Arvamus 16/2020, mis käsitleb Tšehhi Vabariigi pädeva järelevalveasutuse otsuse eelnõu sertifitseerimisasutuse akrediteerimise nõuete heakskiitmise kohta kooskõlas isikuandmete kaitse üldmääruse artikli 43 lõikega 3

Vastu võetud 25. mail 2020

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 Euroopa Majanduspiirkonna (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 ülesehitust, mis on esitatud Euroopa Andmekaitsenõukogu sertifitseerimisasutuste akrediteerimise suuniste lisas, ning teiseks sellega, et analüüsib neid nõudeid 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 või 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.

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

(5) 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 akrediteerimisnõuded juhinduma standardist ISO/IEC 17065 ja neile peaksid lisanduma täiendavad nõuded, mille järelevalveasutus kehtestab kooskõlas 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 töökorra 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. Tšehhi järelevalveasutus esitas Euroopa Andmekaitsenõukogule kooskõlas artikli 43 lõike 1 punktiga b akrediteerimisnõuete eelnõu. Toimik loeti täielikuks 17. veebruaril 2020. Tšehhi riiklik akrediteerimisasutus akrediteerib sertifitseerimisasutusi isikuandmete kaitse üldmääruses esitatud sertifitseerimiskriteeriumide alusel. See tähendab, et riiklik akrediteerimisasutus kasutab sertifitseerimisasutuste akrediteerimiseks standardit ISO 17065 ja Tšehhi järelevalveasutuse kehtestatud täiendavaid nõudeid, kui järelevalveasutus on need pärast andmekaitsenõukogult nõuete eelnõu käsitleva arvamuse saamist heaks kiitnud.

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

[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_et

andmekaitsenõukogu, et Tšehhi järelevalveasutus on otsustanud teha akrediteerimise oma riikliku akrediteerimisasutuse ülesandeks, olles koostanud suuniste järgi täiendavad nõuded, mida riiklik akrediteerimisasutus peaks akrediteerimisel kasutama.

4. Tšehhi järelevalveasutuse täiendavate akrediteerimisnõuete hindamise eesmärk on uurida, kuivõrd need nõuded erinevad suunistes ja eelkõige suuniste 1. lisas 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 saaks järelevalveasutuse konteksti arvestades 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 Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu konkreetse osa kohta midagi öeldud, tähendab see, et andmekaitsenõukogul ei ole selle osa kohta märkusi ning Tšehhi järelevalveasutusel ei ole vaja lisameetmeid võtta.

9. Arvamuses ei käsitleta Tšehhi järelevalveasutuse esitatud teavet, mis ei kuulu isikuandmete kaitse üldmääruse artikli 43 lõike 2 kohaldamisalasse, näiteks viiteid siseriiklikele õigusaktidele. Andmekaitsenõukogu märgib sellegipoolest, et siseriiklikud 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:

a. suuniste lisas märgitud kõigi põhivaldkondade käsitlemine ja lisast hälbimise analüüsimine;

b. sertifitseerimisasutuse sõltumatus;

c. sertifitseerimisasutuse huvide konfliktid;

d. sertifitseerimisasutuse asjatundlikkus;

e. asjakohased kaitsemeetmed tagamaks, et sertifitseerimisasutus kohaldab isikuandmete kaitse üldmääruses sätestatud sertifitseerimiskriteeriume nõuetekohaselt;

f. isikuandmete kaitse üldmääruse kohase sertifikaadi väljastamise, korrapärase läbivaatamise ja tagasivõtmise menetlused ning

g. 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 EESSÕNA

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 asjakohaseks.

