Andmekaitsenõukogu arvamus (art 64)

Arvamus 14/2020, mis käsitleb Iirimaa pädeva järelevalveasutuse otsuse eelnõu sertifitseerimisasutuse akrediteerimise nõuete heakskiitmise kohta kooskõlas isikuandmete kaitse üldmääruse artikli 43 lõikega 3

Vastu võetud 25. mail 2020

Vastu võetud

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 (edaspidi „isikuandmete kaitse üldmäärus“)) artiklit 63, artikli 64 lõike 1 punkti c ja lõikeid 3–8 ning artikli 43 lõiget 3,

võttes arvesse EMP lepingut, eriti selle XI lisa ja protokolli nr 37, mida on muudetud EMP ühiskomitee 6. juuli 2018. aasta otsusega nr 154/2018[1],

võttes arvesse 25. mai 2018. aasta kodukorra artikleid 10 ja 22,

ning arvestades järgmist:

1) Euroopa Andmekaitsenõukogu põhiülesanne on tagada määruse 2016/679 (edaspidi „isikuandmete kaitse üldmäärus“) järjepidev kohaldamine kogu Euroopa Majanduspiirkonnas. Kooskõlas isikuandmete kaitse üldmääruse artikli 64 lõikega 1 esitab andmekaitsenõukogu arvamuse, kui järelevalveasutus kavatseb heaks kiita nõuded artikli 43 kohaseks sertifitseerimisasutuse akrediteerimiseks. Käesoleva arvamuse eesmärk on seega tagada ühtne lähenemine nõuete osas, mida andmekaitse järelevalveasutus või riiklik akrediteerimisasutus kohaldab sertifitseerimisasutuse akrediteerimisel. Ehkki isikuandmete kaitse üldmäärusega ei ole kehtestatud ühtseid akrediteerimisnõudeid, edendatakse sellega järjepidevust. Andmekaitsenõukogu püüab oma arvamustes seda eesmärki saavutada esiteks sellega, et innustab järelevalveasutusi järgima akrediteerimisnõuete koostamisel Euroopa Andmekaitsenõukogu sertifitseerimisasutuste akrediteerimise suuniste 4/2018 lisas 1 esitatud ülesehitust, ning teiseks sellega, et analüüsib neid andmekaitsenõukogu malli põhjal, mis võimaldab nõudeid võrrelda (põhineb standardil ISO 17065 ja Euroopa Andmekaitsenõukogu sertifitseerimisasutuste akrediteerimise suunistel).

2) Kooskõlas isikuandmete kaitse üldmääruse artikliga 43 võtavad pädevad järelevalveasutused vastu akrediteerimisnõuded. Seejuures kohaldavad nad järjepidevuse mehhanismi, et tekitada usaldust sertifitseerimismehhanismi vastu, eelkõige kehtestades ranged nõuded.

3) Ehkki akrediteerimisnõuete suhtes kohaldatakse järjepidevuse mehhanismi, ei tähenda see, et nõuded peaksid olema ühesugused. Pädevatel järelevalveasutustel on vabadus võtta arvesse riiklikku ja piirkondlikku konteksti ning nad peaksid silmas pidama kohalikke õigusakte. Andmekaitsenõukogu arvamuse eesmärk ei ole ühtsete ELi nõuete kehtestamine, vaid pigem oluliste vastuolude vältimine, mis võivad näiteks vähendada usaldust akrediteeritud sertifitseerimisasutuste sõltumatuse või asjatundlikkuse vastu.

4) Järjepidevuse mehhanismi juhtpõhimõtted on suunised 4/2018 isikuandmete kaitse üldmääruse ((EL) 2016/679) artikli 43 kohase sertifitseerimisasutuste akrediteerimise kohta (edaspidi „suunised“) ning suunised 1/2018 määruse (EL) 2016/679 artiklite 42 ja 43 kohase sertifitseerimise ja sertifitseerimiskriteeriumide kindlaksmääramise kohta.

