Arvamus 15/2020, mis käsitleb Saksamaa pädevate järelevalveasutuste 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 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. Kuigi 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 1. lisas 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 kontekstis tuleb lähtuda suunistest 4/2018 isikuandmete kaitse üldmääruse (2016/679) artikli 43 kohase sertifitseerimisasutuste akrediteerimise kohta (edaspidi „suunised“) ning suunistest 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 sertifitseerimisasutusi akrediteerib järelevalveasutus, peaks järelevalveasutus kehtestama akrediteerimisnõuded, mis hõlmavad artikli 43 lõikes 2 sätestatud nõudeid, kuid ei piirdu nendega. 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 eritletakse 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 küsimuse keerukust,

ON VASTU VÕTNUD JÄRGMISE ARVAMUSE:

1 ASJAOLUDE KOKKUVÕTE

1. Saksamaa föderaalne järelevalveasutus ja liidumaade järelevalveasutused (edaspidi „Saksamaa järelevalveasutused“) esitasid Euroopa Andmekaitsenõukogule kooskõlas artikli 43 lõike 1 punktiga b akrediteerimisnõuete eelnõu. Toimik loeti täielikuks 13. veebruaril 2020. Saksamaa riiklik akrediteerimisasutus DAkkS akrediteerib sertifitseerimisasutusi isikuandmete kaitse üldmääruses esitatud sertifitseerimiskriteeriumide alusel. See tähendab, et riiklik akrediteerimisasutus kasutab sertifitseerimisasutuste akrediteerimiseks standardit ISO 17065 ja Saksamaa järelevalveasutuste kehtestatud täiendavaid nõudeid, kui järelevalveasutused on need pärast andmekaitsenõukogult nõuete eelnõu käsitleva arvamuse saamist heaks kiitnud.

2. Kooskõlas andmekaitsenõukogu töökorra artikli 10 lõikega 2 otsustas eesistuja küsimuse keerukuse tõttu pikendada esialgset kaheksanädalast vastuvõtmisperioodi veel kuue nädala võrra.

2 HINNANG

2.1 Euroopa Andmekaitsenõukogu üldine seisukoht esitatud otsuse eelnõu kohta

3. Käesoleva 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

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

ja uuendada. See ei piira pädeva järelevalveasutuse ülesandeid ega volitusi. Käesoleval juhul nendib andmekaitsenõukogu, et Saksamaa järelevalveasutused on otsustanud teha akrediteerimise riikliku akrediteerimisasutuse DAkkS ja pädeva järelevalveasutuse ühiseks ülesandeks, olles koostanud vastavalt suunistele täiendavad nõuded, mida tuleks akrediteerimisel kasutada.

4. Saksamaa järelevalveasutuste 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 peavad järelevalveasutused koostama sertifitseerimisasutuste akrediteerimise nõuded nii, et neid saaks järelevalveasutuste kontekstis praktiliselt ja järjekindlalt kohaldada.

6. Andmekaitsenõukogu tunnistab, et riiklike akrediteerimisasutuste ja pädevate järelevalveasutuste asjatundlikkust arvestades tuleks neile vajaduse korral anda kohaldatavate akrediteerimisnõuete raames teatavate erinõuete määratlemisel tegutsemisvabadust. Andmekaitsenõukogu peab siiski 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 kordamata.

8. Andmekaitsenõukogu järgis hindamisel suuniste 1. lisas (edaspidi „lisa“) ette nähtud ülesehitust. Kui arvamuses ei öelda Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu konkreetse osa kohta midagi, tähendab see, et andmekaitsenõukogul ei ole selle osa kohta märkusi ning Saksamaa järelevalveasutustel ei ole tarvis lisameetmeid võtta.