2.2.2 ÜLDISED MÄRKUSED

12. Andmekaitsenõukogu märgib, et akrediteerimisnõuete eelnõu ei ole täielikult kooskõlas suuniste 1. lisas esitatud ülesehitusega. Näiteks puuduvad jaotised „Kohaldamisala“ ning „Mõisted ja määratlused“. Sellega seoses leiab andmekaitsenõukogu, et selguse huvides ja nõuete hõlpsamaks hindamiseks saaks dokumendi numeratsiooni ja üldist ülesehitust parandada. Seepärast soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel hindamise hõlbustamiseks järgida akrediteerimisnõuete eelnõus lisa ülesehitust ja lisada puuduvad jaotised, sest dokumendis läbivalt kasutatud mõistete määratlus on eriti oluline. Lisaks märgib andmekaitsenõukogu, et Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõus viidatakse mitu korda vastavale ISO 17065 jaotisele

või lisa vastavatele jaotistele, täpsustamata siiski sellist viidet. Seega soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel selgitada viiteid standardi ISO 17065 ja lisa jaotistele.

13. Andmekaitsenõukogu märgib, et Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõus viidatakse mitu korda „hinnatud objektile“ (nt punktid 3.2.1.2.1.2.10; 3.2.1.2.6.3.1; 3.2.1.2.8.1.6.3; 3.2.1.2.10.4.1; 3.1.2.10.7.3.1; 3.1.2.10.7.3.2 ja 3.2.1.2.10.10.2). Andmekaitsenõukogu mõistab, et seda mõistet kasutatakse hindamise objekti sünonüümina. Selguse tagamiseks soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel siiski kasutada järjepidevalt mõistet „hindamise objekt“.

14. Andmekaitsenõukogu märgib, et mitu nõuet ei ole sõnastatud sertifitseerimisasutuse kohustusena (nt 3.2.1.2.2 ja 3.2.1.2.3). Andmekaitsenõukogu soovitab Tšehhi järelevalveasutusel nõudeid muuta, näitamaks selgelt, et need on kohustuslikud, st alustama nõuet sõnadega „sertifitseerimisasutus peab [...]“.

2.2.3 ÜLDISED AKREDITEERIMISNÕUDED

15. Seoses sertifitseerimislepinguga (Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu punkt 3.2.1.2.1.2) märgib andmekaitsenõukogu, et alapunktis 3.2.1.2.1.2.2 ei viidata „konfidentsiaalsetele lepingulistele küsimustele“, millele järelevalveasutusel peab samuti olema juurdepääs. Seepärast soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel eelnõu muuta, lisades kohustuse anda järelevalveasutusele juurdepääs ka konfidentsiaalsetele lepingulistele küsimustele.

16. Seoses Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu alapunktiga 3.2.1.2.1.2.8 märgib andmekaitsenõukogu, et ei ole selge, kellele tuleb teave avalikustada. Seepärast soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel täpsustada, kes on teabe saaja. Lisaks peab osutatud teave olema „vajalik sertifikaadi andmiseks“, nagu on sätestatud lisa jaotise 4.1.2 punktis 7. Andmekaitsenõukogu soovitab Tšehhi järelevalveasutusel asendada sõnad „teave sertifikaadi andmise kohta“ sõnadega „sertifikaadi andmiseks vajalik teave“.

17. Seoses Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu alapunktiga 3.2.1.2.1.2.9 ei ole selge, mis liiki teavet tuleks edastada otse andmekaitsenõukogule. Isikuandmete kaitse üldmääruse artikli 42 lõikes 8 on sätestatud andmekaitsenõukogu kohustus koondada muu hulgas kõik sertifitseerimismehhanismid. Sellega seoses eeldatakse, et pädevad järelevalveasutused esitavad asjakohase teabe andmekaitsenõukogule, kes avaldab selle seejärel avalikus registris. Seepärast soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel täpsustada nõuete eelnõu alapunkti 3.2.1.2.1.2.9 kooskõlas isikuandmete kaitse üldmääruse artikli 42 lõikega 8.

18. Seoses Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu alapunktiga 3.2.1.2.1.2.12 võtab andmekaitsenõukogu teadmiseks asjaolu, et Tšehhi järelevalveasutus on koostanud lisas ette nähtud nõude osa ümbersõnastatud versiooni. Tšehhi järelevalveasutus jättis siiski välja viite sellele, et [kui see on kohaldatav] „tuleks käsitleda ka tagajärgi kliendile“. Seepärast soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel lisada eespool nimetatud nõude puuduv osa.

