Andmekaitsenõukogu arvamus (art 64)

Arvamus 28/2022 Europrivacy sertifitseerimiskriteeriumide Euroopa andmekaitsepitserina heakskiitmise kohta Euroopa Andmekaitsenõukogu poolt vastavalt isikuandmete kaitse üldmääruse artikli 42 lõikele 5

Vastu võetud 10. oktoobril 2022

Euroopa Andmekaitsenõukogu,

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse 2016/679/EL (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 lõiget 2 ja artiklit 42,

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 töökorra artikleid 10 ja 22.

(1) Liikmesriigid, järelevalveasutused, Euroopa Andmekaitsenõukogu ja Euroopa Komisjon julgustavad eelkõige liidu tasandil andmekaitse sertifitseerimise mehhanismide (edaspidi „sertifitseerimismehhanismid“) ning andmekaitsepitserite ja -märgiste kasutuselevõttu selle tõendamiseks, et vastutavate töötlejate ja volitatud töötlejate isikuandmete töötlemise toimingud vastavad isikuandmete kaitse üldmäärusele, võttes arvesse mikro-, väikeste ja keskmise suurusega ettevõtjate konkreetseid vajadusi.[2] Lisaks võib sertifitseerimismehhanismide kasutuselevõtt parandada läbipaistvust ning anda andmesubjektidele võimaluse hinnata asjakohaste toodete ja teenuste andmekaitse taset.[3]

(2) Sertifitseerimiskriteeriumid on sertifitseerimismehhanismi lahutamatu osa. Seetõttu nõutakse isikuandmete kaitse üldmääruses, et riikliku sertifitseerimismehhanismi kriteeriumid kiidaks heaks pädev järelevalveasutus (isikuandmete kaitse üldmääruse artikli 42 lõige 5 ja artikli 43 lõike 2 punkt b) või Euroopa andmekaitsepitseri korral Euroopa Andmekaitsenõukogu (isikuandmete kaitse üldmääruse artikli 42 lõige 5 ja artikli 70 lõike 1 punkt o).

(3) Kui järelevalveasutus kavatseb teha ettepaneku Euroopa andmekaitsepitseri heakskiitmiseks vastavalt isikuandmete kaitse üldmääruse artikli 42 lõikele 5 Euroopa Andmekaitsenõukogu poolt, peaks järelevalveasutus teatama skeemi omaniku kavatsusest pakkuda sertifitseerimismehhanismi kõigis liikmesriikides. Sellisel juhul on Euroopa Andmekaitsenõukogu põhiülesanne tagada isikuandmete kaitse üldmääruse järjepidev kohaldamine isikuandmete kaitse üldmääruse artiklites 63, 64 ja 65 nimetatud järjepidavusmehhanismi abil. Euroopa Andmekaitsenõukogu kiidab selles raamistikus heaks sertifitseerimiskriteeriumid vastavalt isikuandmete kaitse üldmääruse artikli 64 lõikele 2.

(4) Arvamuse eesmärk on tagada isikuandmete kaitse üldmääruse järjepidev kohaldamine, sealhulgas järelevalveasutuste, vastutavate ja volitatud töötlejate poolt, pidades silmas põhielemente, mille sertifitseerimismehhanismid peavad välja töötama. Eelkõige võtab Euroopa Andmekaitsenõukogu hindamisel aluseks suunised 1/2018 määruse (EL) 2016/679 artiklite 42 ja 43 kohase sertifitseerimise ja sertifitseerimiskriteeriumide kindlaksmääramise kohta (edaspidi „suunised“) ning addendumi sertifitseerimiskriteeriumide hindamise suuniste kohta (edaspidi „addendum“), mille avaliku arutelu periood lõppes 26. mail 2021.

(5) Sellest tulenevalt tunnistab Euroopa Andmekaitsenõukogu, et iga sertifitseerimismehhanismiga tuleks tegeleda eraldi ja see ei mõjuta mis tahes muu sertifitseerimismehhanismi hindamist.