5) Kui liikmesriik sätestab, et sertifitseerimisasutused akrediteerib järelevalveasutus, peaks järelevalveasutus kehtestama akrediteerimisnõuded, mis hõlmavad isikuandmete kaitse üldmääruse

[1] Kõiki selle arvamuse viiteid liidule tuleb mõista kui viiteid EMP-le.

artikli 43 lõikes 2 sätestatud nõudeid, kuid ei ole nendega piiratud. Isikuandmete kaitse üldmääruse 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 akrediteerimisnõuded juhinduma standardist ISO/IEC 17065 ja neile peaksid lisanduma täiendavad nõuded, mille järelevalveasutus kehtestab kooskõlas isikuandmete kaitse üldmääruse artikli 43 lõike 1 punktiga b. Euroopa Andmekaitsenõukogu märgib, et artikli 43 lõike 2 punktides a–e kajastatakse ja täpsustatakse standardi ISO 17065 nõudeid, mis aitab suurendada järjepidevust.[2]

6) Euroopa Andmekaitsenõukogu arvamus võetakse vastu isikuandmete kaitse üldmääruse artikli 64 lõike 1 punkti c ning lõigete 3 ja 8 alusel kooskõlas andmekaitsenõukogu kodukorra artikli 10 lõikega 2 kaheksa nädala jooksul alates esimesest tööpäevast pärast seda, kui eesistuja ja pädev järelevalveasutus on otsustanud, et toimik on täielik. Eesistuja otsusel võib seda ajavahemikku pikendada veel kuue nädala võrra, võttes arvesse asja keerukust.

ON VASTU VÕTNUD JÄRGMISE ARVAMUSE:

1 ASJAOLUDE KOKKUVÕTE

1. Iiri järelevalveasutus esitas Euroopa Andmekaitsenõukogule kooskõlas artikli 43 lõike 1 punktiga b akrediteerimisnõuete eelnõu. Toimik loetud täielikuks 13.2.2020. Iiri riiklik akrediteerimisasutus INAB akrediteerib sertifitseerimisasutusi isikuandmete kaitse üldmääruses esitatud sertifitseerimiskriteeriumide alusel. See tähendab, et riiklik akrediteerimisasutus kasutab sertifitseerimisasutuste akrediteerimiseks standardit ISO 17065 ja järelevalveasutuse kehtestatud täiendavaid nõudeid, kui järelevalveasutus on need pärast andmekaitsenõukogult nõuete eelnõud käsitleva arvamuse saamist heaks kiitnud.

2. Kooskõlas andmekaitsenõukogu kodukorra artikli 10 lõikega 2 otsustas eesistuja küsimuse keerukuse tõttu pikendada esialgset kaheksa nädala pikkust vastuvõtmisperioodi kuue nädala võrra.

2 HINNANG

2.1 Euroopa Andmekaitsenõukogu üldine seisukoht esitatud otsuse eelnõu kohta

3. Selle arvamuse eesmärk on hinnata akrediteerimisnõudeid, mille järelevalveasutus on koostanud lisaks standardile ISO 17065 või tervikliku nõuetekogumina, et riiklik akrediteerimisasutus või järelevalveasutus saaks isikuandmete kaitse üldmääruse artikli 43 lõike 1 kohaselt akrediteerida sertifitseerimisasutuse, kelle ülesanne on kooskõlas sama määruse artikliga 42 sertifikaate väljastada ja uuendada. See ei piira pädeva järelevalveasutuse ülesandeid ega volitusi. Käesoleval juhul nendib andmekaitsenõukogu, et Iiri järelevalveasutus on otsustanud teha akrediteerimise oma riikliku

[2] Suunised 4/2018 isikuandmete kaitse üldmääruse artikli 43 kohase sertifitseerimisasutuste akrediteerimise kohta, p 39. Kättesaadav aadressil: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en.

akrediteerimisasutuse ülesandeks, olles koostanud vastavalt suunistele täiendavad nõuded, mida riiklik akrediteerimisasutus peaks akrediteerimisel kasutama.