19. Lisaks on Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu alapunktis 3.2.1.2.1.2.13 sätestatud kohustus „lisada taotleja kohustus teavitada sertifitseerimisasutust kõikidest muudatustest, mis võivad mõjutada sertifitseeritud objekti vastavust sertifitseerimiskriteeriumidele“. Andmekaitsenõukogu peab seda sõnastust liiga üldiseks ja soovitab Tšehhi järelevalveasutusel muuta

nõuete eelnõu nii, et see hõlmaks „kõiki muudatusi tema tegelikus või õiguslikus olukorras ning tema sertifitseerimisega seotud toodetes, protsessides ja teenustes“.

20. Andmekaitsenõukogu märgib seoses andmekaitsepitserite ja -märgiste kasutamisega (Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu punkt 3.2.1.2.1.3), et Tšehhi järelevalveasutuse nõuete eelnõus on sätestatud, et sertifitseerimisleping sisaldab „sertifikaatide, pitserite ja märgiste kasutamise eeskirju, kui sertifitseerimissüsteemi omanik on need ette näinud“. Sama sõnastus on esitatud alapunktis 3.2.1.2.1.2.14. Andmekaitsenõukogu leiab, et see kohustus on juba hõlmatud standardi ISO 17065 jaotise 4.1.2.2 punktiga l ja seetõttu peaks see sisalduma mis tahes sertifitseerimissüsteemis (vt ka standardi ISO 17065 jaotis 4.1.3). Seega soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel selguse huvides jätta eespool nimetatud punktid välja.

21. Seoses erapooletuse tagamise nõuetega on Tšehhi järelevalveasutuse poolt vormil esitatud teabe kohaselt lisa jaotised 4.2.1.b ja 4.2.2 piisavalt hõlmatud standardi ISO 17065 jaotisega 4.2. Andmekaitsenõukogu on siiski seisukohal, et need nõuded tuleb sõnaselgelt lisada järelevalveasutuste poolt kooskõlas lisaga välja töötatud akrediteerimisnõuete eelnõudesse. Seepärast soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel lisada puuduvad erapooletuse tagamise nõuded, mis on ette nähtud lisas.

22. Seoses vastutuse ja rahastamise nõudega (Tšehhi järelevalveasutuse nõuete eelnõu punkt 3.2.1.2.3.1) soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel täpsustada, et see tuleb tagada korrapäraselt.

2.2.4 RESSURSSE KÄSITLEVAD NÕUDED

23. Seoses sertifitseerimisasutuse töötajatega (Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu punkt 3.2.1.2.8.1.6) märgib andmekaitsenõukogu, et hindamise eest vastutavatele töötajatele esitatavad nõuded (alapunkt 3.2.1.2.8.1.6.3) hõlmavad „*vähemalt 5-aastast praktikat, mille korral on sertifitseerimistegevuse käigus tehtud vähemalt 10 auditit samas või sarnases valdkonnas […], või sertifitseerimisasutuste tähelepanu keskmes olevate objektide sertifitseerimise 5-aastast praktikat*“. Samamoodi hõlmavad nõuded otsuse tegemise eest vastutavatele töötajatele (alapunkt 3.2.1.2.8.1.6.4) „*vähemalt 5-aastast praktikat, mille korral on sertifitseerimistegevuse käigus tehtud vähemalt 10 auditit samas või sarnases valdkonnas*“. Andmekaitsenõukogu on seisukohal, et hindajate ja otsusetegijate eksperditeadmistele esitatavad nõuded peaksid olema kohandatud, võttes arvesse nende erinevaid ülesandeid. Seoses sellega on andmekaitsenõukogu arvamusel, et hindajatel peaksid olema erialasemad eksperditeadmised ja töökogemus tehniliste menetluste valdkonnas (nt auditid ja sertifitseerimine), samas kui otsusetegijatel peaksid olema üldisemad ja terviklikumad eksperditeadmised ja töökogemus andmekaitse valdkonnas. Seda arvesse võttes soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel see alapunkt ümber sõnastada, arvestades sisuliste teadmiste ja/või kogemuste suhtes hindajatele ja otsusetegijatele esitatavaid eri nõudeid.

