kasutab ajakohaseid menetlusi, mis tõendavad akrediteerimistingimustes sätestatud õiguslike kohustuste, sealhulgas määruse 2016/679/EÜ kohaldamisega seotud täiendavate nõuete täitmist. Olgu öeldud, et kuna sertifitseerimisasutus on ise andmete vastutav/volitatud töötleja, peab ta suutma esitada tõendeid selle kohta, et ta rakendab määrusega 2016/679/EÜ kooskõlas olevaid menetlusi ja meetmeid, eelkõige kliendi organisatsiooni isikuandmete kontrollimisel ja käsitlemisel sertifitseerimisprotsessi raames.

Pädev järelevalveasutus võib otsustada lisada veel nõudeid ja menetlusi, et kontrollida enne akrediteerimist sertifitseerimisasutuste vastavust isikuandmete kaitse üldmäärusele.

4.1.2 Sertifitseerimisleping

Sertifitseerimislepingu miinimumnõudeid täiendatakse järgmiste punktidega.

Sertifitseerimisasutus peab tõendama lisaks standardi ISO/IEC 17065/2012 nõuete täitmisele, et tema sertifitseerimislepingud vastavad järgmistele nõuetele:

1. sertifitseerimislepingutes nähakse ette, et taotleja peab alati täitma nii üldiseid sertifitseerimisnõudeid standardi ISO/IEC 17065/2012 jaotise 4.1.2.2 lit. a tähenduses kui ka kriteeriumeid, mille pädev järelevalveasutus või Euroopa Andmekaitsenõukogu on heaks kiitnud kooskõlas artikli 43 lõike 2 punktiga b ja artikli 42 lõikega 5;
2. sertifitseerimislepingutes nähakse ette, et taotleja peab tagama pädevale järelevalveasutusele sertifitseerimismenetluses täieliku läbipaistvuse, sealhulgas konfidentsiaalsetes lepingulistes küsimustes, mis on seotud artikli 42 lõike 7 ja artikli 58 lõike 1 punkti c kohase andmekaitsenõuete täitmisega;
3. sertifitseerimislepingutega ei vähendata taotleja kohustust järgida määrust 2016/679/EÜ ega piirata artikli 42 lõike 5 alusel pädeva järelevalveasutuse ülesandeid ega volitusi;
4. sertifitseerimislepingutes nähakse ette, et taotleja peab esitama sertifitseerimisasutusele kogu teabe ja võimaldama kõnealusele asutusele juurdepääsu oma isikuandmete töötlemise toimingutele, mis on vajalik sertifitseerimismenetluse läbiviimiseks, kooskõlas artikli 42 lõikega 6;
5. sertifitseerimislepingutes nähakse ette, et taotleja peab järgima kohaldatavaid tähtaegu ja menetlusi. Sertifitseerimislepingutes tuleb sätestada, et sertifitseerimiskavast või muudest eeskirjadest tulenevatest tähtaegadest ja menetlustest tuleb kinni pidada;
6. sertifitseerimislepingutes sätestatakse seoses standardi ISO/IEC 17065/2012 jaotisega 4.1.2.2 lit. c nr 1 kehtivust, pikendamist ja tagasivõtmist käsitlevad eeskirjad kooskõlas artikli 42 lõikega 7 ja artikli 43 lõikega 4, sealhulgas eeskirjad, millega

määratakse kindlaks uuesti hindamise või läbivaatamise sagedus (korrapärasus) kooskõlas artikli 42 lõikega 7;

7. sertifitseerimislepingud võimaldavad sertifitseerimisasutusel avalikustada kogu teabe, mis on vajalik sertifikaadi andmiseks, kooskõlas artikli 42 lõikega 8 ja artikli 43 lõikega 5;
8. sertifitseerimislepingud sisaldavad eeskirju, mis käsitlevad vajalikke ettevaatusabinõusid, et uurida kaebusi jaotise 4.1.2.2 lit. c nr 2 tähenduses, lisaks tuleb jaotises 4.1.2.2 lit. j sõnaselgelt kirjeldada artikli 43 lõike 2 punkti d kohast kaebuste käsitlemise struktuuri ja menetlust;
9. lisaks standardi ISO/IEC 17065/2012 jaotises 4.1.2.2 osutatud miinimumnõuetele, kui sertifitseerimisasutuse akrediteerimise tühistamisel või peatamisel on tagajärjed kliendile, tuleks vaadelda ka neid tagajärgi;
10. sertifitseerimislepingutes nähakse ette, et taotleja peab teavitama sertifitseerimisasutust, kui tema tegelik või õiguslik olukord või tema sertifitseerimisega seotud tooted, protsessid ja teenused märkimisväärselt muutuvad.