[1] Kõiki selle arvamuse viiteid liikmesriikidele tuleb mõista kui viiteid EMP liikmesriikidele.
[2] Isikuandmete kaitse üldmääruse artikli 42 lõige 1.
[3] Isikuandmete kaitse üldmääruse põhjendus 100.

(6) Sertifitseerimismehhanismid peavad võimaldama vastutavatel ja volitatud töötlejatel tõendada vastavust isikuandmete kaitse üldmäärusele. Seega peaksid nende kriteeriumid kajastama nõuetekohaselt isikuandmete kaitse üldmääruses sätestatud isikuandmete kaitse nõudeid ja põhimõtteid ning aitama kaasa selle ühtsele kohaldamisele.

(7) Samas peaks skeemi omanik tagama, et sertifitseerimismehhanism on vastavuses kõigi lisatud või kasutatud ISO standardite ja sertifitseerimistavadega.

(8) Selle tulemusena peaksid sertifikaadid lisama väärtust vastutavate ja volitatud töötlejate jaoks, aidates neil rakendada standarditud ja kindlaksmääratud tehnilisi ja korralduslikke meetmeid, mis tõendatult soodustavad ja edendavad töötlemistoimingute vastavust isikuandmete kaitse üldmäärusele, võttes arvesse valdkonnapõhiseid nõudeid.

(9) Euroopa Andmekaitsenõukogu väljendab heameelt skeemiomanike tegevuse üle, et koostada sertifitseerimismehhanismid, mis on praktilised ja potentsiaalselt majanduslikult tõhusad vahendid, et tagada parem vastavus isikuandmete kaitse üldmäärusele ning suurendada eraelu puutumatuse ja andmesubjektide andmekaitse õigusi, edendades läbipaistvust.

(10) Euroopa Andmekaitsenõukogu tuletab meelde, et sertifikaadid on vabatahtlikud aruandlusvahendid ja et sertifitseerimismehhanismi järgimine ei vähenda vastutavate ja volitatud töötlejate vastutust isikuandmete kaitse üldmääruse täitmise eest ega piira järelevalveasutuste ülesandeid ja volitusi vastavalt isikuandmete kaitse üldmäärusele ja asjaomastele liikmesriigi õigusaktidele.

(11) Käesolevas arvamuses käsitleb Euroopa Andmekaitsenõukogu selliseid teemasid nagu kriteeriumide kohaldamisala, kohaldatavus ja asjakohasus kõigis liikmesriikides.

(12) Arvamuses keskendutakse sertifitseerimiskriteeriumidele. Juhul kui Euroopa Andmekaitsenõukogu nõuab hindamismeetodite kohta kõrgetasemelist teavet, et ta saaks põhjalikult hinnata kriteeriumide auditeeritavust oma kriteeriume käsitleva arvamuse kontekstis, ei hõlma see nimetatud hindamismeetodite heakskiitu.

(13) Euroopa Andmekaitsenõukogu arvamus võetakse vastu isikuandmete kaitse üldmääruse artikli 64 lõike 2 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. Kui Euroopa Andmekaitsenõukogu arvamuses järeldatakse, et kriteeriumeid ei saa arutelu käigus heaks kiita, võib järelevalveasutus esitada kriteeriumid uuesti heakskiitmiseks, kui esialgses Euroopa Andmekaitsenõukogu arvamuses esiletoodud probleemid on lahendatud,

ON VASTU VÕTNUD JÄRGMISE ARVAMUSE:

ASJAOLUDE KOKKUVÕTE

1. European Center for Certification and Privacy (edaspidi „skeemiomanik“) koostas vastavalt isikuandmete kaitse üldmääruse artikli 42 lõikele 5 ja suunistele Europrivacy v.60 kriteeriumid (edaspidi „sertifitseerimiskriteeriumide kavand“, „sertifitseerimiskriteeriumid“ või „kriteeriumid“).