24. Andmekaitsenõukogu võtab lisaks teadmiseks, et Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu punktis 3.2.1.2.9.1 on sätestatud, et sertifitseerimistegevuste korral ei ole allhange lubatud. Järgmine punkt lubab siiski kasutada hindamiseks välisaudiitoreid ja -eksperte, välja arvatud juhul, kui tegemist on sertifitseerimistegevustega. Andmekaitsenõukogu leiab, et akrediteerimisnõuete eelnõus tuleks täpsustada, millal on tegemist sertifitseerimistegevustega, või selgitada, et

sertifitseerimisasutus jääb otsuste tegemise eest vastutavaks, isegi kui ta kasutab väliseksperte. Seepärast soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel eelnõu vastavalt muuta.

2.2.5 MENETLUSNÕUDED

25. Andmekaitsenõukogu märgib, et Tšehhi järelevalveasutuse täiendavate nõuete eelnõu punktis 3.2.1.2.10.1.1 viidatakse „kõikidele huvide konflikti käsitlevatele täiendavatele nõuetele (jaotise 7.1 punkt 1)“. Tšehhi järelevalveasutuse täiendavate nõuete eelnõu ei sisalda siiski täiendavaid nõudeid huvide konflikti kohta. Seetõttu soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel eelnõu muuta, et vältida segadust.

26. Seoses taotlusnõuetega märgib andmekaitsenõukogu, et Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu alapunkt 3.2.1.2.10.2.3 näib viitavat, et teave edastatud andmete kohta esitatakse taotluses ainult siis, kui andmed edastatakse kolmandale riigile või rahvusvahelisele organisatsioonile. Andmekaitsenõukogu rõhutab, et taotleja peab siiski alati lisama teistele süsteemidele või organisatsioonidele edastatud andmete kirjelduse, olenemata nende asukohast. Seepärast soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel muuta sõnastust, et vältida segadust.

27. Andmekaitsenõukogu märgib, et kohustus sätestada sertifitseerimislepingus siduvad hindamismeetodid (Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu punkt 3.2.1.2.1.2.6) ei sisalda viidet hindamise objektile suuniste lisa jaotise 7.3 punkti 1 kohaselt. Selguse huvides soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel selline viide lisada.

28. Lisaks märgib andmekaitsenõukogu, et Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõus nähakse ette olukord, kus volitatud töötlejaid kasutatakse andmetöötlustoimingute tegemiseks kooskõlas suuniste lisaga (Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu punkt 3.2.1.2.10.2). Andmekaitsenõukogu soovitab Tšehhi järelevalveasutusel kaaluda, kas sel juhul peaks viitama ka kaasvastutavatele töötlejatele ja nendevahelistele erikokkulepetele.

29. Seoses hindamisnõuetega (Tšehhi järelevalveasutuse nõuete eelnõu punkt 3.2.1.2.10.4) märgib andmekaitsenõukogu, et Tšehhi järelevalveasutuse akrediteerimisnõuded ei sisalda sertifitseerimisasutuse kohustust kirjeldada oma sertifitseerimismehhanismis üksikasjalikult, kuidas teatatakse taotlejale standardi ISO 17065 jaotises 7.4.6 nõutav teave sertifitseerimismehhanismiga tuvastatud mittevastavuste kohta. Nagu on sätestatud lisas (alajaotis 7.4), tuleb määrata vähemalt sellise teabe olemus ja esitamise aeg. Seepärast soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel lisada eespool nimetatud kohustus.

30. Lisaks tundub, et Tšehhi järelevalveasutuse nõuete eelnõu alapunkti 3.2.1.2.10.4.2 kohaselt piirduvad hindamismeetodid testimise, auditeerimise või inspekteerimisega. Andmekaitsenõukogu leiab, et kasutada võiks ka muid hindamismeetodeid, ning soovitab seetõttu Tšehhi järelevalveasutusel eelnõu muuta, näitamaks selgelt, et loetelu ei ole ammendav.