4.1.3 Andmekaitsepitserite ja -märgiste kasutamine

Sertifikaate, pitsereid ja märgiseid tuleb kasutada üksnes kooskõlas artiklitega 42 ja 43 ning akrediteerimist ja sertifitseerimist käsitlevate suunistega.

4.2 Erapooletus

Akrediteerimisasutus tagab, et lisaks standardi ISO/IEC 17065/2012 jaotises 4.2 sätestatud nõude täitmisele

1. vastab sertifitseerimisasutus pädeva järelevalveasutuse kehtestatud täiendavatele nõuetele (artikli 43 lõike 1 punkti b kohaselt)
    a. ja esitab kooskõlas artikli 43 lõike 2 punktiga a eraldi tõendi oma sõltumatuse kohta. Erapooletuse kinnitamiseks tuleb esitada tõend eelkõige sertifitseerimisasutuse rahastamise kohta,
    b. ning tema ülesanded ja kohustused ei põhjusta artikli 43 lõike 2 punktis e osutatud huvide konflikti;
2. puudub sertifitseerimisasutusel hinnatava kliendiga oluline seos.

4.3 Vastutus ja rahastamine

Lisaks standardi ISO/IEC 17065/2012 jaotises 4.3.1 sätestatud nõude täitmisele tagab akrediteerimisasutus, et sertifitseerimisasutusel on asjakohased meetmed (nt kindlustus või reservid), mis katavad tema kohustused geograafilises piirkonnas, kus ta tegutseb.

4.4 Mittediskrimineerivad tingimused

Järelevalveasutus võib sõnastada kooskõlas siseriikliku õigusega täiendavad nõuded.

4.5 Konfidentsiaalsus

Järelevalveasutus võib sõnastada kooskõlas siseriikliku õigusega täiendavad nõuded.

4.6 Avalikult kättesaadav teave

Lisaks standardi ISO/IEC 17065/2012 jaotises 4.6 sätestatud nõude täitmisele nõuab akrediteerimisasutus sertifitseerimisasutuselt vähemalt

1. artikli 42 lõike 5 tähenduses kasutatavate heakskiidetud kriteeriumide kõikide versioonide (praeguste ja varasemate) ning sertifitseerimismenetluste avaldamist ja avalikkusele hõlpsasti kättesaadavaks tegemist, nimetades üldjuhul nende kehtivusaja;

2. kaebuste käsitlemise korraga ja edasikaebustega seotud teabe avalikustamist kooskõlas artikli 43 lõike 2 punktiga d.

5 STRUKTUURINÕUDED, ARTIKLI 43 LÕIGE 4 [„NÕUETEKOHANE“ HINDAMINE]

5.1 Organisatsiooniline struktuur ja kõrgem juhtkond

Järelevalveasutus võib sõnastada täiendavad nõuded.

5.2 Erapooletuse tagamise mehhanism

Järelevalveasutus võib sõnastada täiendavad nõuded.

6 VAHENDITEGA SEOTUD NÕUDED

6.1 Asutuse töötajate sertifitseerimine

Lisaks standardi ISO/IEC 17065/2012 jaotises 6 sätestatud nõude täitmisele peab akrediteerimisasutus tagama, et sertifitseerimisasutuse töötajad