4. Iiri järelevalveasutuse täiendavate akrediteerimisnõuete hindamise eesmärk on uurida, kuivõrd need nõuded erinevad suunistes ja eelkõige suuniste lisas 1 esitatust (sh täiendused või väljajätmised). Lisaks pööratakse andmekaitsenõukogu arvamuses tähelepanu kõigile aspektidele, mis võivad mõjutada ühtset lähenemist sertifitseerimisasutuste akrediteerimisele.

5. Tuleb märkida, et sertifitseerimisasutuste akrediteerimise suuniste eesmärk on aidata järelevalveasutusi akrediteerimisnõuete koostamisel. Suuniste lisas esitatud juhised ei ole iseenesest akrediteerimisnõuded. Seega peab järelevalveasutus koostama sertifitseerimisasutuste akrediteerimise nõuded selliselt, et neid oleks võimalik järelevalveasutuse konteksti silmas pidades praktiliselt ja järjekindlalt kohaldada.

6. Andmekaitsenõukogu tunnistab, et riiklike akrediteerimisasutuste asjatundlikkust arvestades tuleks neile kohaldatavate akrediteerimisnõuete raames teatavate erinõuete määratlemisel anda tegutsemisvabadust. Siiski peab andmekaitsenõukogu vajalikuks rõhutada, et täiendavate nõuete kehtestamisel tuleks need määratleda nii, et neid oleks võimalik praktikas järjepidevalt rakendada ja vajaduse korral läbi vaadata.

7. Andmekaitsenõukogu märgib, et ISO standarditele, eelkõige standardile ISO 17065 kehtib intellektuaalomandiõigus, mistõttu ei viita ta käesolevas arvamuses vastava dokumendi tekstile. Selle tulemusena otsustas andmekaitsenõukogu viidata asjakohasel juhul ISO standardi asjaomastele lõikudele nende teksti taas esitamata.

8. Andmekaitsenõukogu järgis hindamisel suuniste 1. lisas (edaspidi: lisa) esitatud ülesehitust. Kui arvamuses ei ole Iiri järelevalveasutuse akrediteerimisnõuete eelnõu konkreetse osa kohta midagi öeldud, tähendab see, et andmekaitsenõukogul ei ole selle osa kohta märkusi ning Iiri järelevalveasutusel ei ole tarvis lisameetmeid võtta.

9. Arvamuses ei käsitleta Iiri järelevalveasutuse esitatud teavet, mis jääb välja isikuandmete kaitse üldmääruse artikli 43 lõike 2 kohaldamisalast, näiteks viiteid riigisisestele õigusaktidele. Andmekaitsenõukogu märgib sellegipoolest, et riigisisesed õigusaktid peaksid, kui nõutud, olema kooskõlas isikuandmete kaitse üldmäärusega.

2.2 Hindamise põhipunktid (isikuandmete kaitse üldmääruse artikli 43 lõige 2 ja andmekaitsenõukogu suuniste 1. lisa), kas akrediteerimisnõuded tagavad järgmiste aspektide järjepideva hindamise:

1) suuniste lisas märgitud kõigi põhivaldkondade käsitlemine ja lisas hälbimise analüüsimine;

2) sertifitseerimisasutuse sõltumatus;

3) sertifitseerimisasutuse huvide konfliktid;

4) sertifitseerimisasutuse asjatundlikkus;

5) asjakohased kaitsemeetmed tagamaks, et sertifitseerimisasutus kohaldab isikuandmete kaitse üldmääruses sätestatud sertifitseerimiskriteeriume nõuetekohaselt;

6) isikuandmete kaitse üldmääruse kohase sertifikaadi väljastamise, korrapärase läbivaatamise ja tagasivõtmise menetlused, ning

7) sertifikaadi rikkumisi käsitlevate kaebuste läbipaistev menetlemine.