9. Käesolevas arvamuses ei käsitleta Saksamaa järelevalveasutuste esitatud teavet, mis jääb välja isikuandmete kaitse üldmääruse artikli 43 lõike 2 kohaldamisalast, näiteks viiteid riiklikele õigusaktidele. Andmekaitsenõukogu märgib siiski, et riiklikud õigusaktid peaksid olema vajaduse korral 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 lisast 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,

on andmekaitsenõukogu järgmisel arvamusel:

2.2.1 EESSÕNA

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

2.2.2 MÕISTED JA MÄÄRATLUSED

12. Andmekaitsenõukogu nendib, et Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu 3. peatükis „Määratlused“ määratletakse, mis liiki sertifitseerimissüsteemid on lubatud, sätestades, et need peavad vastama standardi DIN EN ISO/IEC 17065 nõuetele. Nimetatut käsitledes tuleks rõhutada, et Euroopa Andmekaitsenõukogu suuniste punktides 5.1 ja 5.2 on põhjalik ülevaade sellest, mida on võimalik isikuandmete kaitse üldmääruse kohaselt sertifitseerida. Seepärast sedastab andmekaitsenõukogu, et Saksamaa järelevalveasutuste eesmärk ei ole piirata suunistes sätestatut ja

et Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu 3. peatükis esitatud väiteid tuleb pidada akrediteerimisnõuete kontekstis kehtivaks.

2.2.3 ÜLDMÄRKUSED

13. Andmekaitsenõukogu täheldab, et Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu üldmärkuste punktis viidatakse, et Euroopa Andmekaitsenõukogu kinnitab sertifitseerimiskriteeriumid „isikuandmete kaitse üldmääruse artikli 63 ja artikli 64 lõike 1 punkti c kohaselt“. Andmekaitsenõukogu märgib, et isikuandmete kaitse üldmäärusega ei anta Euroopa Andmekaitsenõukogule pädevust sertifitseerimiskriteeriume kinnitada. Samas võib eespool nimetatud artiklite kohaselt Euroopa Andmekaitsenõukogu sertifitseerimiskriteeriumid heaks kiita. Seepärast soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel oma eelnõu isikuandmete kaitse üldmääruse sõnastusega kooskõlla viimiseks välja jätta viide „Euroopa Andmekaitsenõukogu kinnitab“.

2.2.4 ÜLDISED AKREDITEERIMISNÕUDED (akrediteerimisnõuete eelnõu 4. peatükk)

14. Andmekaitsenõukogu märgib õigusliku vastutuse nõude kohta (Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu punkt 4.1), et Saksamaa järelevalveasutused täpsustavad tugidokumendis, et sertifitseerimisasutuselt eeldatakse ajakohastatud menetlusi ja seetõttu ei ole vaja selle kohta täiendavaid nõudeid sätestada. Andmekaitsenõukogu leiab siiski, et eeldus ei kohusta sertifitseerimisasutusi selliseid menetlusi kehtestama. Suuniste lisa punktis 4.1.1 on ette nähtud, et sertifitseerimisasutused kasutavad ajakohaseid menetlusi, mis tõendavad akrediteerimistingimustes sätestatud õiguslike kohustuste täitmist. Lisaks peab sertifitseerimisasutus suutma tõendada, et ta rakendab isikuandmete kaitse üldmäärusega kooskõlas olevaid menetlusi ja meetmeid, eelkõige kliendi organisatsiooni isikuandmete kontrollimisel ja käsitlemisel sertifitseerimisprotsessi raames. Seepärast soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel muuta nõuete eelnõu, et viia see vastavusse suunistega.

15. Andmekaitsenõukogu märgib Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu alapunkti 4.1.2.2 „Sertifitseerimisleping“ kohta, et Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu ei sisalda kohustust tagada pädevale järelevalveasutusele sertifitseerimismenetluses täielik läbipaistvus muu hulgas konfidentsiaalsetes lepingulistes küsimustes. Lisaks ei viidata taotleja kohustusele anda sertifitseerimisasutusele juurdepääs taotleja töötlemistoimingutele. Seepärast soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel lisada eelnõule eespool nimetatud kohustused.

16. Andmekaitsenõukogu täheldab, et Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu alapunkt 4.1.2.2 ei sisalda (lisa punkti 4.1.2 kolmandas taandes) selgesõnalist nõuet pädeva järelevalveasutuse ülesannetele ja volitustele. Andmekaitsenõukogu on seisukohal, et viide tuleks lisada nõuete eelnõule, ja soovitab seepärast Saksamaa järelevalveasutustel eelnõu vastavalt muuta.