1. on tõendanud, et neil on kooskõlas artikli 43 lõikega 1 andmekaitse vallas asjakohased ja värskendatud eksperditeadmised (ja kogemused);
2. on sõltumatud ja omavad kooskõlas artikli 43 lõike 2 punktiga a eksperditeadmisi sertifitseerimise objekti osas ning neil ei teki artikli 43 lõike 2 punktis e osutatud huvide konflikti;
3. on võtnud endale kooskõlas artikli 43 lõike 2 punktiga b kohustuse järgida artikli 42 lõikes 5 osutatud kriteeriume;
4. omavad asjakohaseid ja piisavaid teadmisi ja kogemusi andmekaitsealaste õigusaktide kohaldamise vallas;
5. omavad asjakohaseid ja piisavaid teadmisi ja kogemusi tehniliste ja korralduslike andmekaitsemeetmete vallas;
6. on võimelised tõendama kogemusi täiendavates nõuetes 6.1.1 ja 6.1.4 ning eriti täiendavas nõudes 6.1.5 nimetatud valdkondades.

Tehnilisi eksperditeadmisi omavate isikute puhul on nõutav järgmine.

- Isik peab olema omandanud valdkonnas, kus tal on tehnilised eksperditeadmised, vähemalt Euroopa kvalifikatsiooniraamistiku[20] 6. astme kvalifikatsiooni, saanud asjaomasel reguleeritud kutsealal tunnustatud kaitstud kutsenimetuse (nt Dipl. Ing.) või omama märkimisväärset kutsealast töökogemust.
- *Sertifitseerimisotsuste eest vastutaval töötajal* peab olema märkimisväärne kutsealane töökogemus andmekaitsemeetmete kindlaksmääramise ja rakendamise vallas.
- *Hindamise eest vastutaval töötajal* peavad olema tehnilised eksperditeadmised tehnilise andmekaitse vallas ning teadmised ja kogemused seoses asjakohaste menetlustega (sertifitseerimine, auditid jne); vajaduse korral peab ta olema registreeritud.

[20] Vt kvalifikatsiooniraamistiku võrdlusvahend aadressil https://ec.europa.eu/ploteus/en/compare?.

Töötaja peab tõendama, et ta säilitab valdkonnapõhised tehnilised ja auditeerimisoskused end pidevalt ametialaselt arendades.

Õigusalaseid eksperditeadmisi omavate isikute puhul on nõutav järgmine.

- Isik peab olema läbinud ELi või riigi tunnustatud ülikoolis vähemalt kaheksa semestrit kestnud õigusalased õpingud, mille tulemusel on omandatud magistrikraad või muu samaväärne kraad, või omama märkimisväärset kutsealast töökogemust.
- *Sertifitseerimisotsuste eest vastutav töötaja* peab tõendama, et tal on märkimisväärne kutsealane töökogemus andmekaitseõiguse vallas, ja ta peab olema liikmesriigi nõudmisel registreeritud.
- *Hindamise eest vastutav töötaja* peab tõendama vähemalt kaheaastast kutsealast töökogemust andmekaitseõiguse vallas, tal peavad olema teadmised ja kogemused seoses asjakohaste menetlustega (sertifitseerimine, auditid jne) ning ta peab olema registreeritud, kui liikmesriik seda nõuab.
    - Töötaja peab tõendama, et ta säilitab valdkonnapõhised tehnilised ja auditeerimisoskused end pidevalt ametialaselt arendades.

6.2 Vahendite hindamine

Järelevalveasutus võib sõnastada kooskõlas siseriikliku õigusega täiendavad nõuded.

7 PROTSESSI KÄSITLEVAD NÕUDED, ARTIKLI 43 LÕIKE 2 PUNKTID C JA D

7.1 Üldist

Lisaks standardi ISO/IEC 17065/2012 jaotises 7.1 sätestatud nõude täitmisele peab akrediteerimisasutus tagama järgmise:

1. sertifitseerimisasutused vastavad taotluse esitamisel pädeva järelevalveasutuse kehtestatud täiendavatele nõuetele (vastavalt artikli 43 lõike 1 punktile b), et ülesanded ja kohustused ei põhjustaks artikli 43 lõike 2 punktis e osutatud huvide konflikti;
2. asjakohast pädevat järelevalveasutust teavitatakse, enne kui sertifitseerimisasutus hakkab juhtima heakskiidetud Euroopa andmekaitsepitseri kasutamist uues liikmesriigis harukontorist.