10. Võttes arvesse, et

a. isikuandmete kaitse üldmääruse artikli 43 lõikes 2 on esitatud loetelu akrediteerimisnõuetest, millele sertifitseerimisasutus peab akrediteerimise jaoks vastama;

b. isikuandmete kaitse üldmääruse artikli 43 lõike 3 kohaselt peab sertifitseerimisasutuste akrediteerimise nõuded heaks kiitma pädev järelevalveasutus;

c. isikuandmete kaitse üldmääruse artikli 57 lõike 1 punktides p ja q on sätestatud, et pädev järelevalveasutus koostab ja avaldab sertifitseerimisasutuste akrediteerimise nõuded ja võib otsustada sertifitseerimisasutused ise akrediteerida;

d. isikuandmete kaitse üldmääruse artikli 64 lõike 1 punkti c kohaselt peab andmekaitsenõukogu esitama arvamuse, kui järelevalveasutus kavatseb heaks kiita nõuded artikli 43 lõike 3 kohaseks sertifitseerimisasutuse akrediteerimiseks;

e. kui akrediteerimise teostab riiklik akrediteerimisasutus standardi ISO/IEC 17065/2012 alusel, tuleb täita ka pädeva järelevalveasutuse kehtestatud täiendavad nõuded;

f. sertifitseerimisasutuste akrediteerimise suuniste 1. lisas nähakse ette andmekaitse järelevalveasutuse koostatavad soovituslikud nõuded, mida riiklik akrediteerimisasutus kohaldab sertifitseerimisasutust akrediteerides,

leiab andmekaitsenõukogu järgmist.

2.2.1 ÜLDISED MÄRKUSED (Iiri järelevalveasutuse täiendavate akrediteerimisnõuete eelnõu jaotis 0)

11. Andmekaitsenõukogu tõdeb, et koostöötingimused, millega reguleeritakse riikliku akrediteerimisasutuse ja selle andmekaitse järelevalveasutuse suhteid, ei ole iseenesest sertifitseerimisasutuste akrediteerimise nõue. Kuid täielikkuse ja läbipaistvuse tagamiseks on andmekaitsenõukogu arvamusel, et kui sellised koostöötingimused on olemas, tuleb need avalikustada vormis, mida järelevalveasutus peab kohaseks.

2.2.2 MÕISTED JA MÄÄRATLUSED

12. Andmekaitsenõukogu märgib, et viidet „WP 261“ akrediteerimise suunistele ei ole värskendatud. Euroopa Andmekaitsenõukogu võttis vastu suunised 4/2018 isikuandmete kaitse üldmääruse (2016/679) artikli 43 kohase sertifitseerimisasutuste akrediteerimise kohta. Seepärast soovitab andmekaitsenõukogu Iiri järelevalveasutusel muuta sõnastust ja viidata suunistele 4/2018.

2.2.3 ÜLDISED MÄRKUSED

13. Andmekaitsenõukogu märgib, et Iiri järelevalveasutuse nõuete eelnõu viitab korduvalt „pädevale järelevalveasutusele“. Kuna pädev järelevalveasutus on antud juhul Iiri järelevalveasutus, soovitab andmekaitsenõukogu Iiri järelevalveasutusel asendada viide „andmekaitsekoordinaatori“ või „Iiri järelevalveasutusega“, et vältida segadust.

14. Andmekaitsenõukogu mõistab, et Iiri järelevalveasutuse nõuete eelnõu sisaldab terminite ja mõistete osa. Mõningaid termineid ei ole aga kasutatud järjepidevalt kogu dokumendis (nt „hindamisese“ ja „hindamistingimused“). Segaduse vältimiseks soovitab andmekaitsenõukogu Iiri järelevalveasutusel kasutad nõuete eelnõus termineid järjepidevalt.