2. Luksemburgi järelevalveasutus esitas 28. septembril 2022. aastal Europrivacy sertifitseerimiskriteeriumid Euroopa Andmekaitsenõukogule heakskiitmiseks vastavalt isikuandmete kaitse üldmääruse artikli 64 lõikele 2. Otsus toimiku täielikkuse kohta tehti 28. septembril 2022.

3. Sertifitseerimismehhanism Europrivacy ei ole isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkti f kohaselt sertifikaat, mis on ette nähtud isikuandmete rahvusvaheliseks edastamiseks ning ei paku seega asjakohast kaitset isikuandmete kolmandatele riikidele või rahvusvahelistele organisatsioonidele edastamise raames vastavalt artikli 46 lõike 2 punktis f sätestatud tingimustele. Tegelikult tohib isikuandmete edastamine kolmandale riigile või rahvusvahelisele organisatsioonile leida aset ainult juhul, kui on täidetud isikuandmete kaitse üldmääruse V peatüki sätted.

2 HINNANG

4. Euroopa Andmekaitsenõukogu on hinnanud sertifitseerimiskriteeriume nende heakskiitmiseks vastavalt isikuandmete kaitse üldmääruse artikli 42 lõikele 5 kooskõlas suuniste lisas 2 (edaspidi „lisa“) ja selle addendumis sätestatud struktuuriga.

5. Euroopa Andmekaitsenõukogu märgib, et skeemi omaniku antud rakendussuunised ja sertifitseerimismehhanismi soovitatud kontrollivahendid ei ole kriteeriumide kogumi lõikes alati järjepidevad. Näiteks jaotises T.2.3.2 nõutakse, et sissetungide avastamiseks ja neist teatamiseks oleks sätestatud eeskirjad, poliitikad, menetlused või mehhanismid (nt sissetungi tuvastamise süsteem, mis jälgib võrguliiklust kahtlase tegevuse tuvastamiseks ja annab teada, kui tuvastab sellise tegevuse), samas kui soovitatud kontrollivahendites viidatakse ülevaatusele ja läbistustestile (nõutud jaotises T.2.3.1). Kuigi sellised vasturääkivused ei ole Euroopa Andmekaitsenõukogu hindamise kohaldamisalas, rõhutab Euroopa Andmekaitsenõukogu, et need võivad saada takistuseks sertifitseerimisasutuse akrediteerimisel, kui skeemiomanik neid ei kõrvalda.

2.1 Sertifitseerimismehhanismi kohaldamisala ja hindamise objekt

6. Europrivacy sertifitseerimismehhanism on üldine skeem, sest see on suunatud tervele reale erinevatele töötlemistoimingutele, mida vastutavad ja volitatud töötlejad viivad läbi erinevates tegevusvaldkondades. Selle sertifitseerimismehhanismi peamised kriteeriumid koosnevad „põhikriteeriumidest“ ning „tehnoloogiliste ja korralduslike meetmete kontrollidest ja järelevalvest“, mis käsitlevad tehnoloogilisi ja korralduslikke meetmeid, mis on kehtestatud töödeldavate isikuandmete kaitseks. „Tehnoloogiliste ja korralduslike meetmete kontrollide ja järelevalve“ kriteeriumide kogumit kohaldatakse üksnes juhul, kui hindamise objekt töötleb andmete erikategooriaid, kuritegudega seotud andmeid või lapse isikuandmeid.

7. Lisaks hõlmavad kriteeriumid samuti „täiendavaid kontekstuaalseid kontrolle ja järelevalvet“, mille eesmärk on tagada, et hindamise objekti andmete töötlemine on kooskõlas valdkonnapõhiste ja tehnoloogiapõhiste nõuetega. Skeemiomaniku esitatud informatiivne maatriks kirjeldab, mis andmetöötlustoimingute kategooriale rakendatakse iga „täiendavate kontekstuaalsete kontrollide ja järelevalve“ kriteeriumide kogumit.