17. Lisaks ei sisalda Saksamaa järelevalveasutuste nõuete eelnõu sertifitseerimislepingu sätted kohustust võimaldada sertifitseerimisasutusel avalikustada kogu isikuandmete kaitse üldmääruse artikli 42 lõike 8 ja artikli 43 lõike 5 kohane sertifitseerimiseks vajalik teave (lisa punkti 4.1.2 seitsmes taane). Andmekaitsenõukogu leiab, et kuigi seda kohustust sisaldab Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu protsessihalduse punkt, peaks see olema kohustuse siduvamaks muutmise eesmärgil sertifitseerimislepingu osa. Seepärast soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel lisada eespool nimetatud kohustus sertifitseerimislepingu sätetele.

18. Taotleja peab lisa kohaselt teavitama sertifitseerimisasutust, kui tema tegelik või õiguslik olukord ning tema sertifitseerimisega seotud tooted, protsessid ja teenused oluliselt muutuvad (lisa punkti 4.1.2 kümnes taane). Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu alapunkti 4.1.2.2 kuues taane sisaldab ainult kohustust teavitada sertifitseerimisasutust, kui taotleja tegelik või õiguslik olukord oluliselt muutub, aga sättes ei ole nimetatud selge sõnaga tooteid, protsesse ega teenuseid. Andmekaitsenõukogu soovitab Saksamaa järelevalveasutustel lisada see viide kooskõlas lisaga.

19. Andmekaitsenõukogu soovitab tugevdada Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu alapunktis 4.2.7 „Erapooletus“ esitatud kriteeriume, mida kohaldatakse eraldi juriidilisele isikule kuuluvatele või alluvatele sertifitseerimisasutustele, et võtta arvesse, et sertifitseerimisasutuse ja juriidilise isiku mis tahes majandussuhted võivad mõjutada tema sertifitseerimistegevuse erapooletust, olenevalt selle eripärast.

20. Andmekaitsenõukogu märgib Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu punkti 4.6 „Avalikult kättesaadav teave“ kohta, et selles ei viidata heakskiidetud kriteeriumide kõigi versioonide ja sertifitseerimismenetluste avaldamisele. Seepärast soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel muuta akrediteerimisnõuete eelnõu, et sätestada selge sõnaga, et avaldatakse heakskiidetud kriteeriumide kõik versioonid ja sertifitseerimismenetlused. Lisaks märgib andmekaitsenõukogu, et punkti 4.6 teises lõigus sätestatakse, et „sertifitseerimisasutuse kasutatavad sertifitseerimissüsteemid, isikuandmete kaitse üldmääruse artikli 42 lõike 5 kohaselt heakskiidetud kriteeriumid, mille alusel kinnitatakse taotluse jätkuvat kehtivust, *üldiselt avaldatakse*“. Andmekaitsenõukogu soovitab Saksamaa järelevalveasutustel arusaamatuste vältimiseks välja jätta sõna „üldiselt“ ja lisada sõna „sertifitseerimissüsteemid“ ja sõnade “isikuandmete kaitse” vahele sidesõna „ja“.

2.2.5 VAHENDITEGA SEOTUD NÕUDED (akrediteerimisnõuete eelnõu 6. peatükk)

21. Andmekaitsenõukogu märgib asjatundlikkusnõudeid ja täpsemalt Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu alapunkti 6.1.2.1 käsitledes, et loetletud valdkondades nõutavad teadmised ei pea sätete kohaselt olema asjakohased ja piisavad. Andmekaitsenõukogu soovitab Saksamaa järelevalveasutustel lisas nõutava asjatundlikkuse tasemega järjepidevuse tagamiseks viia eelnõu vastavusse suuniste sõnastusega, nõudes, et teadmiseks oleksid asjakohased ja piisavad.

