ANDMEKAITSE INSPEKTSIOON

Lp Tõnu Grünberg
Justiits- ja Digiministeerium
info@justdigi.ee

Teie 12.02.2026 nr 7-1/1078

Meie 06.03.2026 nr 2.3-4/26/590-2

Arvamuse avaldamine eelnõule

Täname, et saatsite Andmekaitse Inspektsioonile (AKI) arvamuse avaldamiseks EL küberturvalisuse määruse uue versiooni (CSA2 ja kaasnevatele lihtsustamismeetmetele, mis on seotud küberturvalisuse 2. direktiivi (NIS2) muutmisega) ettepaneku. Käesolevaga esitab AKI oma tähelepanekud.

1. Sertifitseerimine IKÜM ja CSA2 alusel

CSA2 ettepaneku artikli 80 lõike 1 punkti w kohaselt on Euroopa küberturvalisuse sertifitseerimise skeemide sisu ülesandeks tagada isikuandmete töötlemise turvalisus. CSA2 alusel välja antav sertifikaat võib praktikas olla kasulik tõendusmaterjal, mis näitab, et organisatsiooni tehnilised turvameetmed võivad vastata ühtlasi isikuandmete kaitse nõuetele. Seda kinnitab ka CSA2 ettepaneku põhjenduspunkt 79, mille kohaselt peaks sertifitseerimisraamistik (ECCF) andma võimaluse tõendada vastavust erinevatele küber- ja andmeturbenõuetele ühe sertifitseerimismeetme kaudu, et vähendada koormust ja ühtlustada nõudeid. Põhjenduses rõhutatakse, et organisatsioonid seisavad korraga silmitsi mitmete regulatsioonide nõuete täitmisega ning seetõttu võib ühtne sertifikaat aidata lihtsustada mitme paralleelse regulatsiooni täitmist.

Oluline on siiski rõhutada, et CSA2 sertifikaat ei asenda IKÜMi artikli 42 alusel antavat sertifikaati. CSA2 keskendub küberturbe nõuetele, IKÜM seevastu nõuab lisaks tehnilistele meetmetele ka õiguslike põhimõtete järgimist, sealhulgas läbipaistvust, andmete minimaalsust, eesmärgipärasust, andmesubjekti õiguste tagamist ning töötlemise õiguspärasust. Need jäävad CSA2 sertifikaadi ulatusest välja, kuna CSA2 sertifitseerimisskeem ei ole mõeldud hindama isikuandmete kaitset tervikuna. Teatav kattuvus võib esineda IKÜMi artiklis 32 sätestatud töötlemise turvalisuse nõuetega, kuid siinjuures tuleks panna tähele, et IKÜMi artikli 32 lõike 3 kohaselt võib artikli 32 nõuetele vastavust tõendada artikli 42 alusel heakskiidetud sertifitseerimismehhanismi järgimisega.

2. EAKNi ja CSIRT võrgustiku koostöö

CSA2 artikli 68 lõike 1 kohaselt peab ENISA tegema koostööd EAKNiga. On positiivne, et selline koostöökohustus ENISA ja EAKNi vahel on CSA2 selgesõnaliselt ette nähtud. EAKN on varem oma valmidust kinnitanud 22. juuli 2024[1] kirjaga. Küll aga on oluline märkida, et selline koostöö ei tähenda andmekaitseasutuste ja küberturbe intsidentidele lahendamise üksuste (Computer Security Incident Response Teams ehk edaspidi CSIRTid) vahelist süsteemset ja struktureeritud

[1] [1] EAKN vastus ENISA kirjale 22. juulil 2024. EDPB response to letter on collaboration with ENISA | European Data Protection Board

koostööd.

EAKNi moodustavad riiklikud andmekaitseasutused, samal ajal kui CSIRTid on koondatud CSIRT võrgustikku (CSIRTs Network). CSIRT võrgustiku suhe ENISAga on reguleeritud NIS2 direktiivi artiklis 15. Kuigi mõlemate siseriiklike pädevate asutuste võrgustike koostöö ENISAga on kas juba ette nähtud või nähakse käesoleva ettepanekuga, ei ole ette nähtud koostöövormi EAKNi ja CSIRT võrgustiku enda vahele. Samal ajal on Euroopa Liidu õigusruumis sellised koostöövõimalused muude asutuste vahel juba ette nähtud, näiteks digiturgude määruse kõrgetasemeline töörühm (DMA HLG), kus osalevad nii EAKN kui ka Euroopa konkurentsivõrgustik. See näitab, et horisontaalne koostöö erinevate regulatiivsete asutuste vahel on võimalik.