2.2.4 ÜLDISED AKREDITEERIMISNÕUDED (akrediteerimisnõuete eelnõu jaotis 4)

15. Seoses Iiri järelevalveasutuse akrediteerimisnõuete eelnõu punktiga 4.1.2.7 leiab andmekaitsenõukogu, et sõnastus on pisut ebaselge seoses sellega, kellele esitatakse sertifitseerimise heakskiitmise põhjendused. Lisaks on ebaselge ka viide registri lihtsustamisele. Seetõttu soovitab andmekaitsenõukogu Iiri järelevalveasutusel muuta eelnõu sõnastus selgemaks.

2.2.5 STRUKTUURINÕUDED (akrediteerimisnõuete eelnõu jaotis 5)

16. Andmekaitsenõukogu märgib, et Iiri järelevalveasutuse akrediteerimisnõuete eelnõu sisaldab viidet sellise isiku ametisse nimetamisele, kes on „sobiva aja vastutanud andmekaitsenõuete järgimise ja teabehalduse järelevalve eest“. Viidet asjakohasele töökogemusele tuleks selgitada töökogemuse ja volituste ulatusele tuginedes. Selle isiku funktsioonid tunduvad sarnased andmekaitseametniku omadele. Andmekaitsenõukogu soovitab Iiri järelevalveasutusel selgelt määratleda selle isiku funktsioonid ja konkreetne töökogemus.

2.2.6 RESSURSSE KÄSITLEVAD NÕUDED (akrediteerimisnõuete eelnõu jaotis 6)

17. Seoses sertifitseerimisasutuse personaliga (punkt 6.1) märgib andmekaitsenõukogu, et nõuded otsuste tegemise eest vastutavale tehniliste teadmistega personalile hõlmavad vähemalt 5-aastast erialast töökogemust seoses sertifitseerimisesemega, samas kui hindamise eest vastutaval personalil peaks olema vähemalt 2-aastane erialane töökogemus. Otsuseid tegeval õigusteadmistega personalil peaks olema vähemalt 5-aastane erialane töökogemus, samas kui hindamise eest vastutaval õigusteadmistega personalil peaks olema vähemalt 2-aastane töökogemus. Andmekaitsenõukogu märgib, et otsuste tegemise eest vastutavalt personalilt ja hindamise eest vastutavalt personalilt nõutud minimaalse töökogemuse vahel on suur erinevus. Sellega seoses leiab andmekaitsenõukogu, et rõhk peaks olema oskusteabe erinevusel, mitte töökogemuse pikkusel. Andmekaitsenõukogu arvates peaks hindajatel olema kitsemad ja põhjalikumad teadmised ja kogemused tehniliste protseduuride vallas (nt auditid ja sertifitseerimine), samas kui otsustajatel peaks olema üldisemad ja põhjalikumad teadmised ja kogemused andmekaitse vallas. Seda silmas pidades soovitab andmekaitsenõukogu Iiri järelevalveasutusel panna rohkem rõhku hindajate ja otsustajate erinevatele sisulistele teadmistele ja/või kogemustele ning vähendada erinevust neilt oodatava töökogemuse osas.

2.2.7 MENETLUSNÕUDED (akrediteerimisnõuete eelnõu jaotis 7)

18. Seoses Iiri järelevalveasutuse akrediteerimisnõuete eelnõu punktiga 7.10 („Sertifitseerimist mõjutavad muudatused“) märgib andmekaitsenõukogu, et puudub viide kokkulepitavatele muutmisprotseduuridele vastavalt lisa punktile 7.10. Andmekaitsenõukogu soovitab Iiri järelevalveasutusel lisada selline viide ja mainida mõningaid protseduure, mis võidakse kehtestada (nt üleminekuperioodid, pädeva järelevalveasutuse heakskiidumenetlus jms). Lisaks leiab andmekaitsenõukogu, et muudatused tehnika tasemel on samuti olulised ja mõjutavad sertifitseerimist. Seepärast soovitab andmekaitsenõukogu Iiri järelevalveasutusel lisada see võimalus sertifitseerimist mõjutavate muudatuste nimekirja. Lõpetuseks toetab andmekaitsenõukogu isikuandmetega seotud rikkumiste ja isikuandmete kaitse üldmääruse rikkumiste lisamist sertifitseerimist mõjutada võivate muudatuste nimekirja. Selguse tagamiseks soovitab andmekaitsenõukogu Iiri järelevalveasutusel sätestada, et andmetega seotud rikkumisi või isikuandmete kaitse üldmääruse rikkumisi võetakse arvesse ulatuses, milles need on sertifitseerimisega seotud.