31. Seoses Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu punktiga 3.2.1.2.10.4.4.1.4 leiab andmekaitsenõukogu, et nõuetes tuleks selgelt märkida, et sertifitseerimisasutus on kohustatud kontrollima vastavust kriteeriumidele, ja soovitab Tšehhi järelevalveasutusel eelnõu vastavalt muuta.

32. Seoses läbivaatamisnõuetega (Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu alapunkt 3.2.1.2.10.5) täheldab andmekaitsenõukogu, et Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõus ei viidata sertifikaatide väljastamise ja tagasivõtmise menetluste

kehtestamise kohustusele. Andmekaitsenõukogu soovitab Tšehhi järelevalveasutusel eelnõu vastavalt muuta.

33. Seoses sertifitseerimisdokumentidele esitatavate nõuetega märgib andmekaitsenõukogu, et Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu punktis 3.1.2.10.7.2 on sätestatud, et sertifitseerimisasutus täpsustab, et järelevalve on sertifitseerimise kehtivuse tingimus, „kui järelevalve on nõutav sertifitseerimissüsteemiga […]“. Andmekaitsenõukogu leiab, et isikuandmete kaitse üldmääruse kohase sertifitseerimise korral on järelevalve alati kohustuslik, ja soovitab seetõttu Tšehhi järelevalveasutusel lisada selline kohustus.

34. Seoses sertifitseeritud toodete kataloogiga seotud nõuetega (Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu punkt 3.2.1.2.10.8 ja lisa jaotis 7.8) ning eelkõige kohustusega teatada pädevale järelevalveasutusele taotletud sertifikaadi väljastamise või tagasivõtmise põhjused märgib andmekaitsenõukogu, et Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõus viidatakse punktile 3.2.1.2.10.4.5. Selles punktis käsitletakse siiski kohustust teha hindamisdokumendid taotluse korral Tšehhi järelevalveasutusele kättesaadavaks, samas kui suuniste lisa jaotises 7.8 sätestatud nõue sisaldab kohustust teatada järelevalveasutusele ennetavalt sertifikaadi väljastamise või tagasivõtmise põhjused. Seepärast soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel eelnõu vastavalt muuta.

35. Seoses sertifitseerimist mõjutavate muudatustega märgib andmekaitsenõukogu, et Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõus ei nimetata kokkulepitavate menetluste seas suuniste lisas osutatud pädevalt järelevalveasutuselt heakskiidu saamise menetlust (lk 19). Andmekaitsenõukogu tunnistab, et lisa jaotises 7.10 esitatud loetelu ei ole kohustuslik. Järjepidevuse tagamiseks soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel lisada siiski viide järelevalveasutuselt heakskiidu saamise menetlusele.

36. Andmekaitsenõukogu täheldab, et Tšehhi järelevalveasutuse akrediteerimisnõuete eelnõu ei hõlma selgelt sertifitseerimisasutuse kohustust aktsepteerida pädeva järelevalveasutuse otsuseid ja korraldusi võtta sertifikaat tagasi või jätta sertifikaat taotlejale väljastamata, kui sertifitseerimise nõuded ei ole enam täidetud. Andmekaitsenõukogu soovitab Tšehhi järelevalveasutusel lisada see kohustus selgelt akrediteerimisnõuete eelnõusse. Seoses sertifikaadi lõppemise, piiramise, peatamise või tagasivõtmisega märgib andmekaitsenõukogu, et nõuete eelnõu punktides 3.2.1.2.10.10.2 ja 3.2.1.2.10.10.3 osutatakse „algatamisele“. Kui soovitakse viidata järelevalveasutuse „otsustele ja korraldustele“, nagu on sätestatud isikuandmete kaitse üldmääruse artikli 58 lõike 2 punktis h, soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel kasutada isikuandmete kaitse üldmäärusega sama terminoloogiat ning viidata „otsustele ja korraldustele“.