7.2 Kohaldamine

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.2 järgimisele tuleks ette näha, et

1. taotluses tuleb üksikasjalikult kirjeldada sertifitseerimise (hindamise) objekti. Muu hulgas tuleb kirjeldada seoseid muude süsteemide, organisatsioonide, protokollide ja kinnitustega;
2. taotluses peab olema märgitud, kas kasutatakse volitatud töötlejaid, ning kui volitatud töötleja on taotluse esitaja, tuleb kirjeldada tema kohustusi ja ülesandeid, samuti peab taotlus sisaldama asjakohast (asjakohaseid) vastutava töötleja ja volitatud töötleja lepingut (lepinguid).

7.3 Taotluse läbivaatamine

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.3 järgimisele tuleks ette näha, et

1. sertifitseerimislepingus tuleb sätestada hindamise objekti puhul rakendatavad siduvad hindamismeetodid;

2. hinnates jaotise 7.3.e kohaselt piisavate eksperditeadmiste olemasolu, tuleb võtta asjakohasel määral arvesse nii tehnilisi kui ka õigusalaseid eksperditeadmisi andmekaitse vallas.

7.4 Hindamine

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.4 järgimisele tuleb sertifitseerimismehhanismides kirjeldada piisavaid hindamismeetodeid, mida kasutatakse selleks, et hinnata isikuandmete töötlemise toimingu(te) vastavust sertifitseerimiskriteeriumidele, sealhulgas vajaduse korral

1. meetodit, mida rakendades hinnatakse töötlemistoimingute vajalikkust ja proportsionaalsust töötlemise eesmärgi ja asjaomaste andmesubjektide vaatenurgast;
2. meetodit, mida rakendades antakse hinnang kõikide vastutava töötleja ja volitatud töötleja kindlaks tehtud riskide ulatuse, komponentide ja hindamise kohta, võttes arvesse õiguslikke tagajärgi vastavalt isikuandmete kaitse üldmääruse artiklitele 30, 32, 35 ja 36 ning tehniliste ja korralduslike meetmete määratlust vastavalt kõnealuse määruse artiklitele 24, 25 ja 32, kui nimetatud artikleid kohaldatakse sertifitseerimise objekti suhtes;
3. meetodit, mida rakendades hinnatakse õiguskaitsevahendeid, sealhulgas tagatisi, kaitsemeetmeid ja menetlusi, millega tagatakse sertifitseerimise objektiga seostataval isikuandmete töötlemisel isikuandmete kaitse ning tõendatakse, et kriteeriumides sätestatud õiguslikud nõuded on täidetud, ning
4. meetodite ja järelduste dokumenteerimist.

Sertifitseerimisasutuselt tuleks nõuda selle tagamist, et kõnealused hindamismeetodid on standardsed ja üldiselt kohaldatavad. See tähendab, et võrreldavate hindamise objektide puhul kasutatakse võrreldavaid hindamismeetodeid. Sertifitseerimisasutusel tuleb põhjendada mis tahes kõrvalekaldumist sellest menetlusest.

Standardi ISO/IEC 17065/2012 jaotise 7.4.2 järgimise kõrval peaks olema lubatud, et hindamise teevad sertifitseerimisasutuse tunnustatud väliseksperdid.

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.4.5 järgimisele tuleks ette näha, et sertifitseerimisel võib arvesse võtta andmekaitse sertifitseerimist kooskõlas isikuandmete kaitse üldmääruse artiklitega 42 ja 43, mis juba hõlmab osa sertifitseerimise objektist. See ei ole siiski piisav, et täielikult asendada (osalist) hindamist. Sertifitseerimisasutus on kohustatud kontrollima vastavust kriteeriumidele. Tunnustamiseks on igal juhul vaja, et oleks kättesaadav täielik hindamisaruanne või teave, mis võimaldab hinnata varasemat sertifitseerimist ja selle tulemusi. Sertifitseerimist käsitlevat avaldust või sarnast sertifitseerimistõendit ei tohiks pidada aruande asendamiseks piisavaks.

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.4.6 järgimisele tuleks ette näha, et sertifitseerimisasutus peab kirjeldama oma sertifitseerimismehhanismis üksikasjalikult seda, kuidas jaotises 7.4.6 nõutava teabe esitamisega teavitatakse klienti (sertifitseerimise taotlejat) sertifitseerimismehhanismi rakendamisel avastatud mittevastavusest. Selles kontekstis tuleks määrata kindlaks vähemalt sellise teabe laad ja esitamise aeg.