22. Lisaks nendib andmekaitsenõukogu, et otsustamise eest vastutavatele tehniliste teadmiste ja kogemustega töötajatele esitavad nõuded sisaldavad nende haridustasemest sõltuvalt vähemalt 7-aastast töökogemust või 5-aastast tehnilise andmekaitse töökogemust, kuid hindamiste eest vastutavatelt töötajatelt nõutakse nende haridustasemest sõltuvalt vähemalt 4-aastast töökogemust või 2-aastat tehnilise andmekaitse töökogemust ja kogemusi testimismenetluses. Samuti peab otsustamise eest vastutavatel juriidiliste teadmiste ja kogemustega töötajatel olema vähemalt 5-aastane andmekaitseõiguse töökogemus, kuid hindamiste eest vastutavatel töötajatel peab olema vähemalt 2-aastane andmekaitseõiguse ja auditeerimismenetluste töökogemus. Andmekaitsenõukogu märgib, et otsustamise eest vastutavalt personalilt ja hindamise eest vastutavalt personalilt nõutud minimaalse töökogemuse vahel on suur erinevus. Andmekaitsenõukogu arvab selle kohta, et hindajate ja otsustajate pädevusnõudeid tuleks kohandada, võttes arvesse pigem nende täidetavaid erinevaid ülesandeid, mitte töökogemuse kestust. Andmekaitsenõukogu arvates peaks hindajatel olema kitsam ja põhjalikum oskusteave ja töökogemus seoses tehniliste menetlustega (nt auditid ja sertifitseerimine), samas kui otsustajatel peaks olema üldisem ja laiem oskusteave ja töökogemus seoses andmekaitsega. Seda silmas pidades

soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel rohkem rõhutada hindajate ja otsustajate erinevatele sisulistele teadmistele ja/või kogemustele ning vähendada eeldatava töökogemuse erinevust.

23. Veel leiab andmekaitsenõukogu, et sertifitseerimisvaldkonnaga seotud juhtimissüsteemide tundmine peaks hõlmama ka standardit ISO/IEC 27701:2019 „Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines“ (turbemeetodid – eraelu puutumatuse teabe haldamise laiendus standarditele ISO/IEC 27001 ja ISO/IEC 27002 – nõuded ja suunised) ja soovitab Saksamaa järelevalveasutustel selle viite lisada.

24. Andmekaitsenõukogu arvab tehniliste töötajate haridusnõuete kohta, et erialade loetelu on juba kohandatud lisas nõutud tehniliste teadmiste ja kogemustega. Seepärast soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel tehniliste töötajate kõrghariduse erialade loetelust viide loodusteadustele välja jätta.

2.2.6 TÖÖTLEMISNÕUDED (akrediteerimisnõuete eelnõu 7. peatükk)

25. Andmekaitsenõukogu märgib, et Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu 7. peatükis (nt punktides 7.4, 7.6, 7.11 ja 7.13) viidatakse mitu korda „selle kriteeriumidele“. Andmekaitsenõukogu soovitab Saksamaa järelevalveasutustel täpsustada arusaamatuste vältimiseks fraasi tähendust, lisades selle määratluse näiteks 1. lisale „Sõnastik“.

26. Andmekaitsenõukogu märgib Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu punkti 7.1 „Üldteave“ kohta, et selles ei ole selgesõnalist viidet sertifitseerimisasutuse kohustusele vastata täiendavatele nõuetele. Kuigi kohustust võiks järeldada nõuete eelnõu tekstist, leiab andmekaitsenõukogu, et lisada tuleks selgesõnaline viide eespool nimetatud kohustusele. Seepärast soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel oma eelnõu vastavalt muuta.

