Suunised

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

Vastu võetud 4. detsembril 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,

ON VASTU VÕTNUD JÄRGMISED SUUNISED.

1 SISSEJUHATUS

25. mail 2018 jõustunud isikuandmete kaitse üldmääruses (määrus (EL) 2016/679) on sätestatud vastutusel ja põhiõigustel põhinev ajakohastatud vastavusraamistik seoses isikuandmete kaitsega Euroopas. Uue raamistiku keskmes on mitmesugused meetmed, mis aitavad tagada vastavust isikuandmete kaitse üldmääruse sätetele. Need hõlmavad teatud olukordades rakendatavaid kohustuslikke nõudeid (sh andmekaitseametnike määramine ja andmekaitse mõjuhinnangute tegemine) ning vabatahtlikke meetmeid, näiteks toimimisjuhendid ja sertifitseerimismehhanismid.

Vastavalt isikuandmete kaitse üldmääruse artikli 43 lõikele 1 peavad liikmesriigid sertifitseerimismehhanismide ning andmekaitsepitserite ja -märgiste kasutuselevõtu osana kehtestama, 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.

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]

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.

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.

[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.

2 SUUNISTE KOHALDAMISALA

Käesolevates suunistes

- sätestatakse akrediteerimise eesmärk isikuandmete kaitse üldmääruse kontekstis;
- selgitatakse sertifitseerimisasutuste akrediteerimise eri võimalusi vastavalt artikli 43 lõikele 1 ja tuvastatakse arutatavad põhiküsimused;
- esitatakse täiendavate akrediteerimisnõuete kehtestamise raamistik juhuks, kui akrediteerib riiklik akrediteerimisasutus, ja
- esitatakse akrediteerimisnõuete kehtestamise raamistik juhuks, kui akrediteerib järelevalveasutus.

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

Suunised on adresseeritud

- liikmesriikidele, kes peavad kehtestama, 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].

Mõisted

Järgmiste määratluste eesmärk on edendada akrediteerimisprotsessi põhielementide ühist mõistmist. Määratlusi tuleb käsitada võrdlusalusena ja need võivad ajas muutuda. Määratlused põhinevad

[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 mida ta omab, kuid on võimalikud ka olukorrad, kus süsteemi omab üks organisatsioon ja hindab teine (hindavad teised).

olemasolevatel õigusraamistikel ja standarditel, eelkõige isikuandmete kaitse üldmääruse ja standardi ISO/IEC 17065/2012 asjakohastel sätetel.

Suunistes kasutatakse järgmisi mõisteid:

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

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

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

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

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

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

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

3 AKREDITEERIMISE TÕLGENDAMINE ISIKUANDMETE KAITSE ÜLDMÄÄRUSE ARTIKLI 43 KOHALDAMISEL

Isikuandmete kaitse üldmääruses ei ole akrediteerimist määratletud. Akrediteerimise üldnõudeid sätestava määruse (EÜ) nr 765/2008 artikli 2 punktis 10 on akrediteerimine määratletud järgmiselt:

„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“.

---

[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.

Standardis ISO/IEC 17011 on sätestatud:

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

Artikli 43 lõikes 1 on sätestatud:

„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 ekspertteadmised, olles enne järelevalveasutust teavitanud, et see saaks vajaduse korral kasutada oma volitusi vastavalt artikli 58 lõike 2 punktile h. Liikmesriik kehtestab, kas need sertifitseerimisasutused 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 EN-ISO/IEC 17065/2012 ning artiklite 55 või 56 kohaselt pädeva järelevalveasutuse kehtestatud täiendavate nõuete kohaselt nimetatud riiklik akrediteerimisasutus.“

Isikuandmete kaitse üldmääruse kohaldamisel juhinduvad akrediteerimisnõuded

- 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.

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

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

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

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.

[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 20.
[14] Vt seoses termini „akrediteerimine“ määratlusega vastavalt standardile ISO 17011.

4.1 Liikmesriikide roll

Artikli 43 lõikes 1 nõutakse liikmesriikidelt *kehtestamist*, 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).

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

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“.

Artikli 2 punkti 11 võib pidada vastuolus olevaks isikuandmete kaitse üldmääruse artikli 43 lõikega 1, mille kohaselt võib akrediteerida muu asutus kui liikmesriigi riiklik akrediteerimisasutus. Euroopa Andmekaitsenõukogu leiab, et Euroopa Liidu õigusakti kavatsus oli teha erand üldpõhimõttest, et 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

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.