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.4.9 järgimisele tuleks ette näha, et dokumendid tuleb teha taotluse korral andmekaitse järelevalveasutusele täielikult ligipääsetavaks.

7.5 Läbivaatamine

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.5 järgimisele on vaja menetlusi sertifikaatide andmiseks, korrapäraseks läbivaatamiseks ja tagasivõtmiseks kooskõlas artikli 43 lõigetega 2 j 3.

7.6 Sertifitseerimisotsus

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.6.1 järgimisele tuleks ette näha, et sertifitseerimisasutus peab kirjeldama oma menetlustes üksikasjalikult seda, kuidas on tagatud tema sõltumatus ja vastutus konkreetsete sertifitseerimisotsuste tegemisel.

7.7 Sertifitseerimisdokumendid

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.7.1.e järgimisele ja kooskõlas isikuandmete kaitse üldmääruse artikli 42 lõikega 7 tuleks ette näha, et sertifikaatide kehtivusaeg ei tohi ületada kolme aastat.

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.7.1.e järgimisele tuleks ette näha, et dokumenteerida tuleb ka kavandatud järelevalveperiood punkti 7.9 tähenduses.

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.7.1.f järgimisele tuleks ette näha, et sertifitseerimisasutus peab nimetama sertifitseerimisdokumentides sertifitseerimise objekti (märkides vajaduse korral ära versiooni staatuse või muud sarnased omadused).

7.8 Sertifitseeritud toodete kataloog

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.8 järgimisele tuleks ette näha, et sertifitseerimisasutus peab hoidma sertifitseeritud tooteid, protsesse ja teenused käsitleva teabe asutusesiseselt ja avalikkusele kättesaadavana. Sertifitseerimisasutus esitab avalikkusele hindamisaruande kokkuvõtte. Selle kokkuvõtte eesmärk on suurendada läbipaistvust küsimustes, mida on sertifitseeritud ja kuidas seda hinnati. Selles selgitatakse

(a) sertifitseerimise ulatust ja kirjeldatakse sisukalt sertifitseerimise objekti;

(b) vastavaid sertifitseerimiskriteeriume (sh versioon või funktsionaalne staatus);

(c) hindamismeetodeid ja tehtud kontrolle ning

(d) tulemust (tulemusi).

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.8 järgimisele ja kooskõlas isikuandmete kaitse üldmääruse artikli 43 lõikega 5 peab sertifitseerimisasutus teatama pädevale järelevalveasutusele taotletud sertifikaadi väljastamise või sertifikaadi tagasivõtmise põhjused.

7.9 Järelevalve

Lisaks standardi ISO/IEC 17065/2012 jaotiste 7.9.1, 7.9.2 ja 7.9.3 järgimisele ning kooskõlas isikuandmete kaitse üldmääruse artikli 43 lõike 2 punktiga c tuleks ette näha, et sertifikaadi säilitamiseks on järelevalveperioodil vaja korrapärase järelevalve meetmeid.

7.10 Sertifitseerimist mõjutavad muudatused

Lisaks standardi ISO/IEC 17065/2012 jaotistes 7.10.1 ja 7.10.2 sätestatule kuuluvad sertifitseerimist mõjutavate muudatuste hulka, mida sertifitseerimisasutus peab arvesse võtma, andmekaitsealastesse õigusaktidesse tehtud muudatused, Euroopa Komisjoni delegeeritud õigusaktide vastuvõtmine kooskõlas artikli 43 lõigetega 8 ja 9, Euroopa andmekaitsenõukogu otsused ja andmekaitsealased kohtuotsused. Kokkulepitavad muudatustega seotud menetlused võivad hõlmata üleminekuperioode, pädevalt järelevalveasutuselt heakskiidu saamist, asjakohase sertifitseerimise objekti uuesti hindamist ja asjakohaseid meetmeid sertifikaadi tühistamiseks, kui sertifitseeritud töötlemistoiming ei vasta ajakohastatud kriteeriumidele.