27. Andmekaitsenõukogu sedastab, et Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu ei sisalda viidet heakskiidetud Euroopa andmekaitsepitseri kasutamisele (vt lisa punkt 7.1.2). Andmekaitsenõukogu on seisukohal, et viide tuleks lisada, eelkõige arvestades, et Euroopa andmekaitsepitsereid andev sertifitseerimisasutus võidakse akrediteerida sertifitseerimisasutuse asukohaks olevas mis tahes liikmesriigis. [3] Seepärast soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel lisada eespool nimetatud viide. Nõuete eelnõu võiks sisaldada näiteks järgmist sätet: *„Pädevat järelevalveasutust teavitatakse, enne kui sertifitseerimisasutus hakkab kasutama heakskiidetud andmekaitsepitserit uues liikmesriigis harukontorist.“*

28. Andmekaitsenõukogu sedastab, et Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu punktis 7.2 „Taotlus“ nähakse ette olukord, kus andmetöötlustoimingute tegemiseks kasutatakse suuniste lisa kohaselt volitatud töötlejaid. Andmekaitsenõukogu märgib siiski, et volitatud töötlejate kasutamise korral peab taotlus sisaldama asjaomase vastutava/volitatud töötleja lepingut (lepinguid), nagu on sätestatud lisas. Seepärast soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel viia sõnastus vastavusse suunistega, lisades viite vastutava/volitatud töötleja lepingu(te)le. Lisaks soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel kaalutleda, kas sel juhul peaks viitama ka kaasvastutavatele töötlejatele ja nendevahelistele erikokkulepetele.

[3] Vt selle kohta suuniste 1/2018 lõige 44.

29. Andmekaitsenõukogu nendib, et Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu punktis 7.2 on ette nähtud, et „andmete vastutav töötleja ja volitatud töötleja võivad taotleda sertifitseerimist“. See, kas volitatud töötlejatel on õigus taotleda sertifitseerimist, oleneb sertifitseerimissüsteemist. Seepärast soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel arusaamatuste vältimiseks eespool nimetatud viite välja jätta või täpsustada, et volitatud töötlejate sertifitseerimis võimalus sõltub sertifitseerimissüsteemi kohaldamisalast.

30. Andmekaitsenõukogu märgib Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu punkti 7.3 „Hindamistaotlused“ kohta, et Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõus sätestatakse, et „kavandatud hindamismeetodid sätestatakse lepingus“. Andmekaitsenõukogu soovitab Saksamaa järelevalveasutustel esimene lõik ümber sõnastada, et oleks selge, et see on nõue, et sertifitseerimisleping peab sisaldama hindamismeetodeid, st sõnastada nõue ümber järgmiselt: „kavandatud hindamismeetodid tuleb sätestada lepingus“. Lisaks soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel asendada viide standardi ISO 17065 punktile 7.3.1.b viitega standardi ISO 17065 punktile 7.3, et viia sõnastus vastavusse lisaga. Veel täheldab andmekaitsenõukogu, et neljandas lõigus viidatakse piisavale tehnilisele ja õiguslikule pädevusele. Andmekaitsenõukogu soovitab Saksamaa järelevalveasutustel lisada suurema selguse nimel tekst „andmekaitse valdkonnas“.

31. Andmekaitsenõukogu täheldab, et Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu punkt 7.4 „Hindamismeetodid“ ei sisalda sertifitseerimisasutuse kohustust kirjeldada töötlemistoimingu(te) sertifitseerimiskriteeriumidele vastavuse hindamise mõistes piisavaid hindamismeetodeid. Seepärast soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel muuta nõuete eelnõu, et lisada viide. Näiteks võib lisada järgmise: *„Sertifitseerimisasutus tagab, et sertifitseerimiseks kasutatavates mehhanismides kirjeldatakse piisavalt töötlemistoimingu(te) sertifitseerimiskriteeriumidele vastavuse hindamise mõistes piisavaid hindamismeetodeid.“* Lisaks leiab andmekaitsenõukogu esimese hindamismeetoditega hõlmatava valdkonna kohta, et vajalikkust ja proportsionaalsust tuleb hinnata vajaduse korral ka seoses asjaomaste andmesubjektidega. Andmekaitsenõukogu märgib samuti, et meetodite ja leidude dokumenteerimisele ei viidata. Seepärast soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel muuta eelnõu ja lisada selgesõnalised viited.