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

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

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

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

pädev järelevalveasutus, peab akrediteerimist taotlev sertifitseerimisasutus vastama asjaomase järelevalveasutuse kehtestatud nõuetele.

4.4 Järelevalveasutuse roll

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 ekspertteadmisi järelevalveasutuse pakutava sertifitseerimise sisu osas.[16]

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 järjekindlust.

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 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 ekspertteadmiste 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

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

[17] Isikuandmete kaitse üldmääruse artikli 1 lõige 2.

järelevalveasutustele kasulikku teavet, kui nad kehtestavad täiendavaid nõudeid vastavalt artikli 43 lõike 1 punktile b ja lõikele 3.

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 suhtes oleva usalduse nimel on soovitatav, et kõik akrediteerimisnõuded oleksid üldsusele lihtsalt kättesaadavad.

4.5 Sertifitseerimisasutusena tegutsev järelevalveasutus

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 teha mõlemat, akrediteerida ja sertifitseerida, ning ühtlasi anda nõu ja vajaduse korral võtta sertifikaat tagasi või anda sertifitseerimisasutustele korraldus jätta sertifikaat väljastamata.

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 organisatsioonimeetmed 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

Suuniste lisas on juhised, kuidas tuvastada täiendavaid akrediteerimisnõudeid. Selles tuvastatakse isikuandmete kaitse üldmääruse asjakohased sätted ja soovitatakse nõudeid, mida järelevalveasutused ja riiklikud akrediteerimisasutused peaksid kaalutlema, et tagada vastavus isikuandmete kaitse üldmäärusele.

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 kajastab artikli 43 lõige 2 standardi ISO/IEC 17065/2012 üldsätteid. Lisas olev raamistik tuvastab artikli 43 lõike 2 ja standardi ISO/IEC 17065/2012 alusel nõuded ja täiendavad kriteeriumid, millega hinnata sertifitseerimisasutuste andmekaitse ekspertteadmisi ning nende suutlikkust järgida füüsiliste isikute õigusi ja vabadusi isikuandmete töötlemisel vastavalt isikuandmete kaitse üldmäärusele. Euroopa Andmekaitsenõukogu märgib, et on eriti keskendunud tagamisele, et sertifitseerimisasutustel oleksid asjakohasel tasemel andmekaitse ekspertteadmised kooskõlas artikli 43 lõikega 1.

Järelevalveasutuse kehtestatud täiendavaid akrediteerimisnõudeid kohaldatakse kõigi akrediteerimist taotlevate sertifitseerimisasutuste suhtes. Akrediteerimisasutus hindab, kas sertifitseerimisasutus on pädev sertifitseerima kooskõlas täiendavate nõuetega ja sertifitseerimise sisuga. Täpsustada tuleb

konkreetsed sertifitseerimissektorid või -valdkonnad, mille suhtes sertifitseerimisasutus akrediteeritakse.

Ühtlasi märgib Euroopa Andmekaitsenõukogu, et andmekaitse ekspertteadmisi nõutakse lisaks standardi ISO/IEC 17065/2012 nõuetele ka siis, kui teised välisasutused, näiteks laborid või audiitorid, teostavad akrediteeritud sertifitseerimisasutuse nimel sertifitseerimisprotsessi teatud osi või elemente. Sellistel juhtudel ei ole nende välisasutuste akrediteerimine kooskõlas isikuandmete kaitse üldmäärusega võimalik. Et tagada nende asutuste sobivus tegevuseks, mida nad teevad akrediteeritud sertifitseerimisasutuse nimel, peab akrediteeritud sertifitseerimisasutus siiski tagama, et välisasutusel on alati akrediteeritud asutuselt nõutavad andmekaitse ekspertteadmised, ja tõendab nende olemasolu seoses asjaomase tehtava toiminguga.

Suuniste lisas olev täiendavate akrediteerimisnõuete tuvastamise raamistik ei ole riikliku akrediteerimisasutuse või järelevalveasutuse tehtava akrediteerimisprotsessi menetlusjuhend. Selles on struktuuri- ja metoodikajuhised ning see pakub seega järelevalveasutustele abivahendeid täiendavate akrediteerimisnõuete tuvastamisel.

Euroopa Andmekaitsenõukogu nimel

(Andrea Jelinek)

eesistuja