7.11 Sertifikaadi lõppemine, piiramine, peatamine või tagasivõtmine

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.11.1 järgimisele tuleks ette näha, et vajaduse korral peab sertifitseerimisasutus viivitamata kirjalikult teavitama pädevat järelevalveasutust ja riiklikku akrediteerimisasutust sertifikaadi pikendamisest, piiramisest, peatamisest või tagasivõtmisest ning selleks võetud meetmetest.

Vastavalt artikli 58 lõike 2 punktile h peab sertifitseerimisasutus täitma pädeva järelevalveasutuse otsuse või korralduse võtta sertifikaat kliendilt tagasi või jätta sertifikaat taotlejale väljastamata, kui sertifitseerimise nõuded ei ole täidetud või ei ole enam täidetud.

7.12 Andmete säilitamine

Sertifitseerimisasutus peaks olema kohustatud hoidma kõik dokumendid täielikud, arusaadavad, ajakohased ja auditeerimiskõlblikud.

7.13 Kaebused ja edasikaebused, artikli 43 lõike 2 punkt d

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.13.1 järgimisele tuleks ette näha, et sertifitseerimisasutus peab kindlaks määrama

(a) kes saab esitada kaebusi või vastuväiteid,

(b) kes need sertifitseerimisasutuse nimel läbi vaatab,

(c) mida selle käigus kontrollitakse ja

(d) võimalused konsulteerida huvitatud isikutega.

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.13.2 järgimisele tuleks ette näha, et sertifitseerimisasutus peab kindlaks määrama

(a) kuidas ja kellele tuleb sellist teavet anda,

(b) teabe esitamise tähtajad ning

(c) hiljem algatatavad protsessid.

Lisaks standardi ISO/IEC 17065/2012 jaotise 7.13.1 järgimisele peab sertifitseerimisasutus kindlaks määrama, kuidas hoitakse lahus sertifitseerimistegevus ning kaebuste ja edasikaebuste käsitlemine.

8 JUHTIMISSÜSTEEMI KÄSITLEVAD NÕUDED

Standardi ISO/IEC 17065/2012 jaotises 8 sätestatud üldise juhtimissüsteemi käsitleva nõude kohaselt tuleb seda, kuidas akrediteeritud sertifitseerimisasutus rakendab sertifitseerimismehhanismi kohaldamisel kõiki eelmistes jaotistes nimetatud nõudeid, dokumenteerida, hinnata, kontrollida ja jälgida sõltumatult.

Juhtimise aluspõhimõte on määrata sobivate kirjelduste abil kindlaks süsteem, mis võimaldab püstitada tõhusalt ja tulemuslikult eesmärke, eelkõige rakendada sertifitseerimisteenuseid. Selleks on vaja, et sertifitseerimisasutus rakendaks akrediteerimise nõudeid läbipaistval ja kontrollitaval viisil ning alati nõuetekohaselt.

Sellega seoses tuleb juhtimissüsteemis kindlaks määrata metoodika, et saavutada kõnealuste nõuete täitmine ja kontrollida nende täitmist kooskõlas andmekaitse-eeskirjadega ning võimaldamaks akrediteeritud asutusel endal neid nõudeid pidevalt kontrollida.

Kõnealused juhtimispõhimõtted ja nende dokumenteeritud rakendamine peavad olema läbipaistvad ning akrediteeritud sertifitseerimisasutus peab need avalikustama akrediteerimismenetluse käigus kooskõlas artikliga 58 ning seejärel andmekaitse järelevalveasutuse taotlusel ükskõik millal artikli 58

lõike 1 punkti b kohase andmekaitsealase läbivaatamise vormis läbiviidava uurimise käigus või artikli 58 lõike 1 punkti c kohasel artikli 42 lõike 7 alusel väljastatud sertifikaatide läbivaatamisel.

Eelkõige peab akrediteeritud sertifitseerimisasutus avalikustama pidevalt ja püsivalt selle, milline sertifitseerimine on toimunud millistel alustel (sertifitseerimismehhanismid või -kavad), samuti kui kaua ning millise raamistiku ja milliste tingimuste alusel sertifikaadid kehtivad (põhjendus 100).