32. Andmekaitsenõukogu märgib kehtivate sertifikaatide kohta (Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu punkt 7.4), et lehekülje 13 neljas taane tekitab segadust, sest sellest ei selgu, kuidas on omavahel seotud praeguse ja varasema sertifikaadi kehtivusajad ja kuidas need omavahel kokku sobivad. Lisaks ei näi otstarbekas kahelda teise akrediteeritud sertifitseerimisasutuse varem antud sertifikaadi kehtivuses. Kokkuvõttes tuleks lõigule kasuks teatav selgus nimetatud elementide omavahelistes suhetes. Andmekaitsenõukogu soovitab Saksamaa järelevalveasutustel muuta eelnõu eelkõige täpsustamaks, et isikuandmete kaitse üldmääruse kohase sertifikaadi kehtivuse kestus ei tohi sõltuda muud liiki sertifikaadi kehtivusest.

33. Andmekaitsenõukogu soovitab Saksamaa järelevalveasutustel muuta Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu punkti 7.5 pealkiri „Hindamine“ pealkirjaks „Läbivaatamine“.

34. Andmekaitsenõukogu märgib sertifitseerimist mõjutavate muudatuste kohta (Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu punkt 7.10), et Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõus nähakse ette, et „klienti teavitatakse õigel ajal õigusraamistiku muudatustest, mis teda mõjutavad“. Andmekaitsenõukogu soovitab Saksamaa järelevalveasutustel sertifitseerimisasutuse erapooletuse säilimise vajadust silmas pidades sõnastada lause ümber

järgmiselt: „kliendile antakse õigel ajal üldist teavet õigusraamistiku muudatuste kohta, mis võivad teda mõjutada“. Lisaks võiksid väljendi „Euroopa Andmekaitsenõukogu otsuste“ tähenduse selguse huvides Saksamaa järelevalveasutused viidet täpsustada. Näiteks võiks viidata „Euroopa Andmekaitsenõukogu poolt vastuvõetud dokumentidele“.

35. Andmekaitsenõukogu märgib, et Saksamaa järelevalveasutuste akrediteerimisnõuete eelnõu punkt 7.11 (sertifikaadi lõppemine, piiramine, peatamine või tagasivõtmine) ei hõlma sertifitseerimisasutuse kohustust aktsepteerida Saksamaa järelevalveasutuste otsuseid ja korraldusi võtta tagasi või mitte väljastada sertifikaati taotlejale, kui sertifitseerimisnõuded ei ole enam täidetud. Seepärast soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel see kohustus lisada. Lisaks soovitab andmekaitsenõukogu Saksamaa järelevalveasutustel asendada kooskõlas suuniste lisaga punkti pealkirjas sõna „piiramine“ tekstiga „kestuse piiramine“.

2.2.7 MUUD TÄIENDAVAD NÕUDED

36. Andmekaitsenõukogu soovitab Saksamaa järelevalveasutustel asendada suurema selguse huvides Saksamaa järelevalveasutuste akrediteerimisnõuete alapunktis 8.11.3 „Kaebuste käsitlemine“ viite „õigustatud kaebustele“ viitega „põhjendatud kaebustele“.

3 JÄRELDUSED/SOOVITUSED

37. Saksamaa föderaalse järelevalveasutuse ja liidumaade järelevalveasutuste eelnõus sätestatud akrediteerimisnõuded võivad põhjustada järjekindlusetust sertifitseerimisasutuste akrediteerimisel ja seetõttu tuleb teha järgmised muudatused.

38. Andmekaitsenõukogu soovitab Saksamaa järelevalveasutustel üldmärkusi käsitledes

    1) eelnõu isikuandmete kaitse üldmääruse sõnastusega kooskõlla viimiseks välja jätta viite „Euroopa Andmekaitsenõukogu kinnitab“.