8. Euroopa Andmekaitsenõukogu väljendab heameelt üldiste skeemide üle, mis sisaldavad erikriteeriume, et need oleks skaleeritavad ja neid saaks kohaldada konkreetsetele töötlemistoimingutele või tegevusvaldkondadele. Siiski soovib Euroopa Andmekaitsenõukogu lisaks selgitada, et üldise skeemi kontekstis pole konkreetseid töötlemistoiminguid käsitlevate kriteeriumide täielikkus nõutav ja seega seda käesoleva arvamuse raames ei hinnatud. Lisaks tuletab Euroopa Andmekaitsenõukogu meelde, et kui ta avaldab konkreetsete töötlemistoimingutega seotud dokumendid, peavad skeemiomanik ja akrediteeritud sertifitseerimisasutused neid dokumente arvesse võtma.

9. Hindamise objekti spetsifikatsioonile kohaldatavad kriteeriumid on sätestatud jaotises A.2.1.1 esitatud nõuetes. Protsessile kohaldatavad konkreetsed eeskirjad, mida taotleja ja sertifitseerimisasutus peavad järgima, et määrata kindlaks hindamise objekt, on sätestatud Europrivacy skeemis (10.2 – sertifitseerimisele eelnevad tegevused).

10. Euroopa Andmekaitsenõukogu märgib, et Luksemburgi järelevalveasutuse esitatud dokumentides sertifitseerimismehhanismi kohaldamisala kohta on märgitud, et Europrivacy skeemi kohaldatakse vastutavatele ja volitatud töötlejatele, kes asuvad Euroopa Liidus või Euroopa Majanduspiirkonnas. Kriteeriumide kohaldatavus on määratud kindlaks sõltuvalt taotleja rollist ja kohustustest.

11. Euroopa Andmekaitsenõukogu märgib, et vastutav töötleja võib esitada Europrivacy sertifitseerimisprotsessi hindamise objekti, mille puhul rakendatakse kaasvastutust (kriteerium A.2.7.1). Juhul kui hindamise objekti puhul rakendatakse kaasvastutust, soovib Euroopa Andmekaitsenõukogu rõhutada, et akrediteeritud sertifitseerimisasutus peab olema taotlusprotsessi läbiviimisel hoolikas tagamaks, et hindamise objekt oleks mõttekas ning et taotleja vastutaks täielikult selle eest, et hindamise objekt täidaks kõiki isikuandmete kaitse üldmäärusest tulenevaid kohustusi, mida sertifitseerimismehhanism püüab tõendada. Selle tulemusena võib taotleja ja hindamise objektiga seotud teiste kaasvastutajate vahel sõlmitud kokkulepe nende vastavate vastutusalade kohta isikuandmete kaitse üldmääruses[4] sätestatud kohustuste täitmiseks – olenevalt hindamise objekti töötlustoimingute kontekstist – takistada taotlejat sertifitseerimiskriteeriumeid täitmast.

12. Euroopa Andmekaitsenõukogu märgib, et geneetiliste andmete töötlemine jääb Europrivacy sertifitseerimismehhanismi kohaldamisalast välja. Selle tulemusena ei hinnata Euroopa Andmekaitsenõukogu poolse kriteeriumide hindamise raames kriteeriumide sobivust hindamise objektidele, mis hõlmavad sellist andmetöötlust.

2.2 Töötlemistoimingud

13. Kriteeriumides käsitletakse töötlemistoimingute asjaomaseid komponente (andmed, süsteemid ja töötlemine), pidades silmas sertifitseerimismehhanismi üldist ulatust. Eelkõige võimaldavad kriteeriumid teha kindlaks andmete erikategooriad, mis on määratletud isikuandmete kaitse üldmääruse artiklis 9 (kriteeriumide jaotis G.2 – eriandmete töötlemine).