2.2.6 JUHTIMISSÜSTEEM

37. Andmekaitsenõukogu leiab, et Tšehhi järelevalveasutuse täiendavate nõuete eelnõu punkt 3.2.1.2.11 ei sisalda sertifitseerimisasutuse kohustust „avalikustada pidevalt ja püsivalt selle, milline sertifitseerimine on toimunud millistel alustel, samuti kui kaua ning millise raamistiku ja milliste tingimuste aluse sertifikaadid kehtivad“, nagu on sätestatud lisa jaotises 8. Seepärast soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel muuta nõuete eelnõu, lisades sellesse eespool nimetatud viite.

3 JÄRELDUSED/SOOVITUSED

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

39. Seoses üldiste akrediteerimisnõuetega soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel:

    1) lisada punkti 3.2.1.2.1.2 kohustus anda järelevalveasutusele juurdepääs „konfidentsiaalsetele lepingulistele küsimustele“;

    2) asendada alapunktis 3.2.1.2.1.2.8 sõnad „teave sertifikaadi andmise kohta“ sõnadega „sertifikaadi andmiseks vajalik teave“;

    3) täpsustada alapunkti 3.2.1.2.1.2.9 kooskõlas isikuandmete kaitse üldmääruse artikli 42 lõikega 8;

    4) lisada alapunkti 3.2.1.2.1.2.12 viide sellele, et [kui see on kohaldatav] „tuleks käsitleda ka tagajärgi kliendile“;

    5) muuta alapunkti 3.2.1.2.1.2.13, et see hõlmaks „kõiki muudatusi tema tegelikus või õiguslikus olukorras ning tema sertifitseerimisega seotud toodetes, protsessides ja teenustes“;

    6) jätta välja punkt 3.2.1.2.1.3 ja alapunkt 3.2.1.2.1.2.14;

    7) lisada puuduvad erapooletuse tagamise nõuded, mis on ette nähtud lisas.

40. Seoses vahenditega seotud nõuetega soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel:

    1) muuta punkti 3.2.1.2.9.1, et täpsustada, millal on tegemist sertifitseerimistegevusega, või selgitada, et sertifitseerimisasutus vastutab otsuste tegemise eest ka siis, kui ta kasutab väliseksperte.

41. Seoses menetlusnõuetega soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel:

    1) lisada punkti 3.2.1.2.10.4 sertifitseerimisasutuse kohustus kirjeldada oma sertifitseerimismehhanismis üksikasjalikult, kuidas teatatakse taotlejale standardi ISO 17065 jaotises 7.4.6 nõutav teave sertifitseerimismehhanismiga tuvastatud mittevastavuste kohta;

    2) muuta punkti 3.2.1.2.10.5, et viidata kohustusele sätestada sertifikaatide väljastamise ja tagasivõtmise menetlused;

    3) muuta punkti 3.1.2.10.7.2 kajastamaks, et isikuandmete kaitse üldmääruse kohase sertifitseerimise korral on järelevalve alati kohustuslik;

    4) muuta punkti 3.2.1.2.10.8, et kajastada sertifitseerimisasutuse kohustust teatada järelevalveasutusele ennetavalt sertifikaadi väljastamise või tagasivõtmise põhjused;

    5) lisada sertifitseerimisasutuse kohustus aktsepteerida pädeva järelevalveasutuse otsuseid ja korraldusi võtta sertifikaat tagasi või jätta sertifikaat taotlejale väljastamata, kui sertifitseerimise nõuded ei ole enam täidetud.

42. Seoses juhtimissüsteemiga soovitab andmekaitsenõukogu Tšehhi järelevalveasutusel:

1) lisada sertifitseerimisasutuse kohustus „avalikustada pidevalt ja püsivalt, mis sertifitseerimine on toimunud mis alustel, samuti kui kaua ning mis raamistiku ja mis tingimuste alusel sertifikaadid kehtivad“, nagu on sätestatud lisa jaotises 8.

4 LÕPPMÄRKUSED

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

44. 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 eelnõu 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.

45. Tšehhi 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)