EAKN ja CSIRT võrgustiku koostööl oleks märkimisväärsed eelised. Esiteks võimaldaks see välja töötada ühiseid seisukohti olukordades, kus andmekaitse ja küberturbe kohustused põimuvad, näiteks küberturbeintsidentide ja isikuandmete rikkumiste teavitamiskohustuste ristumiskohtades. Ühtsed juhised vähendaksid õiguslikku killustatust ja annaksid ettevõtetele või organisatsioonidele selgemad ootused. Teiseks looks otsene koostöö kanali kiiremaks infovahetuseks olukordades, millel on samaaegselt nii küberturbe- kui ka andmekaitseline mõõde. CSIRTid tuvastavad sageli intsidente enne kui vastutavad töötlejad andmekaitseasutusi teavitavad, mistõttu otsekontakt parandaks oluliselt andmekaitseasutuste informeeritust ja reageerimisvõimet. Samuti oleks andmekaitseasutustel sellisel juhul võimalus anda CSIRTidele juhised olukordadeks, kus vastutavad töötlejad teavitavad küberrikkumistest küll CSIRTe, kuid hindavad rikkumise sellisele tasemele, et andmekaitseasutusi ei teavitata.

Samas tuleb arvestada ka võimalike probleemidega. Andmekaitseasutused ja CSIRTid tegutsevad erinevate õiguslike volituste alusel, andmekaitseasutused rakendavad IKÜMi ja lähtuvad põhiõiguste kaitse loogikast, samal ajal kui CSIRTid tegutsevad küberturbe ja kriitiliste intsidentide lahendamise raamistikus. See tähendab, et riskitõlgendused ja konfidentsiaalsusnormid ei pruugi alati kattuda. CSIRTidel võib olla ligipääs tundlikule tehnilisele teabele, mida ei saa andmekaitseasutustega jagada, samas andmekaitseasutuste käsutuses võivad olla isikuandmed, mida CSIRTidel ei ole volitust töödelda.

Selge õigusliku mehhanismita piirdub koostöö tõenäoliselt siseriiklike *ad hoc* kontaktidega, millel ei ole piisavalt kaalu, et tagada järjepidevust ja õigusselgust. Ühtlasi on selline koostöö vabatahtlik.

3. ENISA andmetöötluse õiguslik alus intsidentidest teavitamisel

CSA2 ettepanek näeb ette ENISA rolli märkimisväärset laiendamist, sealhulgas ülesannete tugevdamist EL-i küberturvalisuse poolel ja intsidentide teavitamise mehhanismide loomisel. Kavandatud ühtne intsidentidest teavitamise mehhanism tähendab, et ENISA hakkab toimima keskse infosõlmena, mille kaudu liiguvad ka isikuandmeid sisaldavad teated, mistõttu on vajalik selge ja konkreetne õiguslik alus isikuandmete töötlemiseks.

Käesolev ettepanek ei sisalda sätteid, mis annaksid ENISA-le õiguse töödelda isikuandmeid nende uute ülesannete täitmiseks. Kuigi ettepanek viitab vajadusele arendada ühtne teavitussüsteem ja toetada liikmesriike koostöös, ei täpsusta see töötluse eesmärke ega andmekategooriaid ning seetõttu ei vasta see määruse (EL) 2018/1725 (edaspidi EUDPR) nõudele, mille kohaselt peab töötlemine tuginema selgele EL-i õiguslikule alusele, mis määratleb täpsed ülesanded ja vajaliku töötlemise ulatuse.