8.1 Üldised juhtimissüsteemi käsitlevad nõuded

Pädev järelevalveasutus võib kooskõlas siseriikliku õigusega määrata kindlaks ja lisada veel täiendavaid nõudeid.

8.2 Juhtimissüsteemi dokumendid

Pädev järelevalveasutus võib kooskõlas siseriikliku õigusega määrata kindlaks ja lisada veel täiendavaid nõudeid.

8.3 Dokumentide kontroll

Pädev järelevalveasutus võib kooskõlas siseriikliku õigusega määrata kindlaks ja lisada veel täiendavaid nõudeid.

8.4 Andmehaldus

Pädev järelevalveasutus võib kooskõlas siseriikliku õigusega määrata kindlaks ja lisada veel täiendavaid nõudeid.

8.5 Juhtkonnapoolne läbivaatamine

Pädev järelevalveasutus võib kooskõlas siseriikliku õigusega määrata kindlaks ja lisada veel täiendavaid nõudeid.

8.6 Siseauditid

Pädev järelevalveasutus võib kooskõlas siseriikliku õigusega määrata kindlaks ja lisada veel täiendavaid nõudeid.

8.7 Parandusmeetmed

Pädev järelevalveasutus võib kooskõlas siseriikliku õigusega määrata kindlaks ja lisada veel täiendavaid nõudeid.

8.8 Ennetusmeetmed

Pädev järelevalveasutus võib kooskõlas siseriikliku õigusega määrata kindlaks ja lisada veel täiendavaid nõudeid.

9 MUUD TÄIENDAVAD NÕUDED[21]

9.1 Hindamismeetodite ajakohastamine

Sertifitseerimisasutus määrab kindlaks hindamismeetodite ajakohastamise menetluse, mida kohaldada punkti 7.4 kohasel hindamisel. Ajakohastamine peab toimuma juhul, kui tehakse muudatusi õigusraamistikku, muutuvad asjakohased riskid, muutub tehnika tase või muutuvad tehniliste ja korralduslike meetmete rakendamise kulud.

[21] Pädev järelevalveasutus võib kooskõlas siseriikliku õigusega määrata kindlaks ja lisada veel täiendavaid nõudeid.

9.2 Pädevuse säilitamine

Sertifitseerimisasutused kehtestavad menetluse, et tagada oma töötajate koolitamine eesmärgiga ajakohastada nende oskusi, võttes arvesse punktis 9.1 osutatud muutusi.

9.3 Kohustused ja pädevus

9.3.1 Sertifitseerimisasutuse ja sertifitseerimisasutuse klientide vaheline teabevahetus

Tuleb kehtestada kord asjakohaste menetluste ja teabevahetusstruktuuride rakendamiseks sertifitseerimisasutuse ja sertifitseerimisasutuse klientide vahel. See hõlmab

1. akrediteeritud sertifitseerimisasutuse poolset ülesandeid ja kohustusi käsitlevate dokumentide säilitamist, juhuks kui esitatakse
    a. teabenõue või
    b. sertifitseerimist käsitlev kaebus;
2. taotlemisprotsessi käsitlevate dokumentide säilitamist, juhuks kui
    a. soovitakse teavet taotluse staatuse kohta,
    b. pädev järelevalveasutus kavatseb korraldada hindamise seoses
        i. tagasisidega,
        ii. enda tehtud otsustega.

9.3.2 Hindamise dokumenteerimine

Järelevalveasutus võib sõnastada täiendavad nõuded.

9.3.3 Kaebuste käsitlemine

Kaebuste käsitlemine on juhtimissüsteemi lahutamatu osa ning selle puhul rakendatakse eelkõige standardi ISO/IEC 17065/2012 jaotistes 4.1.2.2 lit. c, 4.1.2.2 lit. j, 4.6 lit. d ja 7.13 sätestatud nõudeid.

Asjakohaseid kaebusi ja vastuväiteid tuleks jagada pädeva järelevalveasutusega.

9.3.4 Tühistamise käsitlemine

Akrediteerimise peatamise või tühistamise korral rakendatavad menetlused, mis hõlmavad klientide teavitamist, lõimitakse sertifitseerimisasutuse juhtimissüsteemi.