2.3 Töötlemise seaduslikkus

14. Kriteeriumides nõutakse andmetöötluse seaduslikkuse kontrollimist hindamise objekti iga eraldiseisva töötlemistoimingu korral ning õigusliku aluse nõuete kontrollimist, mis on sätestatud isikuandmete kaitse üldmääruse artiklis 6 (kriteeriumide jaotis G.1 – andmetöötluse seaduslikkus).

2.4 Andmetöötluse põhimõtted

15. Kriteeriumides käsitletakse isikuandmete kaitse üldmääruse artiklis 5 sätestatud andmekaitse põhimõtteid asjakohaselt. Eelkõige nõutakse kriteeriumides, et taotleja tõendaks, et isikuandmed on

[4] *Nende vastutuse määramisel tuleb eelkõige arvesse võtta andmesubjektide õiguste kasutamist ja teabe andmise kohustusi. Lisaks peaks vastutuse jaotus hõlmama muid vastutava töötleja kohustusi, näiteks seoses üldiste andmekaitsepõhimõtete, õigusliku aluse, turvameetmete, andmetega seotud rikkumisest teatamise kohustuse, andmekaitse mõjuhinnangute, volitatud töötlejate kasutamise, kolmandatele riikidele andmete edastamise ning andmesubjektide ja järelevalveasutusega suhtlemisega* (suunised 07/2020 vastutava töötleja ja volitatud töötleja mõistete kohta isikuandmete kaitse üldmääruses).

piisavad, asjakohased ja piirduvad sellega, mis on nende töötlemiseks vajalik (võimalikult väheste andmete kogumise põhimõte).

2.5 Vastutavate töötlejate ja volitatud töötlejate üldised kohustused

16. Kriteeriumid kajastavad isikuandmete kaitse üldmääruse artiklis 24 sätestatud vastutava töötleja kohustusi (jaotis G.4 – vastutava töötleja vastutus) ning nõuavad vastutava ja volitatud töötleja vaheliste lepinguliste kokkulepete hindamist kooskõlas isikuandmete kaitse üldmääruse artikliga 28 (kriteeriumide jaotis G.5 – volitatud töötlejad või alamtöötlejad).

17. Kriteeriumides nõutakse, et kõik taotlejad määraksid ametisse andmekaitseametniku isegi juhul, kui taotleja ei pea isikuandmete kaitse üldmääruse artikli 37 kohaselt andmekaitseametnikku ametisse määrama. Kriteeriumidega kontrollitakse, et andmekaitseametnik vastaks artiklite 37–39 nõuetele (kriteeriumide jaotis G.9 – andmekaitseametnik).

18. Kriteeriumidega kontrollitakse isikuandmete töötlemise toimingute kannete sisu kooskõlas isikuandmete kaitse üldmääruse artikliga 30 (kriteeriumide jaotis G.5.3. – isikuandmete töötlemise toimingute kanded).

2.6 Andmesubjektide õigused

19. Kriteeriumides käsitletakse asjakohaselt andmesubjekti õigust saada teavet kooskõlas isikuandmete kaitse üldmääruse III peatükiga ning nõutakse asjaomaste meetmete võtmist. Kriteeriumides nõutakse samuti meetmete võtmist, et näha ette võimalus sekkuda töötlemistoimingutesse, et tagada andmesubjekti õigused ja lubada paranduste tegemist, kustutamist või piirangute kehtestamist (kriteeriumide jaotis G.3 – andmesubjektide õigused).

2.7 Oht õigustele ja vabadustele

20. Kriteeriumidega nõutakse, et hinnataks ohtu hindamise objekti andmetöötlusega seotud füüsiliste isikute õigustele ja vabadustele kooskõlas isikuandmete kaitse üldmääruse artikliga 35 (kriteeriumide jaotis G.8 – andmetöötluse mõjuhinnang).