19. Seoses muudatustega, mis mõjutavad sertifitseerimist (Iiri järelevalveasutuse nõuete eelnõu punkt 7.10) ja iseäranis viienda taandega märgib andmekaitsenõukogu, et Iiri järelevalveasutus viitab „Euroopa Andmekaitsenõukogu kohaldatavatele siduvatele otsustele“ ja Euroopa Andmekaitsenõukogu kodukorra artiklile 39, mis sisaldab „kõiki Euroopa Andmekaitsenõukogu vastuvõetud lõplikke dokumente“. Et aga täpsustada, mida on mõeldud „Euroopa Andmekaitsenõukogu otsuste“ all, võiks Iiri järelevalveasutus viidet selgitada. Näiteks võiks osutada „Euroopa Andmekaitsenõukogu poolt vastuvõetud dokumentidele“.

20. Andmekaitsenõukogu märgib, et Iiri järelevalveasutuse nõuete eelnõu punkt 7.11 (sertifikaadi kehtetuks tunnistamine, kehtivuse piiramine, peatamine või tagasivõtmine) ei hõlma sertifitseerimisasutuse kohustust aktsepteerida Iiri järelevalveasutuse otsuseid ja korraldusi võtta tagasi või mitte väljastada sertifikaati taotlejale, kui sertifitseerimisnõuded ei ole täidetud või kui need ei ole enam täidetud. Seepärast soovitab andmekaitsenõukogu Iiri järelevalveasutusel see kohustus lisada.

3 JÄRELDUSED/SOOVITUSED

21. Iiri järelevalveasutuse eelnõus sätestatud akrediteerimisnõuded võivad põhjustada järjekindlusetust sertifitseerimisasutuste akrediteerimisel ja seetõttu tuleb teha järgmised muudatused.

22. seoses menetlusnõuetega soovitab andmekaitsenõukogu Iiri järelevalveasutusel:

1) lisada punkti 7.11 sertifitseerimisasutuse kohustus aktsepteerida Iiri järelevalveasutuse otsuseid ja korraldusi võtta tagasi või mitte väljastada sertifikaati taotlejale, kui sertifitseerimisnõuded ei ole täidetud või kui need ei ole enam täidetud.

4 LÕPPMÄRKUSED

23. See arvamus on suunatud Iiri järelevalveasutusele ja see avalikustatakse isikuandmete kaitse üldmääruse artikli 64 lõike 5 punkti b alusel.

24. Isikuandmete kaitse üldmääruse artikli 64 lõigete 7 ja 8 kohaselt annab järelevalveasutus kahe nädala jooksul pärast arvamuse saamist eesistujale elektroonilisel teel teada, kas ta muudab oma akrediteerimisnõuete eelnõud või mitte. Sama ajavahemiku jooksul esitab järelevalveasutus muudetud esialgse loetelu või kui ta ei kavatse andmekaitsenõukogu arvamust arvesse võtta, põhjused, miks tal ei ole kavas arvamust tervikuna või osaliselt järgida.

25. Järelevalveasutus edastab andmekaitsenõukogule lõpliku otsuse selle kandmiseks nende otsuste registrisse, mille suhtes on kohaldatud järjepidevuse mehhanismi, kooskõlas isikuandmete kaitse üldmääruse artikli 70 lõike 1 punktiga y.

Euroopa Andmekaitsenõukogu nimel

eesistuja

(Andrea Jelinek)