ENISA andmetöötlust reguleerib EUDPR, mis seab Euroopa Liidu institutsioonidele IKÜM-iga sisuliselt samaväärsed põhimõtted. EUDPR sätestab raamistikud ja tingimused, millele peab töötlemine tuginema, samas kui õiguslik alus isikuandmete töötlemiseks peab tulenema mõnest muust EL-i õigusaktist, mis annab ENISA-le vastava ülesande ning kirjeldab töötluse vältimatut vajadust. Kuna CSA2 ettepanek õiguslikku alust ei sisalda, tekib olukord, kus ENISA-l võivad tulevikus olla ülesanded, mis sisuliselt eeldavad isikuandmete töötlemist, kuid mille töötlemiseks puudub õiguslik alus.

4. Tarneahela turvalisus ja andmete edastamise piirangud kolmandatesse riikidesse

CSA2 artikli 103 lõike 2 punkt b annab komisjonile võimaluse näha rakendusaktiga ette, et teatud üksused ei tohi küberturberiskide maandamiseks edastada andmeid kolmandatesse riikidesse ega kasutada sellist andmetöötlust, mida tehakse kolmandast riigist. Teisisõnu võimaldab see säte piirata olukordi, kus andmetele pääsetakse ligi või neid töödeldakse väljastpoolt Euroopa Liitu, kui sellega kaasneb oht liidu küberturvalisusele, kübervastupidavusele või usaldusele.

Andmete kolmandasse riiki edastamise kohta on sätted ka IKÜMi V peatükis. CSA2 artikli 103 lõike 2 punkti b ja IKÜM V peatüki suhet tuleb mõista kumulatiivsena, mitte alternatiivsetena. Asjaolu, et CSA2 alusel võib komisjon kehtestada teatavatele üksustele keelu seoses andmete edastamisega kolmandatesse riikidesse või kolmandas riigis toimuva andmetöötlusega, ei tähenda, et IKÜM V peatükk muutuks kohaldamatuks. IKÜM V peatükk sätestab tingimused, mille esinemisel võib isikuandmete edastamine kolmandasse riiki olla lubatud, kuid see ei anna iseseisvat ega absoluutset õigust selliseid edastusi teha sõltumata muudest liidu õiguse nõuetest. CSA2 alusel kehtestatud keeld või piirang ei tähenda seda, et IKÜM V peatüki nõuded kaotaksid tähtsuse. Kui tegemist on isikuandmete edastamisega, tuleb paralleelselt hinnata ka vastavust IKÜM V peatükile, kuivõrd IKÜM V peatükk kaitseb isikuandmete edastamisel andmesubjektide õigusi ja tagab kaitsetaseme jätkumise pärast andmete liikumist kolmandasse riiki.

Praktikas võib see tekitada õigusselguse probleeme, sest kolmanda riigi andmeedastuse lubatavus ei sõltu siis enam ainult IKÜM V peatükist, vaid potentsiaalselt ka CSA2 määrusest. Andmetöötleja jaoks ei pruugi olla läbipaistev, millal pelgalt IKÜMi järgimisest enam ei piisa. Seoses CSA2 artikli 103 lõike 2 punktiga b võiks määruses sisalduda täpsustus, et sätte kohaldamine ei piira IKÜM V peatüki kohaldamist, ning selgitus, et isikuandmete puhul tuleb mõlemat raamistikku hinnata paralleelselt.

5. Lunavararünded

Lunavararünnete avastamine, nende kohta teabe kogumine ja juhtumite kohta ülevaate loomine on küberturvalisuse seisukohalt oluline. Samas ei muuda see üleliigseks nõuet, et juhul kui kogutav või jagatav teave sisaldab isikuandmeid, peab selline andmetöötlus olema õiguspärane, eesmärgipärane ja piirduma vajalikuga.

NIS2 määruse ettepaneku põhjenduspunktis 10 kasutatakse lunavararünnete juures väljendit “tundlik teave”. Sellise mõiste kasutamine ei tähenda, et tegemist oleks IKÜM artikli 9 mõttes eriliigiliste isikuandmetega, vaid pigem osutab see sellise teabe tundlikkusele küberturbe ja konfidentsiaalsuse vaatest. Tegemist on olulise vaheteguriga, kuivõrd IKÜM artikli 9 mõttes tundliku teabe töötlemine on üldjuhul keelatud, väljaarvatud IKÜM artikkel 9 lõike 2 erandite kohaldumisel.

Lugupidamisega

(allkirjastatud digitaalselt)

Pille Lehis
peadirektor

Kirsika Nigul
kirsika.nigul@aki.ee
6828712