39. Andmekaitsenõukogu soovitab Saksamaa järelevalveasutustel üldisi akrediteerimisnõudeid käsitledes

    1) muuta õigusliku vastutuse nõudeid (alapunkt 4.1), et viia need vastavusse suunistega;

    2) muuta alapunkti 4.1.2.2, et lisada sertifitseerimislepingule kohustus tagada Saksamaa järelevalveasutustele sertifitseerimismenetluses täielik läbipaistvus ja anda sertifitseerimisasutusele juurdepääs taotleja töötlemistoimingutele;

    3) lisada punktile 4.1.2.2 selgesõnaline viide pädeva järelevalveasutuse ülesannetele ja volitustele kooskõlas lisaga;

    4) lisada sertifitseerimislepingu sätetele kohustus võimaldada sertifitseerimisasutusel avalikustada kogu isikuandmete kaitse üldmääruse artikli 42 lõike 8 ja artikli 43 lõike 5 kohane sertifitseerimiseks vajalik teave;

    5) lisada alapunkti 4.1.2.2 kuuendasse taandesse selgesõnaline viide „sertifitseeritavatele toodetele, protsessidele ja teenustele“.

    6) tugevdada alapunktis 4.2.7 esitatud kriteeriume, mida kohaldatakse eraldi juriidilisele isikule kuuluvatele või alluvatele sertifitseerimisasutustele, et arvestada, et

sertifitseerimisasutuse ja juriidilise isiku mis tahes majandussuhted võivad mõjutada tema sertifitseerimistegevuse erapooletust, olenevalt selle eripärast.

40. Andmekaitsenõukogu soovitab Saksamaa järelevalveasutustel vahenditega seotud nõudeid käsitledes

    1) viia alapunkti 6.1.2.1 sõnastus vastavusse suunistega, nõudes teadmiste asjakohasust ja piisavust.

41. Andmekaitsenõukogu soovitab Saksamaa järelevalveasutustel töötlemisnõudeid käsitledes

    1) muuta punkti 7.1, et see sisaldaks selgesõnalist viidet sertifitseerimisasutuse kohustusele täita täiendavad nõuded;

    2) lisada viide heakskiidetud Euroopa andmekaitsepitseri kasutamisele;

    3) viia punkti 7.2 sõnastus vastavusse suunistega, lisades viite vastutava/volitatud töötleja lepingu(te)le;

    4) lisada punktile 7.4 sertifitseerimisasutuse kohustus kirjeldada töötlemistoimingu(te) sertifitseerimiskriteeriumidele vastavuse hindamise mõistes piisavaid hindamismeetodeid;

    5) täpsustada punktis 7.4, et isikuandmete kaitse üldmääruse kohase sertifikaadi kehtivuse kestus ei tohi sõltuda muud liiki sertifikaadi kehtivusest;

    6) lisada punkti 7.11 sertifitseerimisasutuse kohustus aktsepteerida Saksamaa järelevalveasutuste otsuseid ja korraldusi võtta tagasi või mitte väljastada sertifikaati taotlejale, kui sertifitseerimisnõuded ei ole enam täidetud.

4 LÕPPMÄRKUSED

42. Käesolev arvamus on suunatud Saksamaa föderaalsele järelevalveasutusele ja liidumaade järelevalveasutustele ning see avalikustatakse isikuandmete kaitse üldmääruse artikli 64 lõike 5 punkti b alusel.

43. Isikuandmete kaitse üldmääruse artikli 64 lõigete 7 ja 8 kohaselt teatavad Saksamaa järelevalveasutused kahe nädala jooksul pärast arvamuse saamist eesistujale elektrooniliselt, kas nad muudavad oma otsuse eelnõu või jäävad selle juurde. Sama ajavahemiku jooksul esitavad nad muudetud otsuse eelnõu või, kui nad ei kavatse andmekaitsenõukogu arvamust järgida, asjakohased põhjendused, miks nad ei soovi järgida seda arvamust kas tervikuna või osaliselt.

44. Saksamaa järelevalveasutused edastavad andmekaitsenõukogule lõpliku otsuse selle kandmiseks kooskõlas isikuandmete kaitse üldmääruse artikli 70 lõike 1 punktiga y nende otsuste registrisse, mille suhtes on kohaldatud järjepidevuse mehhanismi.

Euroopa Andmekaitsenõukogu nimel

eesistuja

(Andrea Jelinek)

Vastu võetud