2.8 Tehnilised ja korralduslikud meetmed, millega tagatakse kaitse

21. Kriteeriumides nõutakse tehniliste ja korralduslike meetmete kohaldamist, millega tagatakse töötlemistoimingute konfidentsiaalsus, terviklikkus ja kättesaadavus. Samuti nõutakse kriteeriumides tehniliste meetmete võtmist, et rakendada lõimitud ja vaikimisi andmekaitset vastavalt isikuandmete kaitse üldmääruse artiklitele 25 ja 32 (kriteeriumide jaotis G.6 – töötlemise turvalisus ning lõimitud andmekaitse, kriteeriumide jaotis T.1/T.2 – põhilised turvanõuded / laiendatud turvanõuded).

22. Kriteeriumides nõutakse meetmete kohaldamist tagamaks, et isikuandmetega seotud rikkumisest teavitamise kohustused täidetaks õigeaegselt ja ettenähtud mahus vastavalt isikuandmete kaitse üldmääruse artiklitele 33 ja 34 (kriteeriumide jaotis G.7 – andmetega seotud rikkumistega tegelemine).

2.9 Kriteeriumid, et tõendada isikuandmete edastamiseks asjakohaste kaitsemeetmete olemasolu

23. Kriteeriumides nõutakse, et kooskõlas isikuandmete kaitse üldmääruse V peatükiga tuvastataks kõik hindamise objektiga seotud isikuandmete edastamised kolmandatele riikidele ja rahvusvahelistele organisatsioonidele ning et põhjendataks, miks valiti asjakohaste kaitsemeetmete pakkumiseks

asjaomane andmete edastamise mehhanism (kriteeriumide jaotis G.10 – isikuandmete edastamine kolmandatele riikidele või rahvusvahelistele organisatsioonidele).

3. EUROOPA ANDMEKAITSEPITSERI LISAKRITEERIUMID

24. Vastavalt suunistele hõlmab hindamine küsimust „kas kriteeriumides suudetakse võtta arvesse liikmesriigi andmekaitsealaseid õigusakte või stsenaariume“. Kriteeriumide jaotises G.1.1.3 nõutakse, et taotleja esitaks sellise hinnangu riikliku kohustuste täitmise hindamisaruandes (NOCAR). Euroopa Andmekaitsenõukogu märgib, et see aruanne peab sisaldama hindamise objektile kohaldatavate riiklike kohustuste hinnangut ja dokumenteerib meetmed, mille taotleja võtab kohaldatavate eeskirjade täitmiseks ja vajaduse korral pooleliolevad parandusmeetmed. Taotleja ei kasuta skeemi omaniku poolt iga riigi kohta esitatud peamiste riiklike lisanõuete nimekirja ammendava nimekirjana hindamise objekti jaoks asjakohastest riiklikest kohustustest. Skeemi omaniku esitatud minimaalsete täiendavate kontrollide ja järelevalve nõuete indikatiivne nimekiri ei ole sertifitseerimiskriteeriumid, mis jääksid käesoleva arvamuse kohaldamisalasse.

JÄRELDUSED/SOOVITUSED

25. Kokkuvõttes leiab Euroopa Andmekaitsenõukogu, et Europrivacy sertifitseerimiskriteeriumid on isikuandmete kaitse üldmäärusega kooskõlas ja kiidab need heaks vastavalt Euroopa Andmekaitsenõukogu ülesandele, mis on määratletud isikuandmete kaitse üldmääruse artikli 70 lõike 1 punktis o, mille tulemuseks on ühine sertifikaat (Euroopa andmekaitsepitser).

26. Euroopa Andmekaitsenõukogu registreerib Europrivacy sertifitseerimismehhanismi sertifitseerimismehhanismide ning andmekaitsepitserite ja -märgiste avalikus registris vastavalt artikli 42 lõikele 8.

LÕPPMÄRKUSED

27. Käesolev arvamus on suunatud Luksemburgi järelevalveasutusele ja see avalikustatakse isikuandmete kaitse üldmääruse artikli 64 lõike 5 punkti b alusel.

Euroopa Andmekaitsenõukogu nimel

eesistuja